법제교류 연구 15-18-①
International Legal Collaboration Research 15-18-①

A Comparative Study on ICT Laws in India and Korea

Jiyeon Choi · Jupi Gogoi

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

법제교류 연구 15-18-①
International Legal Collaboration Research 15-18-①

A Comparative Study on ICT Laws in India and Korea

Jiyeon Choi · Jupi Gogoi

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

A Comparative Study on ICT Laws in India and Korea

Researchers : Jiyeon Choi (Research Fellow, KLRI)
Jupi Gogoi (Professor, Indian Law Institute)

Sep. 15, 2015

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

Abstract

Ⅰ. Purpose and Scope of Research

□ In Asia, Korea and India are considered as countries with advanced technology in information and communications field, based on each country's highly developed industrial foundation.

□ With the rapid growth of the business in the ICT field and the take it brings to the national economy, coupled with the level of complexity of the technology that the industry entails, it is obvious that relevant legislation needs to be carefully drawn and match the speed of the development to avoid lagging.

□ Overview of Laws related to ICT issues from India and Korea is provided with introduction and brief analysis of key elements, followed by comparison.

Ⅱ. Contents

□ ICT Laws in India

○ The aim of the 『IT Act』 was to set up India's first ever information technology legislation.

○ To bring the『IT Act』in line with the「Model Law on Electronic Signatures adopted by the UNCITRAL」, the『Information Technology (Amendment) Act, 2008』(『IT(Amendment)Act』) was passed in December 2008, and was made effective from 27th October, 2009.

○ Both the『IT Act』and the『IT Act Amendment』protects data and privacy through various penalization provisions and hold a legal person liable for breach.

○ 『IT Act』and『Copyright Act』provides specific circumstance when intermediaries are held liable

○ Key legal issues pertaining to cloud computing are data protection, privacy and security, and liabilities of the cloud service providers

□ ICT Laws in Korea

○ Historical Developments of ICT Laws in Korea are reviewed: chronologically, laws on ICT can be grouped into five stages - (1) Expansion of Foundation for Telecommunications (1902 - 1986), (2) Drive for Computerization (1987 - 1994), (3) Initiative for National Informatization (1995 - 2003), (4) Full-Scale National Informatization (2004 - 2007), and (5) Regulation for Broadcasting Communications Convergence (2008 -).

○ The amendment on the『Framework Act on Broadcasting Communications Development』that provides the concept of the broadcasting communications and also manages the policy on the broadcasting and communications were made, in the hope of providing a firm legal foundation for the converged and unified sector.

○ 『Special Act on Promotion of Information and Communication Technology, Vitalization of Convergence Thereof, Etc.』 (a/k/a 『Special Act on ICT』) builds itself as a legal foundation for the support for software and web-contents businesses as well as R&D and materialization of business ideas for the new convergence technology and services

○ 『Act on the Development of Cloud Computing Development and the Protection of Users』 aims to reform regulations that hinders development of the cloud computing business, to provide legal foundation for promotion policies for the industry, and also to maintain a secured cloud computing service use to systematically and comprehensively grow the cloud computing business

Ⅲ. Expected Effects

□ Through this comparative analysis of laws on ICT in India and Korea, this research hopes to build a helpful resource for scholars and legislatures as well as entrepreneurs and researchers in the field in their quest of journey for better legislation on and implementation of ICT laws.

□ This research report may be utilized as basic information for ICT Laws in India and Korea

Key Words : Information and Technology Law, ICT Law, India, Korea

Table of Contents

Ⅰ. Introduction

A. Purpose of Research

The dynamics of ICT laws were substantially changed after the inclusion of intellectual property rights in WTO. From mere Copyright (and Related Rights) and Industrial Property, WTO-TRIPS classified intellectual property rights laws in many other forms, which caused changes of regulations on overall ICT laws. In Asia, Korea and India are considered as countries with advanced technology in information and communications field, based on each country's highly developed industrial foundation. With the rapid growth of the business in the ICT field and the take it brings to the national economy, coupled with the level of complexity of the technology that the industry entails, it is obvious that relevant legislation needs to be carefully drawn and match the speed of the development to avoid lagging. India has been implementing the primary law on ICT that governs overall aspects of the ICT sector, while Korea has many different laws that have been enacted and amended to keep up with the speed of technological development. The purpose of this research will be to examine the importance of ICT laws, to review developments and history of ICT laws, to analyze key features of important laws on the subject from both India and Korea, and to draw comparison between the two countries so that to concoct implications for each other. Through this comparative analysis of laws on ICT in India and Korea, this research hopes to build a helpful resource for scholars and legislatures as well as entrepreneurs and researchers in the field in

their quest of journey for better legislation on and implementation of ICT laws.

B. Scope of Research

Overview of laws related to ICT in India is provided, and the primary features and traits on the issue are explained and analyzed more in detail. Discussions on legislative history of enactment and amendment of laws are provided along with explanations of caselaws and anecdotes on the same. Specifically, the original 『Information Technology Act, 2000』 and its Amendment were studied in depth, and the issues of data protection, intermediaries responsibilities, and cloud computing service providers' liabilities are carefully examined.

Korean ICT Laws are introduced, starting from the historical developments, policy issues, to the key laws in the field. As provided in the Indian Chapter, discussion and explanations on legislative history of enactment and amendment of vital laws of the field in Korea are described, with explanations on the background of each rule making, illustration on social circumstances, and narration of the industrial development policies. Analysis on provisions of each law that are of importance in learning and understanding current status of the law in ICT field is to be provided, along with implications of such analysis that lay suggestions for improvements.

Following each country's ICT Laws and developments is the comparison of the two in the conclusion, suggestions for improvements for the two countries from each other's legislative experience.

Jiyeon Choi from Korea Legislation Research Institute and Jupi Gogoi from Indian Law Institute jointly conducted this research project. Jupi

Gogoi provides legal resources and analysis on Indian Law in Chapter Ⅱ while Jiyeon Choi of Korea Legislation Research Institute furnishes the remaining Chapters Ⅰ, Ⅲ, and Ⅳ.

Ⅱ. ICT Laws in India

A. ICT Laws in India: An Overview

1. Background and Overview of the 『Information Technology Act, 2000』

Internet came in India in 1995 and after almost 5 years, the Indian legislature framed its first cyber law[1] titled The 『Information Technology Act』 (hereafter 『IT Act』). It received the assent of the President[2] on the 9th June, 2000 and came into effect on 17th October, 2000.

The preamble to the 『IT Act』 states that the Act is based on the 「Model Law on Electronic Commerce of United Nations Commission on International Trade Law (UNCITRAL)」 which was later adopted by the General Assembly of the United Nations.[3] It cannot be denied that

1) Abha Chauhan, "Evolution and Development of Cyber Law: A study with special reference to India" available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195557 (lat visited August 17, 2015).

2) In India, Bills become an Act only after the President puts assent after the passing of the Bill by both Houses to Parliment.

3) An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law; AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information; AND WHEREAS it is considered necessary to give effect

international pressure and obligation was vital in adoption of this legislation in India. Moreover e-commerce started in India in early nineties and it was also a important catalyst for framing the legislation.

The Preamble to the Act mentions that it is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information. The aim of the 『IT Act』 was to set up India's first ever information technology legislation. The main aim for the enactment of the legislation was (a) to facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions, (b) to enable the use of digital signatures in authentication of electronic records; and (c) to showcase India's growing IT prowess and the role of Government in safeguarding and promoting IT sector. Overall, the 『IT Act 2000』 was important from many perspectives. There were many cyber crimes and that had to be regulated. The recognition of digital signature by the Act for purposes of authentication paved the way for electronic contracts, e filing etc. which further paved the way for electronic commerce in India.[4)]

Due to the increase of information technology enabled services and the increase in cyber crimes, concerns of data security have assumed greater

---

to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. Available at: http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf (last visited August 20, 2015).

4) Aparna Vishwanathan, Cyber Law Indian & International Perspectives 25 (Lexis Nexis Butterworths, Nagpur, 1st edn.,2012). *See also* Vakul Sharma, Information Technology Law & Practice 430 (Universal Law Publishing Co. Ltd., New Delhi, 3rd edn.,2012)

importance. The 『IT Act』 seemed to be inadequate to deal with many problems, such as, how cyber crimes affecting computers in India committed from outside India using the Internet will be handled; there were no provisions regarding domain names and resolving disputes on such names; certain cyber crimes like cyber defamation, cyber harassment and cyber stalking were not defined; privacy and protection of personal data such as medical records were not covered; there were no provisions to punish persons or organizations sending unsolicited mail normally known as spam etc.[5)]

Due to the aforementioned inadequacy, and, to bring the 『IT Act』 in line with the 「Model Law on Electronic Signatures adopted by the UNCITRAL」, the 『Information Technology (Amendment) Act, 2008』 (『IT(Amendment)Act』) was passed in December 2008, and was made effective from 27th October, 2009. A review of the amendments indicates that eight new cyber offences[6)] were introduced. Also several provisions relating to data protection and privacy[7)] as well as provisions to curb terrorism using the electronic and digital medium were introduced into the new Act.

The provisions of the 『IT Act』 deals with various aspects of information technology, the most important provisions include giving legal

---

5) V. Rajaraman, Essentials of E-Commerce Technology 229 (P.H.I. Learning Pvt. Ltd., New Delhi, 1stedn.,2010).

6) Sending offensive messages through a computer or mobile phone (Section 66A), Receiving stolen computer resource or communication device (Section 66B), Punishment for identity theft (Section 66C), Punishment for cheating by personation using computer resource (Section 66D), Punishment for violating privacy or video voyeurism (Section 66E), Cyber Terrorism (Section 66F), Publishing or transmitting material in electronic form containing sexually explicit act (Section 67A) and Child pornography (Section 67B)

7) The IT(Amendment) Act, 2008 incorporates provisions pertaining to data base security and privacy in Section 43, 43 A, 66E and 72A.

recognition to electronic records[8] and to electronic signatures (formerly digital signature).[9] Chapter Ⅱ of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

The Act starts new electronic governance in India. The Act states that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference.

Chapter Ⅲ of the Act includes provisions relating to attribution,[10] acknowledgement,[11] and time of dispatch[12] and receipt of electronic record. Chapter Ⅳ of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of electronic signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue electronic Signature Certificates.

---

8) S.4 of the IT Act.
9) *Id.* at S.5.
10) *Id.* at S.11.
11) *Id.* at S.12.
12) *Id.* at S.13.

Chapter Ⅶ of the Act details about the scheme of things relating to electronic Signature Certificates. The duties of subscribers are also enshrined therein.

Chapter Ⅸ of the said Act talks about penalties and adjudication for various offences. There are penalties for various offences that damages computer, computer systems, computer network etc.

The IT Act creates an Adjudicating Authority who has been given the power of a civil court. The adjudicating authority shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under.

