Asian Journal of Innovation and Policy (2020) 9.3:339-359
DOI: http//dx.doi.org/10.7545/ajip.2020.9.3.339

Keywords Analysis on the Personal Information Protection Act: Focusing on South Korea, the European Union and the United States*

Sung-Uk Park, Moon-Soo Park***, Soo-Hyun Park****, Young-Mi Yun*****

Abstract The policy change in the Data 3 Act is one of the issues that should be noted at a time when non-face-to-face business strategies become important after COVID-19. The Data 3 Act was implemented in South Korea on August 5, 2020, calling 'Big Data 3 Act' and 'Data Economy 3 Act,' and so personal information that was not able to identify a particular individual could be utilized without the consent of the individual. With the implementation of the Data 3 Act, it is possible to establish a fair economic ecosystem by ensuring fair access to data and various uses. In this paper, the law on the protection of personal information, which is the core of the Data 3 Act, was compared around Korea, the European Union and the United States, and the implications were derived through network analysis of keywords.

Keywords Personal Information Protection Act, GDPR, CCPA, Keyword Analysis, Network Analysis

I. Introduction

In the era of the 4th industrial revolution and the data economy, fostering new industries through active use of data has emerged as a national task. In particular, it is necessary to use new technologies such as artificial intelligence, internet-based integration of information and communication resources (cloud), and the Internet of Things, while establishing social norms for safe use of data was also urgently needed. Thus, a revision to the Data 3 Act was proposed on November

Submitted, November 17, 2020; 1st Revised, December 15, 2020; Accepted, December 23, 2020
* This research was supported by the research fund of Hanbat National Universtiy in 2020
** Assistant Professor, Hanbat National University, Daejeon, Korea; supark@hanbat.ac.kr
*** Principal Researcher, Korea Institute of Industrial Technology, Chuncheongnamdo, Korea; mspark@kitech.re.kr
**** Ph.D. Student, University of Science and Technology, Daejeon, Korea; shp@ust.ac.kr
***** Corresponding Author, M.S Student, University of Science and Technology, Daejeon, Korea; youngsim@ust.ac.kr

15, 2018, to solve two problems: regulatory innovation on data use and the personal information protection cooperative system's readjustment.

The Data 3 Act collectively refers to three laws: the Personal Information Protection Act, the Information and Communications Network Utilization Promotion and Information Protection Act (abbreviated as the Information and Communication Network Act), and the Credit Information Utilization and Protection Act (abbreviated as the Credit Information Act).

Under the auspices of the Presidential Committee on the Fourth Industrial Revolution, the legal revision bill reflects the results of the "Hackerton" meeting agreement (February, April 2018) involving experts from various fields, including related ministries, civic groups, industry and legal circles, and the special recommendation of the National Assembly's "Special Committee on the Fourth Industrial Revolution"(May 2018). This was prepared through various procedures for gathering opinions from civic groups, industries, legal circles, and academia. Then, it passed the plenary session of the National Assembly on January 9, 2020, and finally, the revision of the Data 3 Act was implemented on August 5, 2020, signaling the beginning of the revitalization of the data economy.

The Data 3 Act allows the processing of aliased personal information for statistical research and public interest record preservation purposes, combining alias information between different fields to expand data utilization scope.

In this paper, the Korean, European, and American laws related to the Personal Information Protection Act were analyzed through network analysis to analyze the frequency of keywords in each law and each network group's keywords. Through this, we would like to draw implications for the Personal Information Protection Act in each country.

II. Theoretical Backgrounds

The development of information and communication technology greatly improves the storage and processing capacity of data, and various technologies are developing that process a lot of data and deliver the necessary information.

To grasp trends or issues, research is done to search web documents and derive issues through association network analysis. The method of identifying characteristics or topics in the field by simply identifying the frequency of keywords can have a simple and meaningful implication. Network analysis represents the relationship between individuals and groups as nodes and links and is a methodology for analyzing the phase structure, diffusion and evolution process through this.

Keyword network analysis can identify the frequency of simultaneous emergence between keywords within the same document at some point in time

to determine the degree of association between keywords in a timely manner to analyze the keywords that become an issue (Park, et al., 2018, Freeman, L.C., 1979, Choe, et al., 2013).

The network is one of the ways in which various types of systems are structurally represented by humans or objects (Lee, 2012, Jasjit,2005). That is, it is a way to model various systems by expressing things or core words as nodes and internode connections as links. These modeled networks can analyze and understand various characteristics in scientific ways. Keyword network analysis is a technique that deduces the meaning by analyzing the simultaneous appearance relationship of words in the document text.

Yang Hyun-chae (2017) conducted a keyword network analysis under the theme "The Present and Future of the Fourth Industrial Revolution." This study analyzed the relevance of the 4th Industrial Revolution, which has been socially discussed and became an issue but has remained in the general discourse among Internet users through a keyword network. Cho Sung-hwan (2018) conducted a keyword analysis under the theme of "Study on Blockchain Trend Analysis Using Keyword Network Analysis Method," and compared and analyzed articles referring to 'financial,' 'energy,' and 'logistics' mentioned in media and government announcements in the field of industrial utilization of the blockchain using text mining and semantic network analysis methods used for keyword network analysis. Park Sung-uk (2019) conducted a keyword analysis under the theme of "Analysis of Keywords of Data Technology Using Big Data Techniques," and derived that "Big Data," "O2O," "Artificial Intelligence," "Internet of Things" and "Cloud Computing" are related to Data Technology.

III. Analysis target

Among the 3 data laws, keyword network analysis was performed on the personal information protection laws of Europe and the United States, which are benchmarked in Korea in relation to the personal information protection laws, to derive and cluster keywords by frequency. Through keyword network analysis, it is possible to analyze the topics that become issues by identifying the frequency of simultaneous occurrence of keywords in each country's personal information protection law and determining the strength of the connection between specific keywords.

