

미래산업 분야 법제이슈에 관한 연구(VI)

- 클라우드컴퓨팅 환경의 이용자 보호에 관한 법제연구 -

한 정 미



글로벌법제전략 연구 16-20-③

**미래산업 분야 법제이슈에 관한 연구(VI)
- 클라우드컴퓨팅 환경의 이용자 보호에
관한 법제연구 -**

한 정 미

**미래산업 분야 법제이슈에 관한 연구(VI)
- 클라우드컴퓨팅 환경의 이용자 보호에
관한 법제연구 -**

Research on Legal Issues Associated with Future
Industries (VI)

- A Study on the Protect Users in a Cloud Computing
Environment -

연구자 : 한정미 연구위원
Han, Joungmee

2016. 8. 31

요약문

I. 배경 및 목적

□ 클라우드컴퓨팅 국제동향 분석의 필요성

- IoT·빅데이터·모바일 등의 활성화에 따라 데이터량이 폭증하고 클라우드를 통한 트래픽이 대부분(76%)을 차지하고 있으며, 전통적인 SW 기업뿐만 아니라 인터넷 기업, 통신사 등 다양한 ICT기업이 클라우드 시장 선점을 위해 진입 중
- 클라우드컴퓨팅은 우리나라가 주도적으로 정책을 추진하고 있는 ICT 분야의 대표적인 기술·서비스분야라 할 수 있으며, 미래산업의 바탕이 되는 기술 패러다임에 해당

□ 클라우드컴퓨팅 이용자보호의 필요성

- 클라우드컴퓨팅에 관한 규제 유형과 방법은 개인정보보호의 문제와 보안사항에 관한 일반적이고 통일적인 규제를 제외하고는 매우 다양하고 빠른 변화에 따라 함께 변화해야 할 사안
- 최근에는 클라우드컴퓨팅을 통한 계약에 관한 법적 쟁점이 여러 시각에서 제기

II. 주요 내용

□ 클라우드컴퓨팅의 개인정보보호

- 클라우드컴퓨팅의 가장 큰 쟁점은 개인정보의 국외이전에 관한 사항
- 클라우드컴퓨팅 자체의 가장 큰 특성이라 할 수 있는 자유로운 정보의 이동은 국경을 초월하게 되는 것이며 이에 따라 이용자의 개인정보가 저장, 제공되는 기반이 국외에 있는 경우를 고려
- 클라우드컴퓨팅을 포함한 정보통신 분야의 발전은 어느 한 국가 내에서 개발·발전되는 것을 전제로 할 수 없음
- 따라서 국가별 기술이나 보안의 수준뿐만 아니라 이를 운영하는 법제도의 평준화, 개발도상국의 접근성 향상이 필수적인 상황이며, 이에 관한 국가간의 지속적인 논의와 제도로의 수렴이 요구됨

□ 클라우드컴퓨팅의 보안

- 클라우드컴퓨팅에 대한 해킹 등 불법적인 파괴나 변형, 허가되지 않은 정보의 공개나 접근에 대해 적절한 보안조치를 사전에 시행해야 함에도 불구하고 적절한 보안조치의 수준을 상정하는 기준이 국가별로 달라질 수 있음
- 2010년 4월 이후 ITU에서 ‘통신 영역에서의 클라우드컴퓨팅 보안 가이드라인(Security guideline for cloud computing in telecommunication area)’, ‘클라우드 기반의 원격통신 서비스 환경의 체제와 보안에 필요한 요건들(Security requirements and framework of cloud based telecommunication service environment)’, ‘통신조직을 위한 개인정보 관리 지침(Guideline for management of personally identifiable information for telecommunication organizations)’ 등의 작업이 진행결과를 주목할 필요가 있음

- 개인정보·보안에 관한 수준의 차이로 인한 문제도 있는데, 이를 ITU의 ‘커넥트 2020 어젠다’에서는 디지털 격차로 표현하고 정보의 접근성을 높이도록 해마다 목표치를 제시함
- 클라우드컴퓨팅 계약 관련 이용자 보호
 - 국가별 계약법제에 따르는 기존 규제 환경은 클라우드 기반 서비스에 적합하지 않을 수 있다는 문제
 - 클라우드컴퓨팅 서비스 제공자가 동일한 계약 용어를 사용하여 청약하는 경우에도 국가별 계약법제의 차이로 인하여 계약을 체결한 이용자의 법 이해가 다르게 작용하는 문제가 발생
 - 이를 개선하기 위하여 EU에서는 2015년 9월 12일 “디지털 콘텐츠 제공 계약 고려사항에 관한 유럽의회와 이사회의 지침(이하 ‘제안서’라 함)”이 제안되었고, 이를 일명 “현대 디지털 계약 원칙(Modern digital contract rules)”이라고 설명
 - 또한, EU 집행위원회는 클라우드 제공자와 사용자들 간의 서비스 단계 동의서에 사용하는 유럽 모델 계약용어를 개발하고 소비자 및 소규모 기업을 위하여 「유럽 공통매매법(Common European Sales Law)」에 모델용어와 조건이 포함되도록 할 계획

Ⅲ. 기대효과

- 클라우드컴퓨팅 개인정보 보호를 위한 개선방안 제시
 - 클라우드컴퓨팅에 관해서는 우리나라가 최초의 입법을 하는 등 제도적 정비가 빠른 상황이고, IT분야에서는 가장 빠른 발전 속