Under chapter Ⅹ a tribunal has been constituted named Cyber Appellate Tribunal to deal with any matter pertaining to contravention of the Act and the rules. It shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

Chapter Ⅺ of the Act talks about various offences and the said offences shall be investigated only by a police officer not below the rank of the deputy superintendent of police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking. There are provisions relating to liability of intermediaries as well.

2. Other ICT Laws

Besides the 『IT Act』, there are other legislations and various regulations which might directly or indirectly deal with different aspects of ICT. For example, the 『Indian Penal Code』 (『IPC』) is the criminal statute in India and many provisions can be used against person who contravenes or does an act contrary to the ICT norms.

Besides when we go to more technical aspects, such as, banking and telecom sector, the『IT Act』cannot be sufficient. So there are many contemporary regulations which has been framed in order to protect consumers as a part of ICT norms. They are discussed elaborately in the chapters to come.

B. ICT Law: Key Areas of Concern

1. Data Protection and Privacy Issues

a. Data Protection and Privacy in General

The laws concerning data protection and privacy in India can be classified into two time lines, namely the original『IT Act』and the『Amended IT Act』.

i. Provisions regarded as providing rules pertaining to data protection prior to the 2008 Amendments to the『IT Act, 2000』

Even before the 2008 amendments to the『IT Act, 2000』, there were certain provisions which indirectly discussed about data protection in India. There were provisions penalizing contraventions related to unauthorized access to computer, computer system, computer network or resources, unauthorised alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, computer database, etc. Some sections of those Chapters are viewed in India as the “backbone” of the data protection regime. The important provisions are:

Penalty for damage to computer, computer system, etc.

Section 43 states that if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network accesses; downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; introduces any computer contaminant or virus; damages any data, computer data base or any other programmes residing; disrupts; denies access to any person authorized to access any computer, computer system or computer network by any means; provides any assistance to any person to facilitate access in contravention of the provisions of this Act; charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network shall be liable to pay damages by way of compensation to the person so affected.

In nutshell, this section foresees civil liability in case of data, computer database theft and may cover computer trespass, unauthorised digital copying, downloading and extraction of data, computer database or information, theft of data held or stored in media is covered, unauthorised transmission of data or programme residing within a computer, computer system or computer network, use of cookies, or spywares. Digital profiling is not legally permissible, so is unauthorised access to computer data/ databases, etc.

Tampering with computer source documents

Section 65 provides that whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal,

destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment and fine.

Hacking with Computer System

Section 66 first defines hacking. It states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. Section 66 further states that whoever commits hacking shall be punished with imprisonment and fine or with both.

It is important to mention that the word diminishes in value/utility has considerable impact upon the confidentiality of a document. For e.g. if any sensitive personal e-mail is saved in a computer and if any person accesses the said document, then the value of the information is completely lost, this will make then party liable under this provision.

Penalty for breach of confidentiality and privacy

Section 72 penalizes any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there-under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such information to third party.

This was the only section in the original Act requiring the consent of the concerned person but, given its limited scope, it would be difficult to consider that it could provide a sufficient level of personal data protection.

Indeed, this section confines itself to the acts and omissions of those persons, who have been conferred powers under the Act, rules or regulations made there-under.

ii. The 『2008 Amendment to the IT Act』 and path-breaking changing scenario in Data Protection Regime in India

The most important provisions relating to data protection and privacy in India inserted by the Amendment Act are section 43A, section 66A and section 72A of the IT Act. They are:

Compensation for failure to protect data.

Section 43A provided that if a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and causes wrongful loss or wrongful gain to any person shall be liable to pay damages by way of compensation. It is an important provision in the sense that the sole objective of it is to protect personal data and privacy. It creates a responsibility on the 'body corporate' to implement and maintain 'reasonable security practises and procedures' in order to protect sensitive personal data or information. The provision is important because it creates a private right of action in civil law by which any person could move against body corporate for the negligent handling of their personal data or information.[13] The liability is imposed on the body corporate and not the natural person. It is obvious from the First Explanation given under section 43A the term body corporate means any company and includes a firm, sole proprietorship or other association of

13) *Supra* note 4 at 190. Aparna Vishwanathan.

individuals engaged in commercial or professional activities. Although there was a lot of deliberation with regard to inclusion of any person but the Standing Committee who was given the task of bringing our amendment in the Act felt that it should initially be restricted only to body corporate. And once the system is in place it can be extended to individuals as well.[14] Since section 43A did not explain certain important aspects the Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011. These rules defined the term sensitive personal data or information, prescribed specific duties on body corporate to protect the personal data.

Although this is a progressive provision, it has its own drawbacks. Firstly, there is no prescribed amount of compensation that is fixed. Although there was a lot of initial discussion about the fixation of compensation term but eventually when section 43A was inserted no fixed amount was laid down. Moreover since no explanation has been provided for the term 'wrongful loss and wrongful gain' it creates another problem.

Punishment for sending offensive messages through communication service, etc.

Section 66A provides that any person who sends, by means of a computer resource or a communication device, (a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer

14) *Ibid.*

resource or a communication device, (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine. The Explanation to the provision provided the terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

Punishment for Disclosure of information in breach of lawful contract

Section 72A provides for punishment with regard to disclosure of information in breach of lawful contract. This provision reads as "save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment or with both." This provision was inserted by the 2008 Amendment to the IT Act, 2000. It even makes service providers and intermediaries liable for disclosing information which they have received by lawful contract to third parties without consent of the information or data provider.

b. Data Protection in the Banking Sector

Due to the nature and the matters involved, data protection becomes vital in case of financial transaction specially banking transactions. Further, since data which may have facets of sensitive personal information, is being sent from one jurisdiction to another (e.g. BPO operations of banks), its protection is all the more relevant. Banking fraud is a rampant problem. The banking frauds are credit/debit card fraud, electronic fraud, identity theft etc. Identity theft is where personal details are obtained to get some sort of financial or other benefit, leaving the owner of that identity often in large debt with a negative credit history and in some cases with legal implications. Electronic frauds include frauds in internet banking, mail scams etc. Credit or Debit card frauds could be both through electronic and telecom means as well.

In India there have been instances which have prompted the authorities to bring out provisions relating to safety of banking transactions and bank details of customers.

The laws, rules and regulations on online banking frauds in India can be dealt under two heads, first, penal provisions on technology related banking frauds and, second, supervisory and regulatory mechanism to prevent online banking frauds.

The first important provision is section 66 A(c) of the 『IT Act』 which creates an onus on the sender of the message not to send a message by means of computer resource or computer device for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages and shall be punishable with imprisonment for a term which may extend to three years and with fine.

This may be relevant in case of telemarketing where the tele-marketer may mislead the recipient to divulge banking details.

The next important provision is section 66C which provides for punishment for identity theft. A person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. This provision can be applicable in case of theft of banking passwords.

Even section 66D dealing with cheating by personation by using computer resource can be used for banking frauds which are computer based.

The only worry is the fact that nowhere in these provisions the liabilities on the banks are imposed. However there is section 72 and 72 A of the Act which provides that any person and without the consent of the person concerned discloses electronic record, book, register, correspondence, information, document or other material to any other person or any person or intermediary knowing that it is likely to cause wrongful loss or wrongful gain discloses information, without the consent of the person concerned, or in breach of a lawful contract will be held guilty under the 『IT Act』. Section 79 on the other hand provides for exclusion of liability of intermediaries on certain occasions. Whether the banks could be booked under these provisions is not very clear and this aspect needs legal examination.[15)]

15) http://www.rajdeepandjoyeeta.com/internet-banking.html (last visited August 20, 2015).

c. Data Protection in the Telecom Sector

Data theft in telecom sector is not a new thing. Telemarketing is an immensely popular mode of ecommerce but it involves matters of privacy and data theft. Along with the Telecom Regulatory Authority of India (TRAI) and Department of Telecom (DoT) which are the main regulators in India, even the IT Act in some provisions deal with data protection and privacy in telecom sector. Section 66A(c) can be drawn in this regard. Section 66A(c) provides that any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to two three years and with fine. The explanation to the provision mentions that the terms “Electronic mail” and “Electronic Mail Message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message. Moreover section 66D penalizes cheating by personation through communication device or computer resource. Hence along with TRAI regulations and DoT guidelines, they may also be charged under these provisions.

Saying this it is pertinent to mention that in spite of these regulations and laws, the data theft and privacy violation in telecom goes on. There is lack of proper implementation of the law and Regulations. Moreover unawareness is another major hurdle in this regard.

2. Intermediaries Responsibilities

It is a well known fact that parallel to the physical world, a virtual world exist as well. There may be many laws and regulations to protect the privacy and data of people in the physical world but there is an increased need felt for pro.tecting the same in the virtual world. Interestingly, in the virtual world the liability aspect not only involves the person who actively performs the act but also the intermediaries who plays an important role in making the content available.

In case of liabilities of intermediaries, there are two set of laws that are important in India. The first one is 『Copyright Act, 1957』 and the second one is 『Information Technology Act, 2000』 (『IT Act』). The definition of intermediaries as stated in section 2(w) of the IT Act is anyone who receives, stores, transmits or provides any service with respect to electronic message. It is a wide definition which includes telecom provider, internet service providers (ISPs), web hosting service providers, search engines, online payment, online auction, cyber cafes etc.

Intermediaries under both the legislations can be held liable broadly under these two circumstances; (a) When proved that intermediary has conspired/abetted/aided/induced in the commission of unlawful act and (b) when the intermediary do not follow the "Take Down"[16] procedures. Some of the take down provisions are under 『IT Act, 2000』 and few are under the 『Copyright Act, 1957』. In this study only the provision relating to IC Act I included.

16) Take down is a process operated by intermediaries in response to court orders or allegations that content is illegal. Content is removed by the host following notice. Notice and take down is widely operated in relation to libel, copyright infringement and other kinds of illegal content.

Under the 『IT Act, 2000』, section 79 is extremely important. Section 79 is titled as intermediaries not to be liable in certain cases. The conditions provided are that an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.[17] The next provision, that is, section 79(2) states that the intermediaries will also not be liable if the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or the intermediary does not initiate the transmission, select the receiver of the transmission and select or modify the information contained in the transmission. The next provision further state that the intermediaries will also not be responsible if it observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.[18] Due diligence in this provision is explained under Rule 3(2) of

17) Section 79(1).

18) Section 79 in The Information Technology Act, 2000 as amended in 2008. Exemption from liability of intermediary in certain cases. –

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him

(2) The provisions of sub-section (1) shall apply if-(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary does not-(i) initiate the transmission,(ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act; (b) upon receiving

the Information Technology Intermediaries Guidelines Rules 2011 (hereinafter IT Guidelines 2011) which provides that the intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person and shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any objectionable and illegal content.