Korea's Personal Information Protection Act (PIPA), Europe's General Data Protection Regulation (GDPR), and the United States' California Consumer Privacy Act (CCPA) were analyzed based on the original texts. The analysis was conducted by dividing into data collection, pre-processing, and keyword network analysis of data in each text.

In addition, keyword analysis was analyzed using KnowledgeMatrix plus, NodeXL and VOSviewer, which are software programs mainly used for network analysis and keyword analysis.

1. PIPA of South Korea

Korea's Personal Information Protection Act aims to increase the utilization of data through the introduction of pseudonym information. Therefore, the concept of pseudonym information that is safely processed so that individuals cannot be recognized was introduced. In addition, pseudonym information was allowed to be processed without the consent of the data subject for statistical purposes, scientific research, and record preservation for the public interest. In addition, additional use and the provision of personal information are permitted within the scope reasonably related to the purpose of collection set by the President. Among personal information, the scope of personal information is clarified by establishing a standard for determining information that can be easily combined with other information to recognize a specific individual.

As a result of keyword frequency analysis, information was 745 times, personal 598 times, protection 209 times, data 180 times, and commission 160 times.

Table 1 Frequency table of keywords – PIPA (S.Korea)

Keyword	freq	Keyword	Freq	Keyword	freq	Keyword	freq
INFORMATION	745	COMMUNICATIONS	64	PROVIDER	37	RESPECT	26
PERSONAL	598	NEWLY	61	USE	37	APPLICABLE	25
PROTECTION	209	INSERTED	59	STATUTES	36	BUSINESS	25
DATA	180	REQUEST	54	DEEMED	35	DUTIES	25
COMMISSION	160	PARTY	49	PERIOD	33	PROCESSED	25
CONTROLLER	146	RELATED	49	CHAIRPERSON	32	REGISTRATION	25
PURSUANT	128	COMMITTEE	48	DATE	32	CERTIFICATION	24
NECESSARY	121	PROVISIONS	48	SAME	31	MEMBERS	24
MATTERS	115	APPLY	47	ACCESS	30	POLICY	24
PERSON	109	FORCE	46	FEBRUARY	30	SURCHARGES	24
SUBJECT	109	CASE	45	HEREINAFTER	30	INSTITUTIONS	23
PROCESSING	108	PRIVACY	45	NOTIFY	30	LEGAL	23
PRESCRIBED	104	SERVICE	45	ENTERS	29	USERS	23
PRESIDENTIAL	100	REFERRED	43	PERSONS	29	NOTIFICATION	22
DECREE	99	CONCERNING	42	RELATION	29	RIGHTS	22

MEDIATION	99	RELEVANT	42	APPLICATION	28	TIME	22
AMENDED	97	SUBJECTS	42	INDIVIDUAL	28	COLLECTION	21
PROVIDED	92	CENTRAL	41	PENALTY	28	MATERIALS	21
VIOLATION	89	FAILS	41	PROVIDE	28	OBTAIN	21
ADMINISTRATIVE	87	INSTITUTION	41	FILES	27	SPECIAL	21
MEASURES	81	PURPOSE	41	PURPOSES	27	ENSURE	20
PUBLIC	81	HEAD	40	SAFETY	27	METHOD	20
CONSENT	78	NATIONAL	40	COLLECTED	26	PARTIES	20
DISPUTE	75	AGENCY	39	DAMAGE	26	REGULATIONS	20
CASES	70	COURT	37	PROVISION	26	RESIDENT	20

After checking with the network program NodeXL, it can be seen that colors are divided into seven groups.

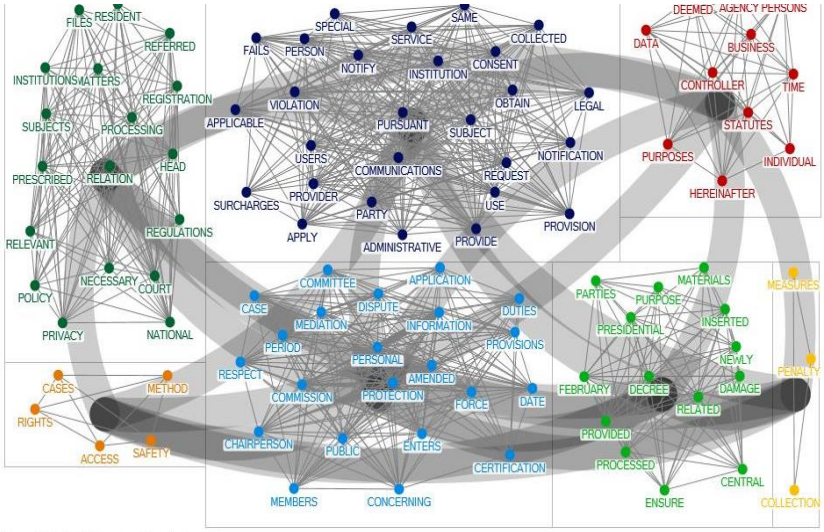

Figure 1 Keyword Network NodeXL Figures – PIPA (S.Korea)

Through VosViewer, it can be confirmed that the relationship between groups is being established based on information.