도를 보이고 있다고 본다면 우리나라에서도 EU에서와 같은 개인정보 보호수준의 적정성에 관한 구체적인 기준을 세우고 이를 충족하는 법제를 갖춘 국가에 대해서만 우리 국민의 개인정보를 이전, 활용이 가능하도록 하는 방안을 고려

□ 새로운 계약 환경의 이용자보호를 위한 개선방안 제시

- 클라우드컴퓨팅 관련 계약에서의 국제동향은 새로운 디지털계약 원칙의 등장과 서비스계약시 표준용어(표준계약서, 서비스 수준협약)의 사용으로 정리
- 「독점규제 및 공정거래에 관한 법률」의 입법례와 같이 해외기업과의 계약의 경우에도 국내시장이나 우리국민에게 영향을 미치는 경우의 국내법 적용을 명시하는 방안을 고려
- 「약관규제법」의 개정을 통하여 클라우드컴퓨팅 등 디지털 환경의 계약시에 사용될 표준계약서, 표준용어 등을 반영할 필요

▶ 주제어 : 클라우드컴퓨팅, 개인식별정보, 디지털 계약, 클라우드컴퓨팅 보안, 개인정보보호, 국경 간 이동

Abstract

I . Background and Objectives

Necessity for analysis of global trends in cloud computing

- With the vitalization of IoT, big data and mobile, data volumes have increased dramatically. Traffic from cloud computing accounts for the majority of data traffic (76%), with traditional software companies vying for market dominance against a variety of ICT companies such as internet companies and telecommunications companies.
- Cloud computing is a leading ICT technology and service area for Korea, which is playing an active part in its future development.

Necessity of protecting cloud computing users

- With the exception of general and unified regulations on personal data protection and security, the types and methods of regulations on cloud computing should be in line with the changing technology landscape.
- More recently, legal controversies have appeared regarding contracts made via cloud computing.

II . Outline

Personal data protection for cloud computing

- The biggest issue regarding cloud computing is the cross-border transfer of personal data.
 - As the free transfer of data, which is the most distinctive feature of cloud computing, is cross-border by its very nature, cases in which the basis on which user's personal data is stored and provided from abroad should be taken in account.
 - It cannot be assumed that ICT, including cloud computing, has been invented and developed within a single country.
 - This makes it essential to standardize technologies and security levels and related legal systems among different countries and improve accessibility for developing countries. Accordingly, it is necessary to continue international discussions and make systematic findings.
- Security for cloud computing
- Although proper prior security actions against illegal destruction or deformation related to cloud computing such as hacking or unauthorized data disclosure or access are needed, there are varying criteria for proper security levels among many different countries.
 - It is worth paying attention to the outcomes of some works performed by ITU from April 2010: including “Security guideline for cloud computing in telecommunication area”, “Security requirements and framework of cloud based telecommunication service environment” and “Guideline for management of personally identifiable information for telecommunication organizations”.

- ITU's "Connect 2020 Agenda" expressed problems derived from a gap in the level of personal data and security as "digital divide" and suggests targets to improve access to information every year.
- Protection of users related to contracts via cloud computing
 - The existing regulatory environment from country-specific contract law may not be suitable to cloud computing-based services.
 - In the case of a cloud computing service provider offering subscription using the same contract terminology, users who signed a contract may take a different legal interpretation due to any differences in country-specific contract laws.
 - In an effort to tackle this problem, EU presented "Proposals for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content" (hereinafter referred to as "Proposal") on September 12, 2015 and explained it as "Modern digital contract rules".
 - The European Commission plans to develop European contract terminology to be used in service level agreements (SLA) between cloud service providers and users and include model terminology and conditions in the Common European Sales Law for consumers and small businesses.

III. Expected Impact

- Remedies to protect personal data related to clouding computing

- Given that Korea has started systematic improvements related to cloud computing early, becoming the first country to legislate cloud computing law in the world. It has consistently shown the fastest growth rate in the IT industry and there is a need for measures to allow the transfer and utilization of personal data of Korean people only to those countries that demonstrate specific standards for personal data protection levels, as in the EU, including having laws that meet such criteria already in place.

- Proposal of remedies to protect users in a new contract environment
 - The global trend of cloud computing-related contracts is summarized into the advent of new digital contract rules and the use of standardized terminology in service agreements (standard contract form, SLA).
 - As shown in the case of legislation of the Monopoly Regulation and Fair Trade Act, it is needed to consider measures to clarify the application of domestic law to contracts with foreign companies that affect the domestic market or people.
 - It is needed to amend the Regulation of Standardized Contracts Act to reflect standard contract form and terminology to be used in contracts in the digital environment, such as cloud computing.