Under the『IT Act』, section 79(3) provides that intermediaries will be held liable when (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act; (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner (basically if they donot follow take down provisions). The Explanation to the provision states that for the purposes of this section, the expression “third party information” means any information dealt with by an intermediary in his capacity as an intermediary. Moreover, Rule 3 (4) of the「IT Guidelines, 2011」provides for a 36 hour deadline for take

---

actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner. Explanation. -For the purpose of this section, the expression “third party information” means any information dealt with by an intermediary in his capacity as an intermediary.]

down after obtaining information or by affected person in writing or email signed with electronic signature.[19] The reason may be copyright infringement, obscenity, hurt of religious sentiments etc.

Before the amendment of section 79 in 2008, the onus was on the intermediaries to prove that they were unaware or that they exercised due diligence about third party information without excluding any categories of intermediaries.[20] But by the 2008 amendment to the provision, the onus has been shifted to the complainant to prove the 'contributory liability' of the intermediary that they have conspired, abetted the commission of the unlawful act which is very difficult to prove.[21] The only positive aspect of the amendment is that the intermediary will be liable if they fail to remove despite the actual knowledge or notice from the government agency.

Another important provision with regard to liability of intermediaries is Section 69A of the IT Act which penalises intermediaries if it fails to comply the direction of Central Government or any of its officer specially authorized by it in this behalf to block access by the public or cause to be blocked for access by public any information generated,

19) Gazzette of India, available at: http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf (last visited August 10, 2015).

20) Section 79 before the Amendment of 2008. Network service providers not to be liable in certain cases.

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Explanation.－For the purposes of this section, － (a) "network service provider" means an intermediary; (b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

21) Karnika Seth, Computers, Internet and New Technology Laws, Lexis Nexis Butterworth 2012 page 460.

transmitted, received, stored or hosted in any computer resource if it is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence.

Censorship of online content is definitely important keeping in mind the trend of posting illegal material. The intermediaries especially that of ISPs role is vital to stop abuse of internet as a medium. But there are important observations which need to be made as to the law that is framed and rules made to make the intermediaries liable. Some concerns that needs to be looked into are that although a time period of thirty six hours is fixed to intermediaries as per section 79(3) of the IT Act read with Rule 3(4) of the IT Intermediaries Guidelines, 2011 as mentioned above to take down content from their website but most social networking sites contend that due to the vast content posted filtering becomes difficult and pre-censoring is also tough as well. Moreover there can be many subjective interpretations of the terms public order or for preventing incitement to the commission of any cognizable offence as provided under section 69A of the IT Act. So until and unless clear guidelines as to implementation and clarification of such subjective terms are given, censorship in many cases might be used for curbing free speech and expression.

3. Cloud Computing and Data Protection

In nutshell, the following are the legal issues pertaining to cloud computing: Data protection, Privacy and Security, and Liabilities of the cloud service providers.

a. Data Protection

Section 2(o) of the 『IT Act, 2000』 define data as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. When an organization or a person decides to use the cloud computing services, they store their vital information in the cloud. It can be ranging from important document of the organizations to private medical history of an individual. Hence the protection of data becomes vital in case of cloud computing.

A perusal of the data protection laws worldwide makes it clear that there are certain vital elements which are essential in order to protect the data.[22)]

The first important element is consent. It is essential to obtain consent for collection, use or disclosure of personal data.[23)] Moreover for processing of data too consent is required. The next important element is data integrity. It is provided in most legislations that personal data should be accurate and updated[24)] and the personal data should also be corrected upon request.[25)]

---

22) EU Directive 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995; Singapore Personal Data Protection Act, 2012; UK Data Protection Act, 1988

23) http://www.gateway-law.com/newsletter/Article%20on%20Data%20Protection%20Bill.pdf. (last visited august 21, 2015).

24) Section 14(1) & Clause 4, Part I of Schedule I of the UK Data Protection Act, 1988 & Section 22 of the Singapore Personal Data Protection Act, 2012

25) Section 22 Singapore Personal Data Protection Act.

The other important element includes retention of data, data access, protection against data loss and prohibition in transferring to other countries. With regard to data retention, it is provided that personal data shall be obtained only for certain specified and lawful purposes and shall not be processed[26] for other purposes. Moreover the data shall not be kept for longer than is necessary for that purpose.[27]

With regard to data access and data loss, it is provided that individuals providing personal data can access their personal data by organisations upon request. Appropriate measures will be taken to prevent unauthorised access, collection, use, disclosure, modification, disposal of personal data. Moreover there will be technical and organizational measures take against accidental loss or destruction of or damage to personal data. The last important element is with regard to data location. Personal data providers may specify a preferred data location and that data should not move beyond the particular location.[28]

The legal regime in India with regard to data protection has been discussed in the previous chapter. In this chapter an analysis is done whether these legal provisions on data protection can be applicable in case of cloud computing.

---

26) Data processing intends to cover any conceivable operation on data, ranging from collecting, recording, holding of the and the carrying out of any operation on those data through to their subsequent disclosure and eventual destruction.

27) *Supra* note 24. Principle 5, Part I of Schedule I of UK Data Protection Act

28) EU directive states that personal data shall not be transferred to a country or territory beyond EEA unless the country or territory has adequate level of protection for the rights and freedom of data subjects (the living individual who can be identifies from those data or from those data together with other information which is in or is likely to come into the possession of the entity who decides what the data will be used for) in relation to the processing of personal data.

In India, the 『IT Act』 has included section 43A which mentions that where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay compensation to the person so affected. Although the provision was included by the 『IT (Amendment) Act, 2008』, but the explanations of important terms in the provision was laid down much later in 2011 by Department of Information Technology in the 「Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011」 (in brief 「The Rules」). 「The Rules」 mentioned that Sensitive Personnel Data or Information consists of (a) Passwords; (b) Financial information such as bank account or credit card or debit card or other payment instrument details; (c) Physical, physiological and mental health condition; (d) Sexual orientation; (e) Medical records and history and (f) Biometric information. This definition is much narrower in scope than the other data protection regimes, take for instance European Union which includes race, etc. But the biggest demerit which occurred later in 2011 was when the Ministry issues a Press Note to clarify the Rules. The clarifications can affect the cloud computing in India as they are regarding sensitive personal data or information and are applicable to the body corporate or any person located within India. The rule was that any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located

within or outside India is not subject to the requirement of Rules 5 (collection of information with consent only) & Rule 6 (disclosure of information). However, body corporate, providing services to the 'provider of information'(natural persons providing sensitive data or information) under a contractual obligation directly with them, as the case may be, however, is subject to Rules 5 & 6.[29] The clarification creates confusion instead of clarifying as to why a body corporate should not be held liable while handling sensitive data under a contract with a legal entity located within or outside India. Moreover making body corporate liable in case of data provided by individuals is hardly of use as rarely individuals enter into agreements with data processors.[30]

The greatest disadvantage is that in India there is yet no proper provision on transfer of data. Most data protection laws mentions about prohibition of data transfer beyond the country or beyond a particular territory.[31] Rule 7 does mention that data will not be transferred until and unless there is same level of protection. This provision is taken from the European directives but the irony is that in the other jurisdictions there are proper principles and laws laid down to decide the parameter on same level of protection before transfer. In India there is no dedicated legislation, but, only section 43A of the 『IT Act』 read with section 72A which vaguely mentions about same level of protection.[32] Thus lack of a concrete provision threatens the protection of data. In a nutshell, broad interpretations of the provisions could deal with cloud computing in

29) http://www.pib.nic.in/newsite/erelease.aspx?relid=74990 (last visited August 10, 2015).

30) Aparna Vishwanathan, *Cyber Law Indian & International Perspectives* 25 (Lexis Nexis Butterworths, Nagpur, 1stedn.,2012)., at 192

31) *Ibid.*

32) Punishment for Disclosure of information in breach of lawful contract

India. Saying this, it is also important to mention that there are many lacunas which need immediate attention.

b. Privacy and Security

In case of sensitive personal data,[33] it is essential in many regimes that explicit consent should be there while collecting or processing data for performing a legal obligation.[34] Sensitive Personnel Data or Information in India consists of (a) Passwords; (b) Financial information such as bank account or credit card or debit card or other payment instrument details; (c) Physical, physiological and mental health condition; (d) Sexual orientation; (e) Medical records and history and (f) Biometric information.[35] This definition of sensitive personal data is quite insufficient as there might be areas like racial, ethnic, religious philosophical beliefs[36] which ought to have been covered in the definition. In future, this lack of comprehensive definition of the term sensitive personal data or information might create serious privacy concerns. So the policy makers need to pay attention in this direction as well.

Further Rule 4 of the Rules provides that the body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information

33) It generally consist of information about race, health, religion, politics, union membership or criminal offences under the UK legislation. An overview of UK data protection law available at: https://www.taylorwessing.com/uploads/tx_siruplawyermanagement/NB_000168_Overview_UK_data_protection_law_WEB.pdf (last visited august 6, 2015).

34) *Id.* at pg. 7.

35) the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, at Rule 3

36) Other regimes includes these under the definition.

including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on web site of body corporate or any person on its behalf and shall provide for (i) Clear and easily accessible statements of its practices and policies; (ii) type of personal or sensitive personal data or information collected under rule 3 (iii) purpose of collection and usage of such information; (iv) disclosure of information including sensitive personal data or information as provided in rule 6; and (v) reasonable security practices and procedures as provided under rule 8.

Under the UK regime, another important provision is that in case of data which are not sensitive data, before processing it consent is required or the processing is necessary for the performance of a contract to which the data subject is a party. But in case of sensitive data protection, additional obligations are imposed, that is, consent has to be 'explicit'. In India, under Rule 6 which deals with the disclosure of information, consent is definitely the cornerstone for disclosing sensitive personal data. However, it is not necessary to obtain consent if such disclosure has been agreed to in the contract between provider of information and body corporate.

Another area which can be quite disturbing is disclosure without prior consent in case of government agencies mandated under the law to obtain information including sensitive personal data or information. The only solace is that the government agency under the rules has to send a request in writing to the body corporate stating the purpose of seeking such information.[37] Increasing government surveillance is a serious concern affecting privacy of citizens.

37) the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, proviso to Rule 6

c. Liabilities of the Cloud Service Providers

Moreover to protect the data and privacy, there is also need to create positive obligations on the cloud service providers with regard to data and privacy protection. Most jurisdictions mention that appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.[38] In some legal systems it is provided that to protect personal data in possession, security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar use must be made. In comparison, the Indian situation can be considered to be better for the reason that Rule 8 is quite comprehensive. Rule 8 provides that a body corporate or a person on its behalf has to formulate and implement acceptable security practices, international standards such as 「IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System – Requirements"」 or other best practices as are recognised by the central government. In the event of an information security breach, they have to prove that they have implemented security control measures as per their documented information security programme and information security policies. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgrade of its process and computer resource.