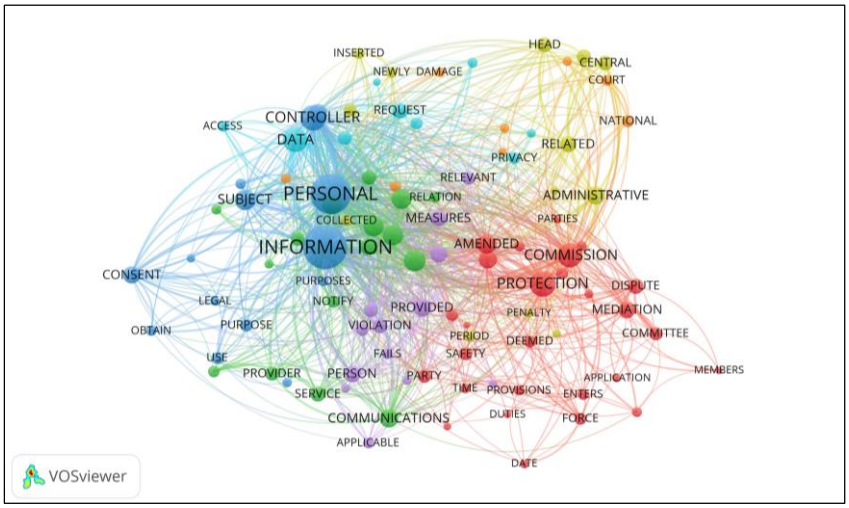

Figure 2 Keyword Network Vosviewer Figures – PIPA (S.Korea)

Finally, analyzing keywords by a network group of the Personal Information Protection Act shows that they are grouped into seven categories: 'COMMISSION,' 'COMMUNICATION,' 'INFORMATION,' 'ADMINISTRATION,' 'PERSON,' 'DATA,' and 'REGULATIONS.'

Table 2 Keywords by Network Group – PIPA (Korea)

Group	Keyword
COMMISSION	COMMISSION, PROTECTION, AMENDED, PUBLIC, PARTY, CASE, DEEMED, STATUTES, INSTITUTIONS, PROVISIONS, SAFETY, TIME, RESPECT, MEDIATION, DISPUTE, PERSONS, COMMITTEE, ENTERS, FORCE, APPLICATION, DUTIES, PARTIES, DATE, SPECIAL, CHAIRPERSON, CERTIFICATION, MEMBERS
COMMUNICATIONS	DECREE, PRESCRIBED, PRESIDENTIAL, NECESSARY, PURSUANT, MATTERS, COMMUNICATIONS, REFERRED, HEREINAFTER, SERVICE, RELATION, NOTIFY, PROVIDER, METHOD, USERS, NOTIFICATION
INFORMATION	INFORMATION, PERSONAL, CONTROLLER, SUBJECT, PROCESSING, USE, PURPOSES, CONSENT, PROCESSED, PURPOSE, PROVISION, LEGAL, COLLECTION, OBTAIN
ADMINISTRATIVE	ADMINISTRATIVE, RELATED, COLLECTED, FEBRUARY, HEAD, NEWLY, INSERTED, CENTRAL,

	PERIOD, AGENCY, MATERIALS, PENALTY, SURCHARGES
PERSON	CASES, PROVIDED, PERSON, MEASURES, APPLY, SAME, VIOLATION, RELEVANT, FAILS, APPLICABLE, CONCERNING, BUSINESS, INDIVIDUAL
DATA	DATA, REQUEST, INSTITUTION, SUBJECTS, PRIVACY, ACCESS, FILES, POLICY, RIGHTS
REGULATIONS	PROVIDE, ENSURE, REGISTRATION, NATIONAL, COURT, DAMAGE, RESIDENT, REGULATIONS

2. GDPR of the European Union

In May 2016, the European Union issued GDPR to ensure the free movement of personal information among EU members in the single digital market while strengthening the right of information subjects to protect personal information. The principles of personal information processing in GDPR are as follows: First, the principle of legality, fairness and transparency; second, the principle of purpose restriction; third, the principle of personal information processing; fourth, the principle of accuracy; fifth, the principle of storage period restriction; sixth, the principle of integrity and confidentiality; and finally the principle of accountability.

GDPR defines "personal information" as all information relating to the identified or identifiable natural person (information subject). In this case, the identifiable natural person can be identified, either directly or indirectly, by reference to identifiers, such as names, identification numbers, location information, online identifiers, or by referring to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, and social identity of the natural person.

GDPR is characterized by the fact that the type of information for evaluating identification is classified into identifiers and identity. Online identifier, one of the identifiers, is widely interpreted as the information that can track or link a specific individual online even if the subject of the information is unknown. GDPR Recital explains that "online identifier" refers to information provided by devices, applications, tools, protocols, etc., such as IP address, cookie ID, and RFID tag. In addition to IP addresses, cookie IDs, and RFID tags, the EU Commission recognizes mobile phone advertisement IDs as online identifiers.

In addition, the EU Commission also recognizes all names, home addresses, e-mail addresses (name.surname@company.com), identification numbers, location information, and symbols uniquely assigned by hospitals or doctors to identify patients as personal information. On the other hand, the business registration number, the company's representative e-mail address (info

@company.com), and anonymous information are not recognized as personal information.

As a result of the GDPR keyword frequency analysis, data was 608 times, PROCESSING 295 times, SUPERVISORY 294 times, PERSONAL 260 times, and CONTROLLER 254 times in that order.