▶▶ Key Words : Cloud Computing, Personally Identifiable Information, Digital Contract, Security for Cloud Computing, Personal Data Protection, Cross-Border

목 차

요 약 문	3
Abstract	7
제 1 장 서 론	13
제 1 절 연구의 필요성 및 목적	13
제 2 절 연구의 방법과 범위	16
제 2 장 클라우드컴퓨팅의 정보보호와 보안	19
제 1 절 쟁점 검토	19
제 2 절 정보보호 관련 논의 동향	20
1. 규제통합의 필요성과 동향	20
2. 서비스운영 및 규제방식의 변화	24
3. 정보보안에 관한 검토	31
제 3 절 우리나라의 클라우드컴퓨팅 정보보호 관련 법제	35
1. 클라우드컴퓨팅법의 개인정보 관련 입법	35
2. 클라우드컴퓨팅 보안 관련 입법	39
제 4 절 소결 : 시사점	40
제 3 장 클라우드컴퓨팅 계약 관련 이용자 보호	45
제 1 절 쟁점 검토	45
제 2 절 계약 관련 논의동향	46
1. 현대 디지털 계약 원칙의 제시	46

2. 디지털 콘텐츠 제공 계약 관련 고려사항	47
3. 모델계약 용어 사용 등 계약 표준화	51
제 3 절 우리나라의 클라우드컴퓨팅 계약 관련 법제	52
1. 클라우드컴퓨팅법의 계약 관련 입법	52
2. 약관규제법의 계약 관련 입법	53
제 4 절 소결 : 시사점	54
제 4 장 결 론	59
참 고 문 헌	63

【참 고 자 료】

결의안 제 200호 (Busan, 2014)	69
결의안 제 200호 부속서 (Busan, 2014)	74

제 1 장 서 론

제 1 절 연구의 필요성 및 목적

IoT·빅데이터·모바일 등의 활성화에 따라 데이터량이 폭증하고 클라우드를 통한 트래픽이 대부분(76%)을 차지하고 있으며, 전통적인 SW 기업뿐만 아니라 인터넷 기업, 통신사 등 다양한 ICT기업이 클라우드 시장 선점을 위해 진입 중인 것으로 나타났다.¹⁾

이와 같이 세계 각국은 ICT를 활용한 산업의 활성화를 위해 다양한 투자와 기술을 개발을 지속하고 있으며, 우리나라도 법과 정책적 기반을 마련하며, 세계시장에 주도적으로 참여하고 있다.

특히, 우리나라는 2015년 3월 27일 세계 최초로 「클라우드컴퓨팅 발전 및 이용자보호에 관한 법률(이하 ‘클라우드컴퓨팅법’이라 함)」을 제정하여 클라우드컴퓨팅에 관한 입법을 실현한 국가이다. 이 법 입법 이후에도 범정부차원의 ‘K-ICT 전략’(‘15.3.)과 제1차 「클라우드컴퓨팅 발전 기본계획(’16~’18년)」을 수립·시행하여, 공공·민간 부문의 클라우드 이용 확산을 통해 비용절감·업무혁신을 하고, 취약한 국내 클라우드 산업의 경쟁력 강화를 추진하고 있다.²⁾

이와 같이 클라우드컴퓨팅은 우리나라가 주도적으로 정책을 추진하고 있는 ICT 분야의 대표적인 기술·서비스분야라 할 수 있으며, 미래산업의 바탕이 되는 기술 패러다임이라 할 수 있다.

이미 기존의 논의들을 통해 어느 정도 논의가 정리 된 클라우드컴퓨팅의 개념에 대해서 정리하여 보면, 우선 EU에서 ‘클라우드컴퓨팅’은 인터넷을 통해 외부에서 컴퓨터의 데이터를 저장, 처리 및 데이터를 사용하는 것으로 설명하면서, 이것은 사용자가 자신의 요구를 충

1) 관계부처 합동, “K-ICT 클라우드컴퓨팅 활성화 계획(안)”, 2015. 11. 10, 3쪽.

2) 관계부처 합동, 앞의 자료, 1쪽.

족하기 위해 자본 투자를 하지 않아도, 수요에 따라 거의 무제한 컴퓨터에 명령을 할 수 있고 어디서나 인터넷 연결에서 데이터를 얻을 수 있다는 것을 의미한다고 하였다.³⁾

우리나라에서 클라우드컴퓨팅의 법적인 개념으로는 「클라우드컴퓨팅법」의 정의규정을 살펴 볼 수 있는데, 이 법에서 “클라우드컴퓨팅(Cloud Computing)이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계”로 정의하고 있다(제2조 제1호).

또한, 같은 법에서 ‘클라우드컴퓨팅기술’이란 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술로서 가상화 기술, 분산처리 기술 등을 대통령령으로 정하도록 하고 있으며(제2조 제2호), ‘클라우드컴퓨팅서비스’란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하도록 하고 있다(제2조 제3호).

이와 같이 클라우드컴퓨팅의 개념에 관한 법적 정의나 일반적인 개념의 정리는 완료된 상태이지만 클라우드컴퓨팅의 기술적인 면에서는 여전히 그 형태가 계속 변하고 있으며,⁴⁾ 이로 인한 서비스의 유형도 고정적이지 않다. 따라서 클라우드컴퓨팅에 관한 규제 유형과 방법은 개인정보보호의 문제와 보안사항에 관한 일반적이고 통일적인 규제를 제외하고는 매우 다양하고 빠른 변화에 따라 함께 변화해야 할 사안이라고 판단된다.

3) EUROPEAN COMMISSION, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Unleashing the Potential of Cloud Computing in Europe”, 2012. 9. 27 p.2.

4) 전세계적으로 ICT활용 패러다임이 HW중심→설치형 SW→서비스 형태로 HW·SW를 사용하는 클라우드 시대로 전환 중이다. 관계부처 합동, “K-ICT 클라우드컴퓨팅 활성화 계획(안)”, 2015. 11. 10, 3쪽.