38) *Supra* note 22, Clause 55 of the EU Directive; Principle 7 Part I of Schedule I of the UK Data Protection Act.

i) Remedies, Compensation, Accountability

Although there are rules which creates a positive obligation on the body corporate to have adequate measures to provide securities and protect data but the proper implementation and unawareness is a major problem.

Moreover under section 72A which provide for punishment for disclosure of information in breach of lawful states that any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. But the definition of intermediary[39] means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. The definition has not yet included the term cloud service provider. So until the definition is amended or the judiciary declares that cloud service can be included within the definition, it might create problems of the public.

Undoubtedly, the concept of data privacy and protection is at a nascent stage in India. Framers of the Rules have attempted to adopt ideas from

39) Section 2(1)(w) of the IT Act.

jurisdictions which have long standing and mature data protection regulations. These Rules are only therefore a first step. Stringent implementation of the law and healthy development of the data privacy and protection is what is required in the long run.

Ⅲ. ICT Laws in Korea

A. Overview

1. Historical Developments of ICT Laws

Along with the rapid developments in the field of the information technology, the laws related to the Information and Communications Technology also experienced evolvement and changes. As shown with the recent government policy focusing on the development and promotion of the Information Technology industry, numerous laws on ICT field including, but not limited to,『Internet Multimedia Broadcast Services Act』and『Act on the Establishment and Operation of Korea Communications Commission』, have been enacted that paved the way to the advancement of information technology business in Korea. From the very early stages of the ICT laws that discussed telecommunications, the rather primitive stage of the technology and the social perception of the field, to the most recent laws that even devises convergence of different fields, many laws on this area have been enacted, amended, and enforced.

It may seem too tangled to tackle each and every law unless a set standard for categorization exists, and there may be multiple ways to group laws: by the controlling government agency, by the nature of the law, by government policy, and so on. As a foundational information report of the current status of ICT laws in Korea for foreign readers, the most logical way to divide laws into different groups would be to bundle them reflecting their chronological order along with the driving force for

each law - based on government policy. This way, chronologically, laws on ICT can be grouped into five stages - (1) Expansion of Foundation for Telecommunications (1902 - 1986), (2) Drive for Computerization (1987 - 1994), (3) Initiative for National Informatization (1995 - 2003), (4) Full-Scale National Informatization (2004 - 2007), and (5) Regulation for Broadcasting Communications Convergence (2008 -).[40]

(1) Expansion of Foundation for Telecommunications (1902 - 1986)

During the period before 1986 when the government focused on forming a non-competitive environment for efficient distribution of the telecommunications resources for the public good, the growth and development of the telecommunications resource pool was the primary goal to achieve. This period of time may be divided into two, having the first half with the government perform exclusive and direct business operations on the telecommunication sector under the 『Telecommunications Act』, and the latter half when the telecommunications service providers were privatized, when the 『Telecommunications Act of 1961』 amended the previous 『Telecommunications Act』.

(2) Drive for Computerization (1987 - 1994)

Between 1987 and 1994, the foundation of the revolutionary development of the information technology and internet that started in the mid-1990 was formed by connecting telecommunication and computer, and the government enacted 『Act on Computing Network Supply Expansion and Use Promotion』 for the creation of the information society.

40) Based on advisory opinion by Professor Sungmin Cha of Hannam University.

(3) Initiative for National Informatization (1995 - 2003)

With the world wide communications system and the domestic tele-communications market opening, liberalization and competition grew more fierce around the world. The collapse of the cold-war system and the beginning of the WTO system in 1995 drove the world to the infinite competition, which positions information technology as the most vital element to compete with each other. Korean government underwent an administrative reform, turning Postal Department into the Department of Information and Telecommunications and forming the Informatization Promotion Committee with ministers of different departments as the committee members. This committee, along with the Department of Information Telecommunications, achieved connecting primary education institution networks with high-speed communications network, and the next Kim Dae-Jung administration also held the Informatization Strategy Meeting that marked the promotion and separate operation of the e-government and economy-booster policy. 『Electronic Government Act』, 『Act on Protection of Information and Communications Infrastructure』, 『Digital Signature Act』, and other laws on promotion of informatization were enacted during this period.[41)]

(4) Full-Scale National Informatization (2004 - 2007)

Development in the Information Technology field reached to the point where IT and administrative work converged and achieved advancement of the electronic government, and broadcasting communication convergence

41) Hyunkyung Kim, "Next Administration's Informatization Governence and its legal implication", Vol.13 Issue 4 of Public Law Research, pp 58-59, 2012

and the convergence between traditional industries became natural. Roh Mu-Hyun Administration pursued the two-way informatization drive, where the government informatization sourced to the government reform, procedural evolution, all-government system building, and electronic- government, whereas the same helped to the information industry including software development and digital contents design.

Laws enacted during this period include 『Internet Address Resources Act』, 『Act on Development of E-Learning Industry and Promotion of Utilization of E-Learning』, 『Act on Protection, Use, Etc. of Location Information』, 『Game Industry Promotion Act』, 『Internet Multimedia Broadcasting Services Act』, to name a few.

As clearly indicated on the provisions of the 『Framework Act of the National Informatization』 in 1995, Korean government conceived Informatization as the primary route and possibly the only way to transfer the society into a "Information Society", and thus any and all regulation that hinders the informatization were considered as to be amended. Thus laws to promote informatization appeared first, followed by laws that were expected to solve any unintended side effects of such informatization.[42)]

(5) Regulation for Broadcasting Communications Convergence (2008 -)

Traditional division of service areas and items became blurry with the convergence of network and convergence of service provisions that developed along with the advancement of technology in communications and information transmissions system. Convergence over the layers, fields,

42) E.g., Framework Act on National Informatization, Digital Signature Act, Act on the Protection of Information and Communications Infrastructure, Telecommunications Business Act.

or sectors introduced new types of corporate merger, acquisition, or strategy alliance between broadcasting business and telecommunications industry.[43] Such association and unification between two sectors that were previously considered different breeds brought about issues with regulation and the regulating body in the government. Need for a unified agency that could oversee all information technology related communications business arose, and Lee Myung-bak government finally came down with an overhaul of the government bodies, abolished the old Information Communications Department and replaced it with the Broadcasting Communications Committee. This resulted numerous laws on IT issues that once were regulated and supervised by one department, the Department of Information and Communications, being scattered into multiple departments and agencies to be enforced and regulated.

2. Current Status of ICT Laws

In furtherance to the initiation, development, and sophistication of ICT laws, a couple of important laws were amended under the current administration.

(1) 『Digital Signature Act』

With the emerging and rapidly-growing e-commerce industry, ensuring security and veracity of electronic documents were considered the primary concern of the government that the government enacted the “Digital Signature Act” in 1999. This Digital Signature Act aims to ensure

43) Sungmin Cha, Analysis on Current Domestic and International Status on the Communications Industry with the Outside Circumstances Change, Report for Korea Electronic Communications Institute, pp. 15-18, 2008

security and trust of electronic documents and to regulate basic provisions on digital signatures. It is used along with the Accredited Certificate in verifying one's identity online, although the Accredited Certificate invited heated criticism for its unstability and inconvenience until now.

(2) 『Framework Act on National Informatization』

Assessment and Accreditation Program for Information Protection System was devised under Section 38 of the 『Framework Act of the National Informatization』 to enhance the level of information protection and to protect valuable assets from any possible side effects of informatization. The K-Standard that conform with the then-current level of assessment in the country was developed and announced in 1998 under the program, and such assessment program expanded its territory to protection systems for OS, virtual network, fingerprint verification system, and to smart cards. Over the past years, the unification of the different standards for evaluation was established through a Common Criteria while levels of security have been adjusted to maintain appropriate protection system. In 2014, a beta service for the web-application firewall and intrusion prevention system launched to attract further research and development as well as distribution of the information protection products.[44)]

(3) 『Act on Promotion of Information and Communications Network Utilization and Information Protection』

With the diversion of the telecommunications and information service into a convergence of the traditional industry with IT, as shown with

44) Ministry of Science, ICT, and Future Planning, 2014 Annual Report on National Informatization, pp. 333-335

social network services, big data, cloud computing, telematics in machinery and automobile industry, smart grid in energy business, and healthcare. Without careful thoughts on security being placed from the beginning of the service or designing of the item, a breach would bring about serious economic loss as well as social chaos. To cope with this issues, ex-ante inspection on information technology was recommended in Section 45-2 of the 『Act on Promotion of Information and Communications Network Utilization and Information Protection』. This ex-ante inspection requires to remove vulnerability prior to the utilization of service or product by detecting the weak point at the structuring stage of the new IT service. Through this inspection, more than 3,000 security vulnerabilities were spotted and removed before the service became available for the public, resulted in heightened security and stability in the field.[45)]

(4) 『Act on the Protection of Information and Communications Infrastructure』

Considering that the main infrastructure and service that a government and its citizens use are closely connected with each other, it is highly possible that any breach in one part of the cyber system will spread to administration, broadcasting, communication, energy, finance, and other information system, affect the society as a whole, and may freeze other parts of the system which in turn also would invoke malfunctioning of the State. For this very reason, the 『Act on the Protection of Information and Communications Infrastructure』 was enacted in 2001, designating Important information system and network of the government as the

45) Ministry of Science, ICT, and Future Planning, 2014 Annual Report on National Informatization, pp. 335-336

essential information and communication infrastructure, being subject to the assessment of weaknesses and establishment of response strategy.

(5) 『Personal Information Protection Act』

Collecting Personal Identification Number without valid legal reason has been banned since 2013 in accordance with the amendment of the 『Personal Information Protection Act』. Violation of such provision may be fined up to 5 hundred million Korean won, along with being subject to disciplinary action for the person in charge of such violation. In order to establish a preemptive measure to any infringement of personal information arose out of public information sharing, Korean government also provided 「Rules for Personal Information Protection per Public Information Sharing and Processing Stages」 in 2013. By this rules declared, the Korean government tries to achieve a set standards and principles on the protection of personal information at each information processing stage.[46)]

B. Key ICT Laws and Their Implications

Along with the laws that were amended to meet the changed needs of the society in the ICT fields, there also are laws newly enacted to cover technological developments and related concerns that sprang up over time. Below, introduction and analysis of the most important laws in ICT fields are provided.

46) Ministry of Science, ICT, and Future Planning, 2014 Annual Report on National Informatization, pp. 335-343

1. 『Framework Act on Broadcasting Communications Development』

(1) Background

With the development of broadcasting and communications technology along the way to the information society, the line between the traditionally considered broadcasting and communications became blurry, with the emerging new convergence services such as IPTV or DMB. To cope with this new era of the convergence and communications environment rather pro-actively, Korean government launched the Broadcasting and Communication Committee that sets out and implements policies on both broadcasting and communications. However, lack of a unified law that covers both broadcasting and communications became an obstacle for the committee to effectively perform its duties that are laying over the two sectors of broadcasting and communications. Thus the amendment on the 『Framework Act on Broadcasting Communications Development』 that provides the concept of the broadcasting communications and also manages the policy on the broadcasting and communications were made, in the hope of providing a firm legal foundation for the converged and unified sector.