Table 3 Frequency table of keywords - GDPR (EU)

Keyword	freq	Keyword	freq	Keyword	freq	Keyword	freq
DATA	608	PARTICULAR	67	APPLICABLE	39	CONSENT	30
PROCESSING	295	MEANS	66	CASE	38	BASIS	30
SUPERVISORY	294	NECESSARY	64	PERSON	36	OBLIGATIONS	29
PERSONAL	260	CERTIFICATION	62	ORDER	36	INTERESTS	29
CONTROLLER	254	OUT	61	APPLY	36	DELAY	29
AUTHORITY	241	COMPETENT	60	ACCOUNT	36	CONDITIONS	29
SUBJECT	195	RULES	59	TRANSFER	34	PREJUDICE	28
MEMBER	177	PROVIDE	56	STATES	34	ESTABLISHED	28
PROTECTION	149	INTERNATIONAL	54	PERSONS	34	COMPLAINT	28
STATE	136	NATURAL	53	OPINION	34	CODE	28
REGULATION	117	PROVIDED	50	OPERATIONS	33	OFFICER	27
UNION	96	REQUEST	49	COMPLIANCE	33	APPLICATION	27
INFORMATION	96	LEGAL	49	PROCESSORS	32	ADOPT	27
BOARD	96	POINT	48	PERIOD	32	ADMINISTRATIVE	27
LAW	93	SAFEGUARDS	45	DRAFT	32	ACTIVITIES	27
RIGHTS	89	COUNTRY	45	CONDUCT	32	REQUIREMENTS	26
PURPOSES	89	CONCERNED	45	CATEGORIES	32	PROCEDURE	26
PUBLIC	87	TASKS	44	BODIES	32	INFORM	26
AUTHORITIES	86	BODY	44	PURPOSE	31	EUROPEAN	26
ACCORDANCE	84	BINDING	44	PROVISIONS	31	CARRIED	26
SUBJECTS	78	SPECIFIC	43	POWERS	31	PROCESSED	25
DECISION	77	CONTROLLERS	43	PERFORMANCE	31	JOINT	25
MEASURES	74	EXERCISE	41	INTEREST	31	ASSESSMENT	25
COMMISSION	74	ORGANISATION	40	ESTABLISHMENT	31	TRANSFERS	24
APPROPRIATE	73	FREEDOMS	40	ADOPTED	31	EFFECTIVE	24
RIGHT	68	ENSURE	40	MEMBERS	30	APPROVED	24

After checking with the network program NodeXL, it can be seen that colors are divided into two groups.

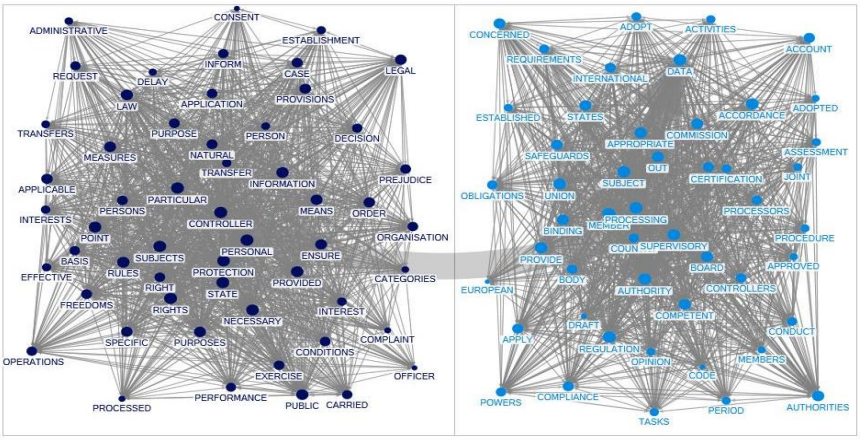

Figure 3 Keyword Network NodeXL Figures - GDPR (EU)

In addition, after analyzing with VOSviewer, it is possible to check the relationship between groups based on DATA.

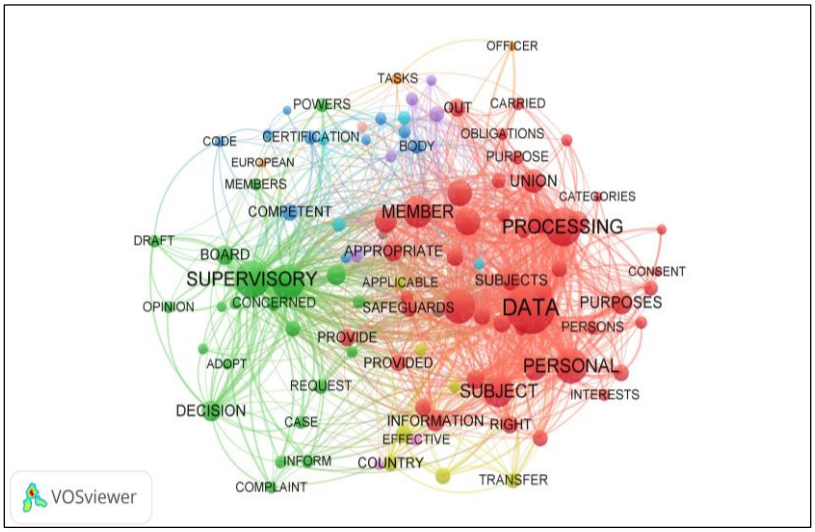

Figure 4 Keyword Network Vosviewer Figures – GDPR (EU)

Keywords by GDPR network group show that there are a total of six groups: 'DATA,' 'SUPERVISORY,' 'CONDUCT,' 'ORGANISATION,' 'PROCESSORS' and 'OPERATIONS.'