이와 관련하여 국제전기통신연합(International Telecommunication Union ; ITU)은 정보통신기술 부분 UN전문기구로 2014년 ICT 개발을 위한 ‘커넥트 2020 어젠다’를 채택하며 브로드밴드 활용 등 ICT 접근성 향상을 위한 다양한 전략을 제시한 바 있고,⁵⁾ EU 집행위원회는 “유럽 클라우드컴퓨팅의 잠재력 실현(2012)”이라는 보고서를 발표하고⁶⁾ 지속적으로 실현방안을 구체화하고 있다.

정부의 공공서비스 영역뿐만 아니라 민간의 기업활동 영역에서도 구글, 아마존 등 대형 글로벌 기업이나 우리나라의 네이버, KT 등의 기업들의 핵심 정보통신기술이 되고 있으며, 관련 사업영역도 무한히 확장되고 있다.⁷⁾⁸⁾

5) 연합뉴스(2014. 11. 5. 보도자료 참조)

<http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=001&aid=00072-30052>(2016. 7. 18 최종접속)

6) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>(2016. 7. 18 최종접속)

7) 관계부처 합동, “K-ICT 클라우드컴퓨팅 활성화 계획(안)”, 2015. 11. 10, 5-7쪽 참조.

8) <표> 서비스 유형에 따른 클라우드컴퓨팅 분류

모델	정의	주요기업
SaaS (Software as a Service)	ERP, CRM, 오피스 등 SW를 필요한 경우 인터넷을 통해 사용	[해외] 구글(오피스), MS(오피스, CRM), Salesforce.com(CRM) 등 [국내] 더존비즈온(회계), 다우기술(협업), 한컴(오피스) 등
PaaS (Platform as a Service)	SW의 개발 및 실행을 위한 개발 환경 제공	[해외] 구글, MS, Salesforce.com 등
IaaS (Infrastructure as a Service)	서버, 스토리지 등 IT 인프라를 구축하지 않고 필요시 서비스로 제공	[해외] 아마존, MS, 구글 등 [국내] KT, SKT, LGCNS 등

출처 : 이인용, “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률안 검토보고서”, 국회 미래창조과학방송통신위원회, 2013. 12. 12쪽.

클라우드컴퓨팅 산업의 성장과 확대에 따른 이용자보호는 우리나라의 입법 진행과정에서부터 입법이후까지도 계속 쟁점으로 논의되고 있다. 클라우드컴퓨팅 등 ICT는 미래산업에 포함되는 중점분야로 우리나라의 독립적인 법제도 수립보다는 글로벌 시장에서의 정책변화를 수용하기 위한 노력이 중요하며, 클라우드컴퓨팅에 기반한 정보의 저장이나 서비스 제공이 우리나라 안에서만 이루어지는 것이 아니므로 우리나라에서 입법이 이루어졌다고 해서 쟁점이 해결된 것은 아니고, 오히려 이에 대한 해외의 정보보안 및 계약관련 이슈 등 이용자보호의 논의에 지속적인 관심을 기울여야 할 필요가 있다.

최근에는 클라우드컴퓨팅을 통한 계약에 관한 법적 쟁점이 여러 시각에서 제기되고 있는데 특히, EU의 경우 클라우드컴퓨팅 계약에 관한 전문가 그룹을 만들고 “2013년 6월 18일 위원회 내 클라우드컴퓨팅 계약관련 전문가 집단 설립에 대한 공식 결정”을 발표하였으며,⁹⁾ EU 집행위원회에서는 “현대 디지털 계약 원칙”을 제안하는 등¹⁰⁾ 적극적인 활동을 통해 클라우드컴퓨팅 계약의 활성화뿐만 아니라 안전하고 공정한 클라우드컴퓨팅 계약의 실현방법을 모색하고 있다.

따라서 이 보고서에서는 클라우드컴퓨팅 관련 정보보호, 서비스 계약 관련 쟁점사항 등 이용자보호에 관한 국제적 논의 동향을 검토하여 우리나라 법제에 시사점을 제시하는 것을 연구의 목적으로 한다.

제 2 절 연구의 방법과 범위

클라우드컴퓨팅에 관해서는 우리나라가 최초의 입법을 하였고, 외국에서는 대체로 기존의 개인정보보호 및 보안 등 관련 법률을 통하거나 관련 정책을 추진하여 제도를 운용하고 있다.¹¹⁾ 따라서 이하에서

9) http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm(2016. 7. 18 최종접속)

10) http://ec.europa.eu/justice/newsroom/contract/news/151209_en.htm(2016. 7. 18 최종접속)

11) 박종수, “클라우드컴퓨팅과 정보보호”, 법제연구 제46호, 2014. 59쪽 이하 ; 이인용,

는 개별 국가의 클라우드컴퓨팅 관련 입법이 아닌, 글로벌 산업과 시장에서의 클라우드컴퓨팅 관련 법적인 논의를 분석해 보고자 정보통신 분야의 국제기구인 ITU와 EU의 클라우드컴퓨팅 관련 자료를 중심으로 분석, 검토한다.