(2) Key Features

It is important to note that the new combined concept of “broadcasting communications” was presented for the first time in the effort of preventing a loophole in terms of the legal definition at Article 2 of this 『Framework Act on Broadcasting Communications Development』.

Article 2

1. The term “broadcast communications” means the transmission (including transmission to the general public) or reception of contents for broadcast communications by a wired, wireless, optical, or other electronic system and a series of activities accompanying such transmission and reception and includes the following:

(a) Broadcasting under Article 2 of the Broadcasting Act;

(b) Internet multimedia broadcasting under Article 2 of the Internet Multimedia Broadcast Services Act;

(c) Telecommunications under Article 2 of the Framework Act on Telecommunications;

As compared to the discussion on each subject separately previously, with this law a new and combined legal definition was provided for broadcasting communications, which also laid ground for related concepts such as broadcasting communications service, broadcasting communications business, broadcasting communications facilities.

Along with the unification of the terminology, the body that regulations the newly defined broadcasting communications business must also be unified and so it did into the broadcasting communications committee; however, the regulations that governs the industry are still split and independent from each other as the traditional 『Broadcasting Act』 and the 『Electronic Communications Business Act』 still stand at large. After the enactment of the 『Framework Act on Broadcasting Communications Development』, efforts were made to also enact a unified business act in the same field but to no avail until present, due to the distinct traits of broadcasting and communications, as well as to the political reasons.

Article 3 through 5 provides the primary direction of the policy for broadcasting communications.

Article 3 (Public Benefit, Public Nature, etc. of Broadcast Communications)

The State and each local government shall endeavor to accomplish the following matters in order to fulfill public responsibilities based on the public benefit and public nature of broadcast communications:

1. The enhancement of public welfare, the balanced development between regions or classes, and the formation of sound social communities through broadcast communications;
2. The promotion of a sound culture for broadcast communications and the creation of proper environments for the use of broadcast communications;
3. The encouragement of the development of technology and services for broadcast communications and the creation of environments for fair competition;
4. The prevention of alienation of social minorities or the socially weak;
5. The boosting of pluralism and diversity of the media environment by means of broadcast communications;
6. The establishment and implementation of policies on broadcast communications through transparent and open decision-making.

Article 4 (Protection of Rights and Interests of Viewers and Users)

(1) No broadcast communications business entity shall discriminate against viewers or users without a justifiable cause in rendering broadcast communications services.

(2) Every broadcast communications business entity shall endeavor to heighten the convenience of viewers and users through broadcast communications.

(3) No one shall undermine another person's reputation or violate other person's rights without a justifiable cause by means of broadcast communications.

Article 5 (Principles in Regulation on Broadcast Communications)

(1) The Korea Communications Commission shall endeavor to ensure that it

equally regulates services considered identical, taking into comprehensive consideration distinct characteristics of, or technology for, broadcast communications services or the forms in which services are rendered to views and users, etc.
(2) The Korea Communications Commission shall establish an independent evaluation plan each year for the regulation of broadcast communications, conduct evaluations, and establish and publicly release a plan necessary for the rational regulation of broadcast communications based on the results of such evaluations.

The public concern and public benefits trait of broadcasting communications were pronounced through articles 2 to 5 while vesting obligations for the State and the municipalities to enhance such publicness of broadcasting communications. It is obvious that broadcasting communications has inherent publicness due to its effectiveness towards the society, yet it cannot be overlooked that broadcasting communications are still the combination of two distinctive features of broadcasting and communications previously. Broadcasting traditionally valued service for the public heavily whereas communications industry placed more weight on generating profit as business enterprises. When applying a comprehensive law to those two concepts (that has been converged as one), there could be issues of too much/too little regulation unless each separate sectors' inherent traits were carefully considered and balanced.

And of course the drive for the policy for transition and convergence of broadcasting communications and the related services would be possible when suitable and workable funding system is established. Related provisions on the fund are listed from Article 24 through Article 27.

Article 24 (Establishment of Broadcast Communications Development Fund)
The Korea Communications Commission shall establish Broad Communications Development Fund (hereinafter referred to as the "Fund") in order to support promotion of the development of broadcast communications.

Article 25 (Formation of Fund)
(1) The Fund shall be formed with the following financial resources:
1. The Government"s contributions and loans;
2. The charges collected pursuant to Article 7 (2) of the Radio Waves Act, the considerations for the allocation of frequencies under Article 11 (1) of the aforesaid Act (including cases to which the aforesaid paragraph shall apply mutatis mutandis pursuant to Article 16 (4) of the aforesaid Act), guarantee money under Article 11 (5) of the aforesaid Act, and the amount calculated in accordance with Article 17 (2) of the aforesaid Act;
3. The charges under paragraphs (2) through (4);
4. Contributions by broadcasting business entities;
5. Gains from the operation of the Fund;
6. Other revenues specified by Presidential Decree.

(2) The Korea Communications Commission may collect a charge from each terrestrial broadcasting business entity and each business entity using a broadcasting channel for general service or specialized news service within 6/100 of sales of broadcast advertisement during the relevant year, as prescribed by Presidential Decree.

(3) The Korea Communications Commission may collect a charge from each general cable broadcasting business entity and each satellite broadcasting business entity under the Broadcasting Act and each internet multimedia broadcasting business entity under the Internet Multimedia Broadcast Services Act within 6/100 of sales of broadcasting services during the relevant year, as prescribed by Presidential Decree.

(4) The Korea Communications Commission may collect a charge from each business entity using a broadcasting channel for specialized services

of the introduction and sales of goods within 15/100 of operating income at the time of the settlement of accounts for the previous year, as prescribed by Presidential Decree.

(5) The Korea Communications Commission may exempt or abate the charge under paragraph (1) 3 for a person whose scale of business or capability to assume the burden does not reach a specified level and may establish a differential charge rate to each broadcast communications business entity in the light of the public nature and profitability of broadcast communications, etc., as prescribed by Presidential Decree.

(6) If a person obligated to pay a charge in accordance with any provision of paragraphs (2) through (4) fails to pay it by the payment deadline, the Korea Communications Commission may impose an additional charge within 5/100 of the past due amount, as prescribed by Presidential Decree.

(7) If a person obligated to pay a charge under paragraph (1) 3 and an additional charge under paragraph (6) fails to pay them by the payment deadline, the Korea Communications Commission shall collect them in the same manner as delinquent national taxes are collected.

Article 26 (Use of Fund)

(1) The Fund shall be used for the following projects and activities: <Amended by Act No. 11373, Feb. 22, 2012>

1. Projects for the research and development of broadcast communications;
2. Projects for the development, establishment, and dissemination of standards for broadcast communications;
3. Projects for training human resources for broadcast communications;
4. Projects for boosting broadcast communications services and developing the foundation for broadcast communications services;
5. Supporting broadcast communications operated for public interests and public services;

5-2. Supporting the production of broadcasting programs for public interests pursued by a terrestrial broadcasting business entity in a local area of a network and a small- and medium-sized terrestrial

broadcasting business entity under Article 22 of the Act on Broadcast Advertising Sales Agencies, etc.;

6. Supporting the production and distribution of content for broadcast communications;
7. Supporting broadcast programs produced by viewers themselves and media education;
8. Remedial measures for damage sustained by viewers and users and projects for the enhancement of their rights and interests;
9. Rendering assistance for the development of advertisements through broadcast communications;

9-2. Supporting expenses incurred in the operation of the committee for the balanced development of broadcast advertising under Article 23 (7) of the Act on Broadcast Advertising Sales Agencies, etc.;

10. Rendering assistance to classes of society alienated from broadcast communications in their access to broadcast communications;
11. Supporting international exchange and cooperation and inter-Korean exchange and cooperation in broadcast communications;
12. Supporting overseas broadcasting in Korean language;
13. Compensation for losses under Article 7 (1) of the Radio Waves Act;
14. Consideration for the allocation of frequencies, which shall be returned pursuant to Article 7 (5) of the Radio Waves Act;
15. Other projects resolved by the Korea Communications Commission as necessary for the development of broadcast communications.

(2) The Korea Communications Commission may utilize part of the Fund as financial resources for loans and investments for enhancing the public nature of broadcast communications and promoting the development of broadcast communications as well as for the welfare of viewers.

(3) Matters under paragraph (1) 1 shall be subject to prior consultation with the Minister of Knowledge Economy

Article 27 (Management and Operation of Fund)

(1) The Fund shall be managed and operated by the Korea Communications Commission.

(2) Council for the Operation of the Broadcast Communications Development Fund shall be established for the fair and efficient management and operation of the Fund.
(3) Council for the Operation of the Broadcast Communications Development Fund shall be comprised of not more than ten members who shall be appointed by the Chairperson of the Korea Communications Commission, subject to the resolution by the Korea Communications Commission.
(4) Necessary matters concerning the composition and operation of Council for the Operation of the Broadcast Communications Development Fund shall be prescribed by Presidential Decree.
(5) The Korea Communications Commission may entrust the part of administrative affairs related to the collection, operation, and management of the Fund to an institution or organization related to broadcast communications services, as prescribed by Presidential Decree.
(6) Further details necessary for the operation and management of the Fund shall be prescribed by Presidential Decree.

It is much needed to secure funding for the policy implementation, and the utilization of the funds available towards R&D, standard development and distribution are specified in the provisions. Another provision on funding in the field of broadcasting and communications is provided in the Article 41 of the『Act on Promotion for Information Communications Industry』. When compared those two provisions, Article 24 of the『Framework Act of Broadcasting Communications Development』and Article 41 of the『Act on Promotion for Information Communications Industry』, function of the two funding are similar while the sources place stark difference – The former supplies its funding from the contributions of the broadcasting businesses whereas the latter furnishes its capital by the share of expenses paid by telecommunications businesses.

Along with the convergence of broadcasting and communications, the 『Framework Act on Broadcasting Communications Development』 serves as "The Law" for all broadcasting and communications field; then it is rightful to place the fund provision currently left in the 『Act on Promotion for Information Communications Industry』 to be also stationed in the 『Framework Act on Broadcasting Communications Development』.

2. 『Special Act on Promotion of Information and Communication Technology, Vitalization of Convergence Thereof, Etc.』 (a/k/a 『Special Act on ICT』)

(1) Background

With the new administration, the government experienced major re-construction of the government body, having the "Ministry of Science, ICT, and Future Planning" newly established. The enactment of the 『Special Act on ICT』 was also in line with having the Ministry of Science, ICT, and Future Planning to work towards what its initial plan aimed for - to achieve the "creative economy and citizens' happiness through science technology and ICT," which was presented as one of the main goals to accomplish by this administration.