Table 4 Keywords by Network Group - GDPR (EU)

Group	Keyword
DATA	DATA, PROCESSING, PERSONAL, CONTROLLER, SUBJECT, MEMBER, STATE, PROTECTION, LAW, RIGHTS, REGULATION, UNION, PURPOSES, PUBLIC, INFORMATION, APPROPRIATE, SUBJECTS, MEASURES, NECESSARY, PARTICULAR, RULES, OUT, RIGHT, MEANS, LEGAL, PROVIDE, SAFEGUARDS, SPECIFIC, PROVIDED, NATURAL, FREEDOMS, ENSURE, EXERCISE, INTEREST, PERSONS, BASIS, POINT, PURPOSE, PERSON, CARRIED, OBLIGATIONS, PERFORMANCE, INTERESTS, CONDITIONS, PROCESSED, CATEGORIES, CONSENT
SUPERVISORY	SUPERVISORY, AUTHORITY, DECISION, AUTHORITIES, ACCORDANCE, BOARD, COMMISSION, CONCERNED, REQUEST, POWERS, INFORM, ACCOUNT, CASE, DELAY, DRAFT, OPINION, COMPLAINT, MEMBERS, ESTABLISHMENT, PERIOD, ADOPT, ADOPTED, PROCEDURE
CONDUCT	COMPETENT, CERTIFICATION, BODY, BODIES, COMPLIANCE, CONDUCT, PREJUDICE, CODE, REQUIREMENTS, APPROVED
ORGANISATION	INTERNATIONAL, COUNTRY, ORGANISATION, TRANSFER, APPLICABLE, PROVISIONS, TRANSFERS
PROCESSORS	CONTROLLERS, BINDING, PROCESSORS, APPLY, ESTABLISHED
OPERATIONS	STATES, OPERATIONS, JOINT, ASSESSMENT

3. CCPA of the United States

CCPA in the United States was enacted as a state law of California, not a federal law, and went into effect on January 1, 2020. CCPA is the latest law in California that serves as a general law on private-sector privacy and reflects recent technological developments such as big data, profiling, and artificial intelligence (AI), with very specific and modern definitions of the concept and scope of personal information. CCPA defines "personal information" as information that, directly or indirectly, identifies, describes, relates, or can be reasonably associated or linked. This applies in principle to services that provide services to Californians. The CCPA personal information processing principles are as follows. First, when collecting personal information, it is obligatory to notify and disclose. Second, it is obligatory to notify and disclose personal information when selling and disclosing personal information. Third, it is

obligatory to establish and disclose online personal information processing policies. Finally, we follow the OPT-OUT method of handling personal information.

CCPA also has a separate definition for "unique identifiers" that are most commonly used in online environments. "Unique identifier or unique personal identifier" means a continuous identifier that can be used to recognize a device connected to a consumer, family, consumer, or family over a variety of services despite the passage of time. This includes a device identifier, an Internet Protocol (IP) address, cookies, beacons, pixel tags, mobile advertising ID, and similar technologies, customer numbers, unique nicknames, phone numbers, phone numbers, other forms of permanent or probabilistic identifiers that can be used to identify a particular consumer or device. In this legislation, "probabilistic identifiers" mean identifying consumers or terminals with a degree of "probability," not based on the information listed in the definition of personal information or similar types of personal information. However, information that is publicly available and de-identified consumer information or aggregated consumer information is not included in personal information. "Publicly Available Information" means only information that is lawfully available in federal, state, or local government records. For example, biometric information collected by a business operator about a consumer without the consumer's knowledge is not included in publicly available information. "De-identified information" means information that cannot reasonably identify a particular consumer, cannot be related, cannot be described, cannot be directly or indirectly associated or linked. In this case, the business operator using the de-identified information must take the following measures (1798.140.(h)). First, implement technical safeguards to prohibit re-identification of consumers related to the information. Second, implement a business process that specifically prohibits re-identification of the information. Third, implement a business process to prevent accidental disclosure of non-identifying information. Finally, no attempt will be made to re-identify the information. In addition, CCPA also defines pseudonymization measures. For example, "Pseudonymize or Pseudonymization" means processing personal information in a way that can no longer be attributable to specific consumers without using additional information. In this case, additional information should be stored separately, and technical and administrative measures should be taken to ensure that personal information is not attributed to the identified or identifiable consumer.

As a result of keyword frequency analysis, information 305 times, CONSUMER 271 times, BUSINESS 228 times, PERSONAL 192 times, and SECTION 92 times were derived in this order.

Table 5 Frequency table of keywords – CCPA (U.S.)

Keyword	freq	Keyword	freq	Keyword	freq	Keyword	freq
INFORMATION	305	APPLY	19	ACTION	14	SUBJECT	11
CONSUMER	271	CODE	19	COMMERCIAL	14	TIME	11
BUSINESS	228	SOLD	19	LAW	14	UNITED	11
PERSONAL	192	GENERAL	18	PROVIDING	14	COLLECTION	10
SECTION	92	PROVIDER	18	AVAILABLE	13	COLLECTS	10
PURSUANT	58	DISCLOSED	17	COMPLY	13	ENUMERATED	10
CONSUMERS	52	LIMITED	17	DATA	13	IDENTIFIER	10
SUBDIVISION	52	REASONABLY	17	EXERCISE	13	INDIVIDUAL	10
COLLECTED	47	REQUIRED	17	OPERATIVE	13	MEDICAL	10
MEANS	46	SELL	17	VEHICLE	13	NOTICE	10
REQUEST	43	USE	17	DEVICE	12	PARTIES	10
PERSON	39	CATEGORY	16	ENTITY	12	REQUESTS	10
CATEGORIES	37	HEALTH	16	MANNER	12	SHARES	10
PURPOSES	37	INTERNET	16	REGULATIONS	12	SOLELY	10
PURPOSE	32	PARTY	16	VIOLATION	12	ADDRESS	9
PRIVACY	27	RIGHTS	16	ADDITIONAL	11	BEHALF	9
PROVIDED	27	SECTIONS	16	CONTRACT	11	COMPANY	9
SERVICE	26	STATE	16	DEFINED	11	GOODS	9
SERVICES	24	USED	16	FINANCIAL	11	OFFICER	9
CALIFORNIA	23	ATTORNEY	15	IDENTIFY	11	OWNER	9
EFFECTIVE	23	FEDERAL	15	NECESSARY	11	POLICY	9
RIGHT	21	OPTOUT	15	NUMBER	11	PUBLIC	9
SALE	21	PROVIDE	15	RESEARCH	11	RECEIVING	9
DISCLOSE	20	VERIFIABLE	15	SECURITY	11	USES	9
NATURAL	20	ACCOUNT	14	STATES	11		

After checking with the network program NodeXL, it can be seen that colors are divided into two groups.