국제전기통신연합(ITU)의 ‘커넥트 2020 어젠다’를 채택하고, 2015년 정기이사회에서는 이에 따른 이행전략을 수립한 바 있다. ‘커넥트 2020 어젠다’는 ICT의 미래비전을 제시하고 4개의 상위목표와 17건의 구체적 실행목적을 설정한 것으로 ITU 회원국과 ICT 관련 모든 국가에 관련되는 사항이라 할 것이며, 우리나라가 주도적으로 발의하고 채택한 것으로 이에 따른 이행전략 분석과 국제적인 현안 대응의 분석의 의미가 클 것이라 판단된다.

한편, EU를 중심으로 제시되고 있는 이용자 관련 정보의 보호 및 클라우드컴퓨팅을 통한 계약상의 권고사항 등은 향후 우리사회에서도 해결되어야 할 법적인 과제의 선행자료로서 분석할 의미가 있다.

문헌연구를 중심으로 수행하며 전문가 워크숍과 자문의견도 추가하여 보고서를 작성한다.

앞의 검토보고서”, 국회 미래창조과학방송통신위원회, 2013. 12. 49-50쪽.

제 2 장 클라우드컴퓨팅의 정보보호와 보안

제 1 절 쟁점 검토

클라우드컴퓨팅의 이용에 있어서 가장 문제가 되는 것은 개인정보의 보호와 보안에 관한 사항이라는 것은 이견의 여지가 없다. 그런데 개인정보의 정보보호와 보안 관련 쟁점도 그 범위가 넓기 때문에 구체적으로 클라우드컴퓨팅의 이용자보호를 위한 쟁점을 설정할 필요가 있다.

「클라우드컴퓨팅법」의 입법과정에서 제기되고 논의되었던 바와 같이 가장 큰 쟁점은 개인정보의 국외이전에 관한 사항이라 할 수 있다.

개인정보 관련법이 속지주의 원칙에 따라 운용됨에 따라 기본적으로 국내에서 수집되거나 가공되어진 개인정보에 대한 법적책임은 국내법에 의해 정해진다.¹²⁾ 이와 같은 개인정보 관련 법제의 적용원칙은 다른 국가에서도 대동소이할 것이며, 여기에서 클라우드컴퓨팅의 개인정보 관련 법적인 문제가 발생한다.

클라우드컴퓨팅 자체의 가장 큰 특성이라 할 수 있는 자유로운 정보의 이동은 국경을 초월하게 되는 것이며 이에 따라 이용자의 개인정보가 저장, 제공되는 기반이 국외에 있는 경우를 당연히 고려하여야 한다.¹³⁾ 실제 대부분의 클라우드컴퓨팅 서비스 제공회사는 다국적 기업인 경우가 많으며 이러한 경우 기존의 통신관련 법률이나 보안관련 법률의 내용으로 규율하기 어려운 상황이 발생할 우려가 있는 것

12) 박영규, “클라우드컴퓨팅의 법적 문제에 관한 고찰”, 법조 2012. 8.(Vol.671), 192쪽.

13) 2015년 WTO에서는 국경간 전자상거래 규모는 매년 15% 이상 증가하고 있는 추세이며, 이중 상당의 자료가 개인정보를 포함하고 있을 것으로 추정된다고 밝히고 있다. 행정자치부 보도자료, 2015. 12. 15. 재인용.

(http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_00000000008&nttId=47865), 2016. 8. 3. 최종방문.

이다.¹⁴⁾ 예컨대, Facebook, Google+, Dropbox&Co 등 미국계 클라우드 서비스가 증가하고 있으며, 이들의 서버에 있는 정보에 대해서는 우리 국민이 국내에서 정보보호를 받을 수 없는 한계를 갖고 있기 때문이다.¹⁵⁾

다음으로 클라우드컴퓨팅 개인정보 및 보안 규제기관의 업무영역 혹은 역할의 변화를 생각해 볼 수 있다. 클라우드컴퓨팅 자체가 기존의 통신 영역에서만 서비스 되는 것이라 볼 수 없으므로 해당 영역의 규제를 어떠한 기관에서 어떤 방식으로 운영해 가는 것이 바람직할 것인지에 대한 논의가 필요하다.

제 2 절 정보보호 관련 논의 동향

1. 규제통합의 필요성과 동향

(1) EU의 규제통합 동향

오늘날 대다수의 온라인 서비스들은 통합적 서비스의 제공이 용이한 클라우드 기반으로 이동하고 있는 추세이며, 이러한 추세는 EU 각 국가에서도 동일하게 나타나고 있다. 이에 따라 EU에서는 클라우드컴퓨팅 관련 규제를 여러 가지 각도에서 논의하고 현상에 맞도록 변화시켜나가고 있다.

2012년 1월 25일, 유럽연합 집행위원회는 현재의 “개별적이고 오래된” 정보보호법 입법구조를 통일시키기 위한 유럽연합 정보보호지침 개정안을 발표했다.¹⁶⁾ 여기서 제안된 변경 사항은 ① 국가 규제기관은 특정한 상황에서 회원국에 속한 조직을 규제하는 조치를 취할 권

14) http://www.dt.co.kr/contents.html?article_no=2016042702109960813013(디지털 타임스 2016. 4. 27 기사 참조), 2016. 7. 26 최종방문.

15) 박중수, 앞의 논문, 58쪽.