The 『Special Act on ICT』 as the vehicle to promote national economy and convergence of different fields of industry, especially IT businesses and others, is meaningful. The 『Special Act on ICT』 also supplements what were lacking through the government body restructuring and provides a comprehensive management system for the Ministry of Science, ICT, and Future Planning to oversee and control all ICT industry. The

Act builds itself as a legal foundation for the support for software and web-contents businesses as well as R&D and materialization of business ideas for the new convergence technology and services.

(2) Key Features

The 『Special Act on ICT』 left a remarkable distinction by clearly declaring that the law was set for the promotion and convergence of information and communications businesses and by backing up such notion with practical provisions that effectively realizes such promotion even in innovative ways. For example, the 『Special Act on ICT』 flipped the regulatory system from positive to negative, setting out allowing new convergence services and technologies as the principle of the market unless proven illegitimate. Article 3-7 provides:

> (7) The State and each local government shall, in principle, allow new technologies and services for the convergence, etc. of information and communications technology insofar as relevant statutes are not violated, and make active efforts to vitalize such matters.

Keeping a narrow door open and letting only lawful devices in to the market has been the foundational system of almost all regulation; however, in the fast-phased technology arena where yesterday's high-tech no longer remain as hip today, maintaining the door open for any and all possibly legitimate technology encourages development and promotion of new thoughts which leads to innovation and progress of industry. This Article 3(7) turning the positive entry list to the negative block list clearly plays a tremendous role in improving and boosting fast commercialization of technology, and this vividly shows the core spirit of this law

that aims to promote convergence of information and communications business.[47)]

With the clear goal to accomplish, what counts next is whether the support system exists to run the vehicle to reach the finish line. In this law, Article 15 through Article 20, and Article 30 systematically works as a comprehensive support system for the promotion and convergence of information and communications business.

> Article 15 (Designation, etc. of Promising Technologies, Services, etc.)
>
> (1) In order to vitalize new technologies and services for information and communications and to link them with other industries, the Minister of Science, ICT and Future Planning may, each year, designate and support promising technologies and services (including digital contents) for the convergence, etc. of information and communications technology, as prescribed by Presidential Decree.
>
> (2) Where the Minister of Science, ICT and Future Planning makes designation pursuant to paragraph (1), he/she shall publicly notify such designation; and the methods for designation and the scope and details of support shall be prescribed by Presidential Decree.
>
> (3) In order to construct foundations for the vitalization of promising technologies and services, etc. for the convergence, etc. of information and communications technology designated pursuant to paragraph (1), the Minister of Science, ICT and Future Planning may support the vitalization of cooperation among central administrative agencies, public institutions, enterprises, universities, and research institutes.

Article 15 formed legal basis for the Minister of the Ministry of Science, ICT, and Future Planning to designate and support promising

47) (7) The State and each local government shall, in principle, allow new technologies and services for the convergence, etc. of information and communications technology insofar as relevant statutes are not violated, and make active efforts to vitalize such matters.

technology and service to activate and collaborate with other industries, and the Minister also may perform investigation and conduct R&D projects for standardization of technology and service, as allowed in Article 16.

Article 16 (Standardization of Technologies, Services, etc.)

(1) In order to promote information and communications technology and to vitalize the convergence thereof, the Minister of Science, ICT and Future Planning may implement the following projects concerning the standardization of technologies, services, etc. for the convergence, etc. of information and communications technology:

1. Establishment, amendment, repeal, and dissemination of standards concerning new technologies, services, etc. for the convergence, etc. of information and communications technology: *Provided*, That where a Korean industrial standard thereof is established pursuant to the Industrial Standardization Act, such standard shall govern;
2. Inspection, research and development of domestic and foreign standards concerning new technologies, services, etc. for the convergence, etc. of information and communications technology;
3. Other matters necessary for the standardization of new technologies, services, etc. for the convergence, etc. of information and communications technology.

(2) The Minister of Science, ICT and Future Planning may support projects for the standardization of technologies, services, etc. for the convergence, etc. of information and communications technology promoted by the private sector.

(3) The Minister of Science, ICT and Future Planning may designate institutions specialized in conducting projects for the standardization of technologies, services, etc. for the convergence, etc. of information and communications technology, and fully or partially subsidize them the necessary expenses.

(4) Matters necessary for the projects under paragraph (1) and the designation,

etc. of specialized institutions under paragraph (3) shall be prescribed by Presidential Decree.

Article 17 vested the Minister with the right to set the industry standards for technology and also to license the same.

Article 17 (Quality Certification of Technologies, Services, etc.)

(1) The Minister of Science, ICT and Future Planning may determine and publicly notify the standards for certification (hereinafter referred to as "quality standards") concerning the convenience, stability, reliability, expandability, etc. of technologies, services, etc. for the convergence, etc. of information and communications technology.

(2) The Minister of Science, ICT and Future Planning may certify whether the quality of technologies, services, etc. for the convergence, etc. of information and communications technology complies with the quality standards publicly notified pursuant to paragraph (1). In such cases, expenses incurred for certification shall be borne by applicants.

(3) In order to efficiently implement certification duties under paragraph (2), the Minister of Science, ICT and Future Planning may designate certification organizations.

(4) Persons who obtain certification pursuant to paragraph (2) may indicate or publicize the contents of certification, as prescribed by Presidential Decree. No person who fail to obtain certification shall indicate a certification mark or similar thereto.

(5) Where certification under paragraph (2) falls under any of the following subparagraphs, the Minister of Science, ICT and Future Planning shall revoke the certification:

1. Where certification is obtained by deceit or other wrongful means;
2. Where it fails to meet quality standards;
3. Where this Act or orders issued under this Act are violated.

(6) An insurance company under subparagraph 6 of Article 2 of the

Insurance Business Act may guarantee compensation for damage suffered by users due to certification under paragraph (2), as prescribed by Presidential Decree.

(7) Matters necessary for procedures for certification under paragraph (2), revocation of certification under paragraph (5), etc. shall be prescribed by Presidential Decree.

Support for R&D projects for small and mid-sized enterprises are specified in Article 18, and commercialization of technology and services may be funded in accordance to Article 19.

Article 18 (Support for Research and Development of Small and Medium Enterprises, etc.)

(1) In implementing a research and development project concerning information and communications technology prescribed by this Act, the Minister of Science, ICT and Future Planning shall preferentially use above the rate prescribed by Presidential Decree, out of the budget of the relevant project, for small and medium enterprises and venture businesses.

(2) The Minister of Science, ICT and Future Planning shall endeavor to vitalize investment in and financing for the intellectual property rights of small and medium enterprises and venture businesses.

(3) Matters necessary for the procedures, methods, etc. for implementation under paragraphs (1) and (2) shall be prescribed by Presidential Decree.

The Minister may encourage and vitalize public procurement of information and communications convergence technology and services as provided in Article 20.

Article 20 (Vitalization of Public Purchase of Technologies and Services for Convergence, etc. of Information and Communications)

> In order to create demand for technologies and services for the convergence, etc. of information and communications of which the quality is certified by the Minister of Science, ICT and Future Planning pursuant to Article 17, the Government shall take necessary supportive measures, such as preferential purchase thereof.

> Article 19 (Support for Commercialization of Promising Technologies, Services, etc. for Convergence, etc. of Information and Communications Technology)
> (1) The Minister of Science, ICT and Future Planning may provide necessary support for the commercialization of promising technologies, services, etc. for the convergence, etc. of information and communications technology publicly announced by the Minister of Science, ICT and Future Planning pursuant to Article 15.
> (2) The Minister of Science, ICT and Future Planning may collect a price for the use, transfer, lease, or export of the results of projects from a person who makes success in commercialization after receiving support under paragraph (1).
> (3) Matters necessary for support and the collection, management, etc. of money under paragraphs (1) and (2) shall be prescribed by Presidential Decree.

Also based on Article 30, the ministry of Science, ICT, and Future Planning is vested of the right to support small and medium sized start-ups with their founding the enterprises and also with expanding their businesses to overseas.

> Article 30 (Establishment of Small and Medium Enterprises, Venture Businesses, etc., Entry into Overseas Markets, etc.)
> (1) In order to vitalize and support the establishment of small and medium enterprises, venture businesses, etc. related to the convergence, etc. of information and communications technology, the Minister of Science, ICT

and Future Planning may implement the following projects:

1. Support for the establishment of small and medium enterprises, venture businesses, etc. relating to the convergence, etc. of information and communications technology in Korea and abroad, and for entry into overseas markets;
2. Supply of work space and conference halls to small and medium enterprises, venture businesses, etc. relating to the convergence, etc. of information and communications technology;
3. Supply of information on financing, human resources, markets, etc., and support therefor to small and medium enterprises, venture businesses, etc. relating to the convergence, etc. of information and communications technology;
4. Consultation on laws, management, tax, etc. for small and medium enterprises, venture businesses, etc. relating to the convergence, etc. of information and communications technology;
5. Overseas publicity of technologies developed by small and medium enterprises, venture businesses, etc. relating to the convergence, etc. of information and communications technology, supply of information on purchasers, and referral and brokerage of sale;
6. Support for translation services and legal services for the easy entry into overseas markets by small and medium enterprises, venture businesses, etc. relating to the convergence, etc. of information and communications technology;
7. Supply of information on overseas markets concerning the convergence, etc. of information and communications technology and support for the inducement of investment;
8. Building and operation of a base for entry into overseas markets by small and medium enterprises, venture businesses, etc. relating to the convergence, etc. of information and communications technology;
9. Exchange and cooperation with relevant institutions in Korea and abroad for the development of venture businesses relating to the convergence, etc. of information and communications technology;

10. Other projects necessary for the vitalization and support of business startups and entry into overseas markets.

(2) In order to efficiently implement projects listed in paragraph (1), the Minister of Science, ICT and Future Planning may designate and operate institutions or organizations prescribed by Presidential Decree as specialized institutions, and fully or partially subsidize them the necessary expenses.

In relation with the full support, fast introduction and commercialization of technology and service, the most significant feature of this 『Special Act on ICT』 may well be addressed as the 'Prompt Handling' and the 'Temporary Permission' as provided in Articles 36 and 37, respectively.

Article 36 (Prompt Handling of New Technologies and Services for Convergence, etc. of Information and Communications)

(1) Where a person who develops new technologies and services for the convergence, etc. of information and communications fails to obtain permission, approval, registration, authentication, verification, etc. (hereinafter referred to as "permission, etc.") under statutes due to any of the following causes, or whether he/she needs permission, etc. is not clear, he/she may file with the Minister of Science, ICT and Future Planning an application for prompt handling of the new technologies and services for the convergence, etc. of information and communications, as prescribed by Presidential Decree:

1. Where standards, specifications, requirements, etc. compatible with new technologies and services for the convergence, etc. of information and communications are not prescribed by statutes being the grounds for permission, etc.;
2. Where applying the standards, specifications, requirements, etc. under statutes being the grounds for permission, etc. to the relevant new technologies and services for the convergence, etc. of information and communications is not appropriate.