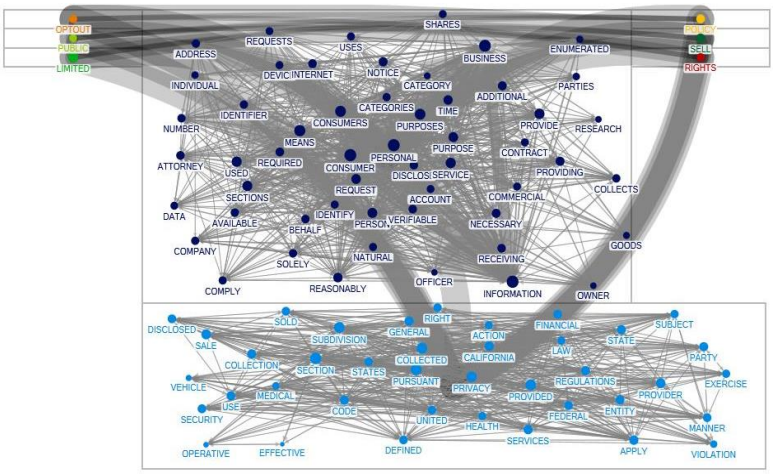

Figure 5 Keyword Network NodeXL Figures – CCPA (U.S.)

This is the result of checking the relationship between groups through colors centered on INFORMATION and CONSUMER through VOSviewer.

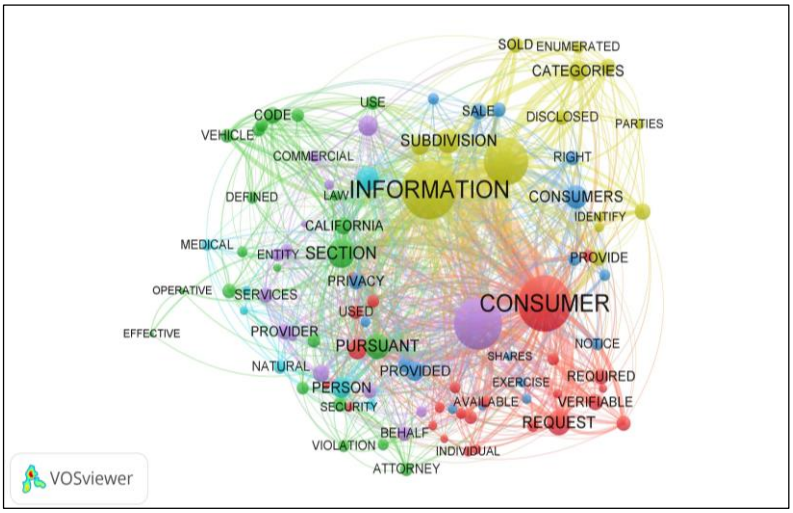

Figure 6 Keyword Network Vosviewer Figures – CCPA (U.S.)

Keywords by CCPA network group show that they consist of a total of six groups: 'CONSUMER,' 'REGULATIONS,' 'RIGHT,' 'INFORMATION,' 'BUSINESS' and 'PERSON.'

Table 6 Keywords by Network Group – CCPA (U.S.)

Group	Keyword
CONSUMER	CONSUMER, REQUEST, MEANS, VERIFIABLE, REQUIRED, ACCOUNT, USED, REASONABLY, LIMITED, TIME, INTERNET, ADDITIONAL, AVAILABLE, DEVICE, IDENTIFIER, NECESSARY, INDIVIDUAL, NUMBER, ADDRESS, SECURITY, PUBLIC, REQUESTS, DATA, RESEARCH, COMPLY
REGULATIONS	SECTION, PURSUANT, CALIFORNIA, CODE, GENERAL, HEALTH, VEHICLE, USE, APPLY, ATTORNEY, STATES, UNITED, REGULATIONS, STATE, DEFINED, VIOLATION, ACTION, FEDERAL, LAW, SUBJECT, OPERATIVE, EFFECTIVE
RIGHT	CONSUMERS, PROVIDED, SALE, PRIVACY, SELL, SECTIONS, RIGHT, NOTICE, PARTY, COLLECTION, OPTOUT, MANNER, POLICY, USES, RIGHTS, EXERCISE, SHARES
INFORMATION	INFORMATION, PERSONAL, SUBDIVISION, CATEGORIES, PURPOSES, DISCLOSE, PROVIDE, CATEGORY, SOLD, DISCLOSED, ENUMERATED, PARTIES, IDENTIFY, COLLECTS
BUSINESS	BUSINESS, PURPOSE, SERVICE, PROVIDER, SERVICES, BEHALF, PROVIDING, CONTRACT, ENTITY, COMMERCIAL, RECEIVING, FINANCIAL, COMPANY, GOODS
PERSON	COLLECTED, PERSON, NATURAL, MEDICAL, SOLELY, OFFICER, OWNER

IV. Analysis result

The comparison of Korea's Personal Information Protection Act, the EU's GDPR, and CCPA in the U.S. can give the following implications.

First, it is about online identifiers, device identifiers, and form information. The U.S. CCPA and EU GDPR clearly include online and device identifiers in the definition of personal information in order to eliminate wasteful controversy over identity. In particular, the U.S. CCPA has specific definitions of online contact information, online unique identifiers, and inference information. The EU GDPR does not have separate definitions for online identifiers or device identifiers, but clarifies its meaning and scope through official handbooks, opinions and Q&A to resolve any controversy that may arise in interpretation. Korea's revised Personal Information Protection Act has also been trying to redesign and materialize personal information by dividing the types of personal information into direct, indirect and alias information, reflecting criticism from

industry and experts that the definition of personal information is abstract and unclear. However, it remains silent on online identifiers, device identifiers, behavioral information, advertising information, inference information, Internet browsing and search records, and information about Internet websites/ application programs/advertisements and user interactions, which are at the center of the most controversy in big data and artificial intelligence. Therefore, the revised Privacy Act alone does not seem to be enough to solve personal information problems related to newly born-digital data in the era of the data economy.