16) <https://itunews.itu.int/En/3414-Regulation-in-the-cloud.note.aspx>(2016. 8. 2. 최종접속)

한을 가지며, 상황에 따라 백만 유로 이하 혹은 조직의 연간매출의 2% 이하의 벌금을 부과할 수 있다. ② 개인정보의 정의는 정보 대상과 연관된 모든 정보를 포괄하며, 데이터 수집을 위한 규정에 의해 개개인의 명확한 동의가 요구된다. ③ 개정안은 유럽연합 뿐 아니라, 유럽연합 국민들과 관련된 개인정보를 다루는 비유럽연합 독립체까지 영향력을 가진다. ④ 개인정보를 다루는 조직은 정보유출 사항에 대하여 보고해야 할 의무를 가진다. 부당한 지연은 허락되지 않으며, 가능하다면 정보가 유출된 후 24시간 이내에 보고해야 한다. ⑤ 데이터 관리자는 정보보호 영향력 평가를 시행해야 하며, 정보보호관들을 임명하고, 정보유출이 발생한 경우에는 제3의 이해관계자들에게 이를 전달해야 할 의무를 가진다. ⑥ 개개인들은 특정 상황의 경우, “잊혀질 권리”를 새로이 부여 받게 되며, 그들의 정보에 접근하기 위하여 추가적인 대가를 지불하지 않아도 된다. ⑦ 데이터 관리자에게 이전 규정 보다 제한적 특례가 적용되는 한편, 국제적 정보의 이동은 보호장치와 사전검토를 시행할 규제기관이 요구되는 까다로운 규제 구조의 대상이 된다는 내용을 포함하고 있으나 이러한 제안의 내용은 여러 국가의 이해관계가 달라 많은 토의와 협의를 거친 이후에 개정될 것으로 예상될 것으로 전망되었다.¹⁷⁾

이와 같은 EU의 정보보호 관련 규제통합 및 적용에 관한 논의는 클라우드컴퓨팅에 관해서도 적용해 볼 수 있는데, 클라우드컴퓨팅의 확산 추세는 복합관할권의 확장을 일으키는 많은 문제들을 포함하고 있다는 점에서 동일하기 때문이다. 또한, 새로운 서비스와 관련된 불법정보나 행위에 대한 법의 적용이나 법의 관할권 결정과 연관된 의문들이 제기되고 있는 것이다.¹⁸⁾

17) <https://itunews.itu.int/En/3414-Regulation-in-the-cloud.note.aspx>(2016. 8. 2 최종접속)

18) EUROPEAN COMMISSION, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Unleashing

특히 EU의 경우 많은 회원국가의 서로 다른 법체계를 고려한다면 디지털 단일시장으로 클라우드컴퓨팅을 운용하고 효율적인 해결책을 제시하는 것이 어려운 상황이고 이러한 논의는 결국 EU뿐만 아니라 범세계적인 문제로 볼 수 있다.¹⁹⁾

이러한 문제를 해결하기 위하여 EU 집행위원회는 세 가지 클라우드 관련 특별정책을 제시하였는데 이를 보면, ① 산발적 기준의 단순화, ② 공정하고 안전한 계약용어와 조건, ③ 공공부문 리더십의 혁신과 성장을 도모할 유럽 클라우드 파트너십의 설립이다.²⁰⁾

이들 클라우드컴퓨팅 관련 특별정책을 자세히 설명한 내용을 정리하면 다음과 같다. 단, 여기에서 “공정하고 안전한 계약용어와 조건”의 경우 뒤에 다루게 될 클라우드컴퓨팅의 계약관련 쟁점에도 영향을 주는 사안이기 때문에 뒤에서 설명한다.

(2) 산발적 기준의 단순화 · 표준화

이미 클라우드컴퓨팅에 대해 표준화 및 인증된 제도가 세계 여러 국가에서 존재하고 있다.

그러나 유럽 전기통신표준협회(ETSI)는 기존의 다양한 기준을 재정비하고 클라우드 표준화와 정보처리 상호운용성의 기준에 대한 적합성을 판단하기 위한 클라우드 그룹을 만들고 이 그룹을 통해서 필수 기준(특히 보안, 정보처리의 상호운용성, 데이터의 이동성과 가역성)에 대한 가이드라인을 제시하도록 하여 신뢰할 만한 클라우드컴퓨팅의 서비스를 제공할 수 있도록 하는 한편, EU 내에서 클라우드컴퓨팅 분야의 자발적 인증제도개발도 하도록 하였다.²¹⁾

the Potential of Cloud Computing in Europe”, 2012. 9. 27 p.7.

19) *Id.* p.8.

20) *Id.* p.10.

21) *Id.* p.10-11.

한편, 우리나라의 경우 「클라우드컴퓨팅법」에서는 인증제도가 도입되지 못하였으나, 이미 2012년 2월에 “클라우드 서비스 인증제 운영요령(안)”이 제안된 바 있다.²²⁾

이 운영요령에서 클라우드 서비스 인증이라 함은 클라우드 서비스가 인증심사기준에 적합함을 클라우드 서비스 인증위원회가 심의·의결하는 것으로 규정하고, 보안, 서비스지속성, 데이터 관리 등에 관한 상세한 지표로 인증기준을 설정하고 있다. 다만, 이후 「클라우드컴퓨팅법」에 인증제도가 포함되지 못하였기 때문에 인증제도의 유효성에 대해서는 법적으로 인정되지 않는 상태이다.