(2) Where the Minister of Science, ICT and Future Planning receives an application under paragraph (1), he/she shall notify the head of a relevant central administrative agency of the fact that an application for permission, etc. for new technologies and services for the convergence, etc. of information and communications is filed and of the details of the application.

(3) The head of the relevant central administrative agency shall reply to the Minister of Science, ICT and Future Planning whether the new technologies and services for the convergence, etc. of information and communications are under his/her jurisdiction or whether permission, etc. therefor are needed within 30 days from the date he/she receives notification under paragraph (2). Where he/she fails to make reply within 30 days, the duties shall be deemed not to fall under his/her jurisdiction or permission therefor of the head of the relevant central administrative agency shall be deemed unnecessary.

(4) The Minister of Science, ICT and Future Planning shall immediately notify the applicant of a reply under paragraph (3) (including whether permission, etc. pursuant to statutes under the jurisdiction of the Ministry of Science, ICT and Future Planning are necessary), or whether temporary permission, etc. under Article 37 (1) is needed, etc.

(5) Except for cases in which notification received from the Minister of Science, ICT and Future Planning pursuant to paragraph (4) states that permission, etc. of the Minister of Science, ICT and Future Planning or the head of the relevant central administrative agency are needed or that temporary permission under Article 37 (1) is needed, the relevant applicant may freely launch new technologies and services for the convergence, etc. of information and communications on the market.

(6) Where the head of the relevant central administrative agency deems that an application for new technologies and services for the convergence, etc. of information and communications under paragraph (1) is in need of permission, etc. under related statutes, he/she shall reply the conditions, procedures, etc. necessary for permission, etc.; and where the applicant

applies for permission, etc. according to the contents of the reply, he/she shall promptly handle it according to the related statutes.

(7) Except as otherwise provided for in paragraphs (1) through (6), matters necessary for prompt handling, etc. of new technologies and services for convergence, etc. of information and communications shall be prescribed by Presidential Decree.

Article 37 (Temporary Permission)

(1) Where the Minister of Science, ICT and Future Planning receives a reply that new technologies and services for the convergence, etc. of information and communications for which an application for prompt handling is filed pursuant to Article 36 (1) do not fall under the jurisdiction of the heads of other relevant central administrative agencies according to abovementioned Article or deems that they do not fall under the jurisdiction of the heads of other relevant central administrative agencies, and needs to establish proper or appropriate standards, specifications, requirements, etc. in consideration of the characteristics of the relevant new technologies and services for the convergence, etc. of information and communications, he/she may temporarily grant permission, etc. (hereinafter referred to as "temporary permission"). In such cases, the Minister of Science, ICT and Future Planning may attach necessary conditions for the stability, etc. of new technologies and services for the convergence, etc. of information and communications.

(2) The Minister of Science, ICT and Future Planning may conduct any test and inspection for temporary permission or designate an institution or organization having specialized human resources and technology as an institution for testing and inspection.

(3) The term of validity of temporary permission shall be up to one year, as prescribed by Presidential Decree. The term of validity may be extended one time only; a person who intends to have the term of validity extended shall file an application with the Minister of Science, ICT and Future Planning two months before the term of validity expires.

(4) In order to compensate for damage that the users of new technologies

and services for the convergence, etc. of information and communications may suffer if a person who intends to supply new technologies and services for the convergence, etc. of information and communications after obtaining temporary permission fails to supply such services, he/she shall, before supplying such services, take out guarantee insurance which names a person designated by the Minister of Science, ICT and Future Planning as the insured in an amount calculated according to the standard prescribed by Presidential Decree within the scope of total fees that he/she is to charge: *Provided*, That where the Minister of Science, ICT and Future Planning deems guarantee insurance is unnecessary in consideration of the characteristics of new technologies and services for the convergence, etc. of information and communications or the financial ability of the enterpriser, he/she may be allowed not to take out guarantee insurance.

(5) A person designated as the insured pursuant to paragraph (4) shall pay insurance claims which he/she receives according to the guarantee insurance to users who are not supplied with services after paying fees.

(6) A person who obtains temporary permission shall notify the users of the relevant new technologies and services for the convergence, etc. of information and communications of the temporary permission and the term of validity.

(7) The heads of relevant central administrative agencies who are influenced by temporary permission may submit their opinions to the Minister of Science, ICT and Future Planning.

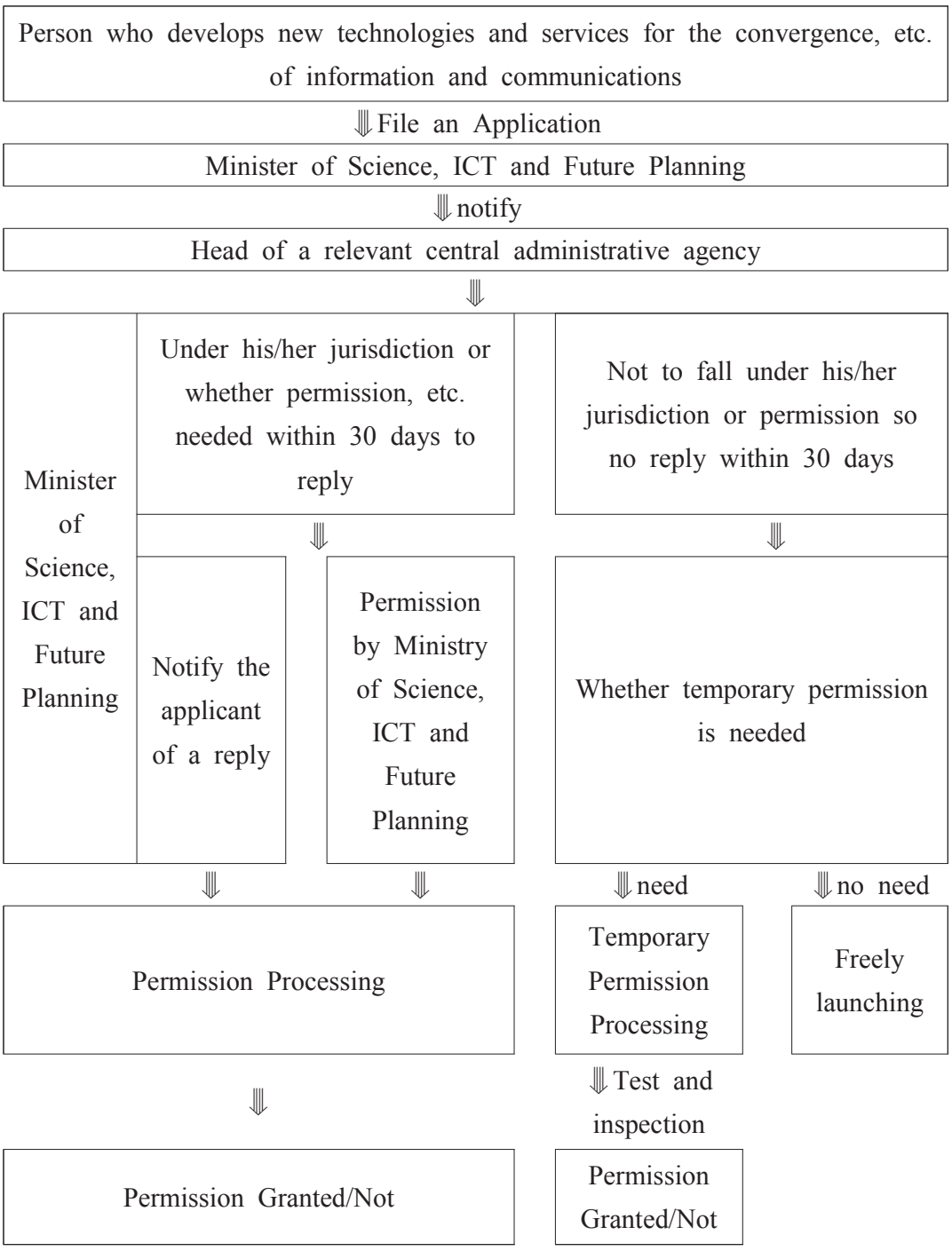
(8) Necessary matters, such as standards for examination of new technologies and services for the convergence, etc. of information and communications, and the procedures, methods, etc. therefor shall be prescribed by Presidential Decree.

Prompt Handling was devised for newly converged technologies and/or services as most often those new technologies and/or services, due to its newness, do not fit in under existing laws and regulations providing licenses and authorizations. Prompt Handling under Article 36 is designed

for such newly converged technologies and services, allowing them to be activated and be available for use, provided that the existing laws and regulations fail to cover them. Only in such case that no existing laws may regulate the new technologies and services the Prompt Handling may be requested.

Temporary Permission is what comes next to the Prompt Handling request. When the technology or service subjected is clearly not under any other government agency's umbrella and also a new set of standard, requirements, and tools are needed to be drawn to meet the needs for the new technology or service, in the effort to not to delay commercialization of the new technology or service further than necessary, a Temporary Permission is rendered. For a period set under the Presidential decree, not over a year, the Temporary Permission performs and enjoys the same legal effects as with the full-blown approval under any other law.

[Prompt Handling and Temporary Permission Process Flow Chart][48)]



48) Kyongo Chung, Implication of the Special Act on ICT and the Review of the Improvement Methods, pp. 75-76; Recited, Sei-Jin Kim, Yun-Jeong Kim, A Study on Legislation Regarding Invigoration of IT Convergence, p. 39

As much as this Prompt Handling and the Temporary Permission shed glamorous lights for those who develop newly converged technology and service that do not fit in under existing, old law, probably the most critical shortfall of this Prompt Handling and the Temporary Permission would be that the approval, although easier to obtain, is only provisional. It may be renewed for another year, but this Temporary Permission may not be renewed further. If no full-blown approval is obtained before the expiration of the Temporary Permission, or upon recession of the Temporary Permission as illegitimacy involved in the process was later revealed, who gets hurt the most is the consumers who have been using the technology or the service. As a protectional gear for those vulnerable consumers, Article 37(4) mandates the businesses obtaining Temporary Permission to get insured and pay premiums to cover damages for the consumers for the amounts that they pay as their user fees for the technology or service.

Article 37-4

(4) In order to compensate for damage that the users of new technologies and services for the convergence, etc. of information and communications may suffer if a person who intends to supply new technologies and services for the convergence, etc. of information and communications after obtaining temporary permission fails to supply such services, he/she shall, before supplying such services, take out guarantee insurance which names a person designated by the Minister of Science, ICT and Future Planning as the insured in an amount calculated according to the standard prescribed by Presidential Decree within the scope of total fees that he/she is to charge: *Provided*, That where the Minister of Science, ICT and Future Planning deems guarantee insurance is unnecessary in consideration of the characteristics of new technologies and services for the convergence, etc. of information and communications or the financial ability of the enterpriser, he/she may be allowed not to take out guarantee insurance.