Second, it concerns the subject, criteria and methods of determining identity. The U.S.'s CCPA, the EU's GDPR, does not provide clear criteria for who determines identity, standards and methods. However, the countries provide relatively clear criteria for the subject, criteria and methods of determining identity through documentation or guidelines. The U.S. FTC objectifies the identity subject by acknowledging the difficulty of distinguishing between identification and non-identification information in reality and taking the position that it should also decide whether to protect the information based on "whether the processing of the information can affect the privacy of consumers." Meanwhile, EU WP29 extends to third parties by considering 'all means reasonably available to any third party or personal information processor.' Korea's revised Personal Information Protection Act defines the information that can be easily combined with other information as a type of personal information, even if the information alone does not identify a particular individual, and stipulates that the time, cost, and technology required to recognize an individual, such as the availability of other information, should be considered rationally. Therefore, it can be said that this specifically sets out the criteria for judging the uniqueness of identification. However, it is not clear from whom the availability should be judged, whether only time, cost, technology, or other factors should be considered, and to what extent single out, linkability, and information should be considered identifiable.

In addition, according to the frequency of keywords in the Personal Information Protection Act of Korea, EU, and the U.S. through the network analysis method, all three countries ranked the word 'PERSONAL' at the top, while 'INFORMATION' and 'DATA' were ranked at the top of both countries. This shows that 'PERSONAL,' 'INFORMATION' and 'DATA' are the key keywords in each country's legislation.

Table 7 Keyword Frequency Results by Country

PIPA (Korea)		GDPR (European Union)		CCPA (United States)	
Keyword	**Freq.**	**Keyword**	**Freq.**	**Keyword**	**Freq.**
INFORMATION	745	DATA	608	INFORMATION	305
PERSONAL	598	PROCESSING	295	CONSUMER	271
PROTECTION	209	SUPERVISORY	294	BUSINESS	228
DATA	180	PERSONAL	260	PERSONAL	192
COMMISSION	160	CONTROLLER	254	SECTION	92

The grouped keywords between keywords derived by the network analysis method show that 'PERSONAL,' 'INFORMATION,' and 'DATA' are also derived from grouped keywords.

Table 8 Keywords by Network Group by Country

PIPA (Korea)	GDPR (European Union)	CCPA (United States)
COMMISSION	DATA	CONSUMER
COMMUNICATIONS	SUPERVISORY	REGULATIONS
INFORMATION	CONDUCT	RIGHT
ADMINISTRATIVE	ORGANISATION	INFORMATION
PERSON	PROCESSORS	BUSINESS
DATA	OPERATIONS	PERSON
REGULATIONS		

PIPA (Korea)	GDPR (European Union)	CCPA (United States)
COMMISSION	DATA	CONSUMER
COMMUNICATIONS	SUPERVISORY	REGULATIONS
INFORMATION	CONDUCT	RIGHT
ADMINISTRATIVE	ORGANISATION	INFORMATION
PERSON	PROCESSORS	BUSINESS
DATA	OPERATIONS	PERSON
REGULATIONS		

The following can be found through a comparison of the laws of the three countries. First, it is about the mechanism of the law. GDPR takes an opt-in

mechanism and CCPA takes an opt-out mechanism. The basic assumption of GDPR is that personal data should not be collected and sold without consent.

GDPR applies to the actions of the controller throughout the lifecycle of the information, including collection, use, sharing, and deletion of personal information. It stipulates that the collection and processing of information must meet one of the six requirements set by law, including consent. On the other hand, CCPA, based on the fact that a business operator can collect, use, distribute, and sell personal information, takes a form that cannot be sold if an opt-out is exercised. CCPA has no practical restrictions on the collection, use, and sharing because there is no need to obtain consent or provide an opportunity to refuse the collection. However, it only provides for consumers to exercise their opt-out rights. Second, it is about the rights of the data subject. South Korea's personal information protection law as in Article 4, the rights of the information subject ① The right to receive information ② Consent or not, The right to select and decide the scope of consent ③ Request to view personal information right to seek ④ The right to request suspension, correction, deletion and destruction of personal information ⑤ It is listed as the right to remedy the damage in accordance with prompt and fair procedures. In addition, various rights are guaranteed according to regulations. GDPR and Compared to the rights protected under CCPA, our law is the right to be informed. Similar to the right to delete, right to delete, right to correct, right to read, right to restrict processing, and right not to be discriminated against it contains one rule.

V. Conclusion

With the 4th Industrial Revolution and the entry into the data economy, the digital transformation that began in the 1970s has been developing into a deeper process with the background of recent advances in information technology such as artificial intelligence, IoT, and big data. Digital transformation takes place through data, and various innovations are created through the process of receiving data from the real world, processing it in the virtual world, and applying it back to the real world. With the digital transformation of data-mediated data spreading across industries and social sectors, the business of utilizing personal information is increasing, and thus, personal information protection has emerged as an important social issue, and the implementation of the European Union's GDPR has put the personal information protection system into a new phase.

Europe and the United States have different cultures about the right to self-determination of personal information. Similar methods starting in 2018 when GDPR came into force and CCPA was enacted. Contents of rights protection are

converging toward incense. These two laws can be applied offshore. Since there is a surname, there is a possibility that Korean companies will also comply, and better Information transcends national borders in a global market that is forming a single digital market. Because it is a transboundary commodity that is a transboundary commodity, it is also important in terms of the need for rain. By comparing GDPR and CCPA, writing can get implications for Korea's personal information protection law.