(3) 공공부문 리더십의 혁신과 성장을 도모할 유럽 클라우드 파트너십의 설립

EU 회원국 중 이미 몇몇의 회원국들은 프랑스의 안드로메데(Andromede), 영국의 지클라우드(G-Cloud), 독일의 트러스티드 클라우드(Trusted Cloud)와 같은 공공분야의 클라우드 서비스를 시작하고 있다. 민간영역에서의 클라우드 서비스 보다 공공영역에서의 클라우드 서비스(e-헬스, 세무행정, 복지행정, 그리고 오픈데이터와 같은 전자정부 등)는 비용을 절감하며 상호운용이 가능하다는 장점이 있다.²³⁾

이와 관련하여 유럽 클라우드 파트너십(ECP)은 상호운용이 가능한 공공 클라우드를 보장하고 업계 내 기관들과 협력하는 공공기관들이 클라우드를 통한 공공구매를 할 수 있도록 하고 몇 가지 기준을 제안하고 있다.²⁴⁾ 그 내용으로는 첫째, 공공 클라우드의 요구조건 확립으

22) 미래창조과학부 홈페이지,

<http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw44&artId=1186502>
(2016. 8. 22. 최종접속)

23) EUROPEAN COMMISSION, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Unleashing the Potential of Cloud Computing in Europe”, 2012. 9. 27 p.14.

24) *Id.* p.14.

로서 IT 관련 물품 조달을 위한 규격개발 및 적합성과 실적을 증명하기 위한 참고자료 확보하고 둘째, 새로이 발생한 사용자의 요구에 따라 공공기관들이 클라우드컴퓨팅 서비스를 공공구매 하도록 유도한다는 것이다. 또한, 셋째로는 주주들과의 협업을 요하는 다양한 계획들을 수립하고 집행한다는 것이다.²⁵⁾

그런데 공공기관의 클라우드컴퓨팅 서비스 사용에 관해서 참고해야 할 사례가 덴마크 지방자치단체에서 있었다.

2011년 2월 덴마크의 정보보호기관(DDPA)에서 클라우드컴퓨팅 이용 사례에 대한 발표가 있었다. 해당 사례는 덴마크의 지방자치단체인 오덴세(Odense)에서 학업계획과 평가, 학생 개인의 교육적 발전에 대한 정보를 등록할 때, 개인의 민감한 정보 처리를 위해 학교 시스템에 구글 앱을 도입하고자 하는 계획에 대한 것이었다.²⁶⁾

이에 대하여 DDPA는 특정한 개인의 민감정보의 저장을 위해 클라우드컴퓨팅을 사용하려는 해당 지방자치단체의 요청을 거절했는데, 이와 같은 사례를 통해서 클라우드 서비스가 사용되기 전에 중대한 위험평가가 진행되어야 하고, 표준체계의 도입이 필요하다는 것을 확인할 수 있는 계기가 된 것으로 평가되고 있다.²⁷⁾

2. 서비스운영 및 규제방식의 변화

(1) 클라우드 서비스 운영방식

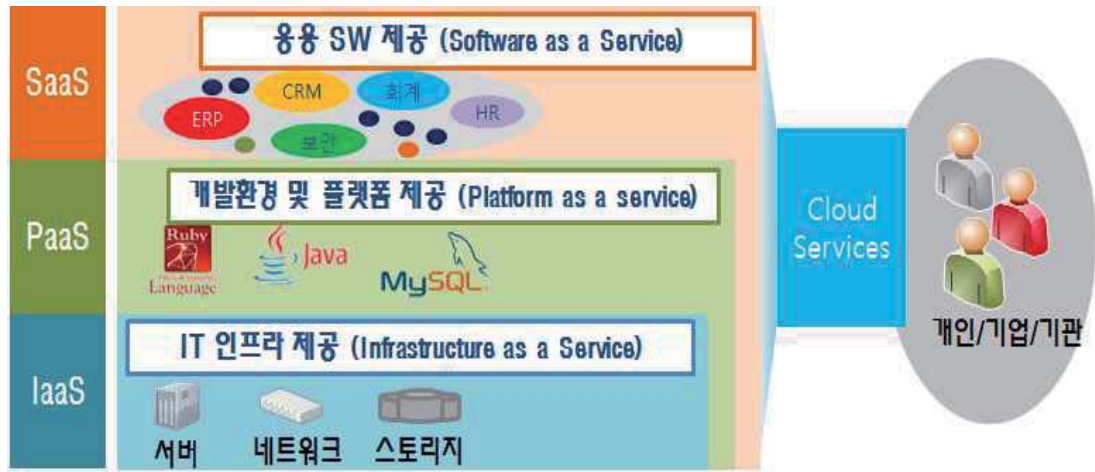
클라우드 서비스 모델 유형에 따라 개념을 정리하면 아래 그림과 같다.

25) *Id.*

26) ITU, 「Privacy in Cloud Computing」, 2012. 3, p.8

27) *Id.*

<그림-1> 클라우드의 유형



출처 : 관계부처 합동, “K-ICT 클라우드컴퓨팅 활성화 계획(안)”, 2015. 11. 10, 2쪽.