However, such insurance only covers the amount that the consumers paid for the technology or service that failed to be provided. It is foreseeable that abrupt cease of technology or service would incur additional damage on the consumer's end, not to mention the fees that they paid, but no methods resolving such additional damage are built in on the Temporary Permission system.[49)]

3. 『Act on the Development of Cloud Computing and the Protection of Users』

(1) Background

For the most efficient use of the information communication resources through the information communications network, legal foundation for the policies were in need.[50)] It is expected that the cloud computing[51)] industry would show steep expanding on the business shares, especially in the mobile cloud arena. However, domestic players in the field still is behind in technology needed for the industry and the regulations on the business are rather strict that it may not provide the best business environment. Thus the 『Act on the Development of Cloud Computing

49) Jongkwan Lee, "Significance, Limits, and Improvements for ICT Promotion Special Act." Korea Legislation Research Institute, A Study on Legislation Regarding Invigoration of IT Convergence the 2nd Workshop Booklet; recited from Sei-Jin Kim, Yun-Jeong Kim, A Study on Legislation regarding Invigoration of IT Coinvergence, KLRI, 2013. p.44

50) Inyong Lee, Review reports on the Act on Cloud Computing Development and User Protection, Science, ICT, and Future Planning Broadcasting and Communications Committee, 2013.

51) Instead of saving information on each user's PC, cloud computing enables users to save their IT resources in the web network (in the "cloud") and make them available in may different venue such as software, platform, infrastructure. Users are required to pay for such 'cloud' space and service.

and the Protection of Users』 aims to reform regulations that hinders development of the cloud computing business, to provide legal foundation for promotion policies for the industry, and also to maintain a secured cloud computing service use to systematically and comprehensively grow the cloud computing business.

(2) Key Features

According to Article 5 of the 『Act on the Development of Cloud Computing and the Protection of Users』, the Minister of Ministry of Science, ICT, and Future Planning is required to set up a framework plan for promotion of development and use of cloud computing and for user protection in every three years, and such plan must be reviewed and ratified by the Telecommunication Strategy Committee in accordance with the Article 7 of the 『Special Act on ICT』.

> Article 5 (Formulation of Master Plans and Implementation Plans)
> (1) The Minister of Science, ICT and Future Planning shall collect plans, policies, etc. formulated by central administrative agencies related to the promotion of development and use of cloud computing and the protection of users (hereinafter referred to "relevant central administrative agencies"), formulate a master plan every three years (hereinafter referred to as "master plan"), and finalize the plan after deliberation by the Information Communications Strategy Committee under Article 7 of the Special Act on the Promotion of Information and Communications, the Invigoration of Convergence, etc.

It is interesting to note that the 『Act on the Development of Cloud Computing and the Protection of Users』 did not establish a separate committee. It rather allowed Telecommunication Strategy Committee to

review and ratify plans regarding cloud computing, as operated under the 『Special Act on ICT』, and this can be appreciated as a well-thought systematic structure as unifying the decision making body for related issues keeps the overall policy direction consistent and also it increases the effectiveness of the agencies.

Another important feature of the 『Act on the Development of Cloud Computing and the Protection of Users』 is that the government manifests its intention to utilize cloud computing to the fullest by placing cloud computing use as a priority in executing expenses and also in implementing the same in government offices, as noted on Article 12 and Article 20.

> Article 12 (Facilitation of Introduction of Cloud Computing to State Agencies and Other Public Authorities)
> (1) The State agencies and other public authorities shall endeavor to introduce cloud computing.
> (2) Where the Government formulates a budget necessary for the implementation of a policy or project for national informatization under the Framework Act on National Informatization, it shall give preference to the introduction of cloud computing.

> Article 20 (Facilitating Public Institutions' Use of Cloud Computing Services) The Government shall endeavor to encourage public institutions to use cloud computing services provided by cloud computing service providers for their work process.

As one of the symbolic new technology being legalized, cloud computing law draws attention and concerns regarding the level of user protection the law may provide. While the title of the law has protection of the users vividly listed almost as having comparable weight as the

cloud computing legalization itself, the violations of the duties and the fines attached to such violations seem minimal. Article 37 provides only less than ten million Korean Won for violations of service providers duties against users, such as duty to inform in case of breach in Article 19, duty to notify server location upon user's request in Article 20, and duty not to use or share user information without consent in Article 21.

> Article 37 (Administrative Fines)
>
> Any of the following persons shall be punished by an administrative fine not exceeding ten million won:
>
> 1. A person who fails to notify users of an intrusion, the leakage of user information, or the interruption of service, in violation of Article 25 (1);
> 2. A person who fails to notify the Minister of Science, ICT and Future Planning of the leakage of user information, in violation of Article 25 (2);
> 3. A person who fails to return or destroy user information, in violation of Article 27 (3) or (4);
> 4. A person who fails to comply with an order issued under Article 30 (5) to cease a violation or to take corrective measures.
>
> (2) The administrative fines under paragraph (1) shall be imposed and collected by the Minister of Science, ICT and Future Planning, as prescribed by Presidential Decree.

Those built-in protection measures are carefully crafted to meet the user protection standards that this law aims to achieve as shown on its title, the matching fines for violations of such duties fall far short.

Ⅳ. Conclusion

India has one major law (IT Act, amended) that governs all of the ICT related issues from the data protection and privacy issues to the banking and e-commerce regulations, even to the penalization methods built in. It may be a very effective way to have all related issues in one place so that one thing links to another and all are working for each other, matching. On the flip side, however, it may seem as a downfall as there may be areas where optimized attention and careful crafting of laws may be better to serve than having this current catch-all type one general law to cover all areas. Yet one cannot overlook the fact that the IT Act covers very up-to-date technologies and issues in one law including big data issues and cloud computing. It is highly appreciated that those two important and high-tech subjects were already included and covered in the 2008 IT Act, when other countries like Korea have separate laws enacted to regulate and promote the same as the issue sprang up through the time. Overall, the introduction and development of the ICT laws in India was driven by the strong and fast growth in IT industry and the international pressure and domestic need for protection of user rights and businesses.

It would be hard to say that laws and policies related to network and information technology in Korea for the last couple of years have been enacted and designed not for the expansion of freedom of expression or development of the communications tool; rather, the overall direction for the policies and laws were set towards utilizing creative force from the ICT industry for the economic gain, and it is very well conveyed in the recent dialogue on the regulatory reform on internet, especially in the

voices from the current administration.[52] On the contrary, proposed laws by the congress tends to reflect protective measures on the citizens' rights. Having those two very different directions shown on laws enacted and amended, it is only natural that the laws on ICT may lack systematic consistency. This statement by no means suggests that the one umbrella law like in India would better serve the needs in Korea. Korea and India are two different countries with distinctive business customs and developmental phases that one suit will not fit both perfectly. Considering the dynamics of the industry in Korean and the fast-phased developments in legal aspects reflecting the ever more speedy industrial development, it may make more sense that those specific and separate laws be drawn and enacted as per urgent needs arising. However, as mentioned previously, lack of consistency and the distractions in governing body would be the ever-present issues in this type of legislative history. A separate and independent tribunal for ICT issues as introduced in India's case may provide a solution, and inducing further creative, innovative, and effective idea would be the main task left for legislators to resolve the pressing circumstances.

52) Woomin Shim, "Current Legislative Status in Information Communications Law," Journalism and Law, Vol. 13, Issue 1, p.98, 2014

References

India

Abha Chauhan, Evolution and Development of Cyber Law: A Study with Special Reference to India

Aparna Vishwanathan, Cyber Law Indian & International Perspectives 25, Lexis Nexis Butterworths, Nagpur, 1st Edition 2012

Vakul Sharma, Information Technology Law & Practice 430, Universal Law Publishing Co. Ltd., New Delhi, 3rd edn., 2012

V. Rajaraman, Essentials of E-Commerce Technology 229, P.H.I. Learning Pvt. Ltd., New Delhi, 1st Edition, 2010

Karnika Seth, Computers, Internet and New Technology Laws, Lexis Nexis Butterworth 2012.

Gazzette of India

(deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf)

The Information Technology Act 2000

The Information Technolgy Amendment Act 2008

The Information Technology (Reasonalb Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

EU Directive 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995

Singapore Personel Data Protection Act 2012

UK Data Protection Act 1988

www.rajdeepandjoyeeta.com/internet-banking.html

Korea

Hyunkyung Kim, Next Administration's Informatization Governmence and its Legal Implication, Vol. 13 Issue 4 of Public Law Research, 2012

Sungmin Cha, Analysis on Current Domestic and International Status on the Communications Industry with the Outside Circumstances Change, Report for Korea Electronic Communications Institute, 2008

Ministry of Science, ICT, and Future Planning, 2014 Annual Report on Natioinal Informatization

Jongkwan Lee, Significance, Limits, and Improvements for ICT Promotion Special Act, Korea Legislation Research Institute, a Study on Legislation Regarding Invigoration of IT Convergence the 2nd Workshop Booklet; Recited from Sei-Jin Kim, Yun-Jeong Kim, A Study on Legislation Regarding Invigoration of IT Convergence

Inyong Lee, Review reports on the Act on the Development of Cloud Computing Development and the Protection of Users, Science, ICT, and Future Planning Broadcasting and Communications Committee, 2013

Kyongo Chung, Implication of the Special Act on ICT and the Review of the Improvement Methods, pp. 75-76; Recited, Sei-Jin Kim,

Yun-Jeong Kim, A Study on Legislation Regarding Invigoration of IT Convergence

Woomin Shim, Curent Legislative Status in Information Communications Law, Journalism and LAw, Vol. 13, Issue 1, 2014

Internet Multimedia Broadcast Services Act

Act on the Establishment and Operation of Korea Communications Commission

Telecommunications Act

Act on Computing Network Supply Exapnsion and Use Promotion

Electronic Government Act

Act on Protection of Information and Communications Infrastructure

Digital Signature Act

Internet Address Resources Act

Act on Development of E-Learning Industry and Promotion of Utilization of E-Learning

Act on Protection, Use, Etc. of Location Information

Game Industry Promotion Act

Internet Multimedia Broadcasting Services Act

Framework Act of the National Informatization

Act on Promotion of Information and Communications Network Utilization and Information Protection

Act on the Protection of Information and Communications Infrastructure

Personal Information Protection Act

Framework Act on Broadcasting Communications Development

Broadcasting Act

Electronic Communications Buysiness Act

Act on Promotion for Information Communications Industry

Special Act on Promotion of Information and Communication Technology, Vitalization of Convergence Thereof, Etc.

Act on the Development of Cloud Computing Development and the Protection of Users