In this paper, we compared South Korea, the EU, and the United States in relation to the Personal Information Protection Act and visualized using the keywords derived from the frequency analysis with the network analysis method.

Through this paper, some implications have been derived regarding the Personal Information Protection Act of Korea, the EU, and the United States. First, in relation to alias information, Korea provided special cases for the definition of alias information and processing of alias information, and the United States classified it as unidentified information without distinction between alias information and anonymous information. Second, regarding the right to information mobility and the right to decision making of algorithms, Korea applied only to credit information, and the United States recognized general application in areas other than credit information. Third, as for user control, the EU required that enterprises collect and process data only on at least one of the six legal grounds described in law, while the United States allowed entities to collect data from consumers without first obtaining consent. Finally, according to the results of the network analysis, Korea is focusing on personal information and information subjects, the EU is focusing on Data, Processing, and Supervision, and the United States is focusing on Information, Consumer, and Business. Fourth, This is part of the scope of the law. According to the definition of the subject of the information to be protected, the personal information, and the controller who is obligated to comply, the scope of the law is the intersection. GDPR protects individuals as living natural persons, regardless of nationality or place of residence, whereas CCPA protects consumers who are residents of California, so GDPR is more protected. Personal data under GDPR is defined as any information relating to an identified or identifiable natural person. However, in CCPA, personal information is a concept that includes information on homes and devices as well as natural persons, so CCPA is wider for personal information subject to the law. GDPR is suitable for controllers that provide goods or services to data subjects in the EU, even if they have a place of business in the EU or do not have a place in the EU used.

In line with the global economic crisis caused by COVID-19, data is considered crude oil in the data economy era and is the biggest driving force behind the vitalization of the data economy. With the implementation of the Data 3 Act (Personal Information Protection Act, Information and

Communication Network Act and Credit Information Act) in Korea, the Korean government is accelerating the transition to the data economy through the government's digital New Deal policy, which will cost 7.9 trillion won. The completion of the Personal Information Protection Act, the core of the Data 3 Act, will be the starting point for the data economy's success. We hope this paper will be used to provide implications for the Personal Information Protection Act as a starting point for the data economy's success.

References

California Consumer Privacy ACT (2020), https://oag.ca.gov/privacy/ccpa

Cho, S.H. (2018), "A Study on Analysis of the Trend of Blockchain by Key Words Network Analysis", Journal of Korea Institute of Information, Electronics, and Communication Technology, 18(10): 550-555.

Choe, H.C., Lee, D. H, Seo, I.W., Kim, H.D. (2013), "Patent citation network analysis for the domain of organic photovoltaic cells: Country, institution, and technology field", Renewable and Sustainable Energy Reviews, 26© , 492-505.

Economic Times, "India to approach the EU seeking 'adequacy' status with the GDPR" , 2019.7.30.

Freeman, L.C. (1979), "Centrality in Social Networks Conceptual Clarification", Social Networks, 215-239.

General Data Protection Regulation (2020), https://gdpr-info.eu/

Jasjit, S. (2005), "Collaborative Networks as Determinants of Knowledge Diffusion Patterns", Management Science, 5, 756-770.

Kim, D.H., Lee, B.K., Sohn, S.Y (2016), "Quantifying technology-industry spillover effects based on patent citation network analysis of unmanned aerial vehicle(UAV)", Technological Forecasting & Social Change, 140-157.

Korea Internet & Security Agency, "EU General Privacy Act (GDPR) Guidebook", 2020. 06. 30.

Lee, C.B. (2020), "Comparison of the concept and scope of personal information in the US, EU and Japan", 2020 KISA REPORT, Vol. 8.

Lee, S. S. (2012), "Network Analysis Methods", Nonhyeong, pp. 5-25.

Lexology, "The impact of the GDPR outside the EU" , 2019.9.17.

Park, J. J., Kim N. R., Han E. J. (2018), "Analysis of Trends in Science and Technology using Keyword Network Analysis", Journal of the Korea Information Systems Research, Vol. 23, No. 2, pp. 63-73.

Park. S.U. (2019), "Keyword Analysis of Data Technology Using Big Data Technique", Journal of Korea Technology Innovation Society, 22(2): 265-281.

Personal Information Protection Act (2020) https://www.law.go.kr

Tong, Q., Wei, S., Chang, Z (2017), "How to Identify the Most Powerful Node in Complex Networks?: A Novel Entropy Centrality Approach", Entropy, 11, 1-24.

Tseng, F.M., Hsieh, C.H., Peng, Y.N., Chu, Y.W. (2011), "Using patent data to analyze trends and the technological strategies of the amorphous silicon thin-film solar cell industry", Technological Forecasting and Social Change, 2, 332-345.

The Washington Post, "The Technology 202: More than 200 companies are calling for a national privacy law. Here's an inside look at their proposal" , 2018.12.6.

Wasserman, S. Faust, K. (1994), "Social Network Analysis", Cambridge University Press.

Yang, H.C. (2017), "Present and Future of the 4th Industrial Revolution: Focusing on Keyword Network Analysis", STEPI WORKKING PAPER SERIES, WP 2017-02.

Zhao, R., Chen, B. (2014), "Applying author co-citation analysis to user interaction analysis: a case study on instant messaging groups", Scientometrics, 2, 985-997.

KnowledgeMartix Plus, http://mirian.kisti.re.kr/km/
NodeXL, https://www.smrfoundation.org/nodexl/
VOSviewer, https://www.vosviewer.com/
https://doi.org/10.22837/pac.2020.6.1.71