우리나라에서 정리된 위의 모델 그림보다 앞서, ITU에서 2012년 4월에 발표된 ITU의 발표문에서 클라우드 서비스의 운영에 관하여 ① 정보 보호와 보안문제를 염두에 둔 규제, ② 모범적인 규제운영에 대한 국가의식 보장, ③ 정보 보안과 효용에 관한 조항을 포함한 클라우드컴퓨팅 아웃소싱 계약 마련, ④ 클라우드 계약의 규제조건 반영 보장, ⑤ 대역폭의 비용감소와 접근 속도 증폭을 위해 아프리카에 정보 중심가 설립, ⑥ 서비스가 빠르고 자동화되었으며 보안이 잘 되어 있고 생태학적으로 바람직한 정보 중심 보장, ⑦ 정보보호 관련법과 같은 규제의 도입 및 개선, ⑧ 훈련 프로그램 도입, ⑨ 클라우드 표준 규정 계획 수립의 수용을 통한 국경 외 표준규정 및 규제를 보장할 것을 권장하고 있다.²⁸⁾

한편, 마드리드 결의안에 언급된 개방 원칙에 의하면, 개인정보처리에 관하여 책임이 있는 모든 사람은 투명하게 처리하여야 한다고 밝

28) <https://itunews.itu.int/En/3414-Regulation-in-the-cloud.note.aspx>(2016. 8. 2 최종접속)

히고 있는데, 이와 관련해서는 정보 처리과정에 대한 설명이 그 첫 번째 단계이다. 이것은 평가위험과 적당한 수준의 보안을 입증하기에 필수적이다. 다음에 제시하고 있는 정보흐름표는 감사, 위험평가, 인증과 관련하여 프라이버시 컨트롤 시행에 책임이 있는 정보 관리자들에게 매우 유용한 도구이다. 이 표는, 정보의 생활주기 단계를 따르고 있다. 예컨대, 수집, 이동, 활용, 저장, 공유 그리고 개인식별정보 (personally identifiable information ; PII) 처리가 있다. 이것은 개인 정보의 유형, 처리하는 사람, 운영되는 플랫폼, 처리되는 어플리케이션, 처리의 목적, 보안 방법, 저장 가능한 기간, 개인정보를 수신하는 주체와 저장될 장소 등의 정보를 포함한다.²⁹⁾

<표-1> 데이터 흐름 예시

정보유형
개인정보 처리 자격을 갖춘 자
운영되는 플랫폼
처리되는 어플리케이션
정보 처리의 목적
보안방법
저장기한 및 처리의 목적
정보 수신주체
외국으로 정보가 이동되는 경우 보내지는 국가 통지

출처 : ITU, 『Privacy in Cloud Computing』, 2012. 3, p.11.

29) ITU, 『Privacy in Cloud Computing』, 2012. 3, p.11.

(2) 경쟁 및 소비자 분야의 규제

클라우드컴퓨팅 서비스는 경쟁분야에서도 고려할 사항을 가지고 있다.

클라우드컴퓨팅의 인프라 서비스(IaaS)모델³⁰⁾에서는 클라우드 서비스 제공자가 관련시장에서 자신의 지위를 유지하기 위한 목적으로 응용소프트웨어 제공자에게 자신의 클라우드 인프라에 대한 접근을 거절하였는지에 따라 시장지배적 지위의 남용이 있었는지가 결정된다고 하였다.³¹⁾

한편, 소프트웨어 서비스(SaaS),³²⁾ 플랫폼 서비스(PaaS)³³⁾에서는 저작권에 대한 라이선스 거절이 시장지배적 지위의 남용으로 인정될 수 있다고 하였다.³⁴⁾

이에 관한 한 예로, 미국의 소송 사례 중 구글 v. 미국 내무성 사례를 살펴 볼 수 있다. 2010년 10월 구글은 미국 내무성을 상대로 ICT 서비스에 대한 (미화)5천 9백 만 달러짜리 계약 내 메시지 전송 기술

30) 서비스로서의 인프라스트럭처라는 의미로, 가상화된 인프라 환경만을 사용할 수 있도록 하는 서비스다. 기업의 환경에 의해 표준화된 솔루션을 사용하지 못할 때 제시된다. 이는 직접 서버에 서비스를 구성하는 것과 같이 가상 서버에 서비스를 구성하고 관리한다.

<http://terms.naver.com/entry.nhn?docId=20154&cid=43659&categoryId=43659>, 2016. 9. 4. 최종접속.

31) 박영규, 앞의 논문, 198쪽.

32) 소프트웨어의 기능 중 유저가 필요로 하는 것만을 서비스로 배포해 이용이 가능하도록 한 소프트웨어의 배포형태이다. 서비스형 소프트웨어로도 불린다. 유저는 필요한 기능만을 필요할 때에 이용할 수 있으며, 이용하는 기능만큼만 요금을 지불한다.

<http://terms.naver.com/entry.nhn?docId=20139&cid=43659&categoryId=43659>, 2016. 9. 4. 최종접속.

33) 서비스로서의 플랫폼이라는 뜻으로, 표준화된 플랫폼을 제공하는 서비스다. 이는 가상화된 하드웨어와 소프트웨어 등을 필요에 따라 제공하며, 모든 개발과 관련된 환경 및 프로세스를 제공한다.

<http://terms.naver.com/entry.nhn?docId=20155&cid=43659&categoryId=43659>, 2016. 9. 4. 최종접속.

34) 박영규, 앞의 논문, 199쪽.

을 마이크로 소프트 비즈니스 생산성 온라인 세트에 기반을 두어야 한다고 요구함으로써, 공공 조달업무에서 구글을 배제하고, 이에 따른 정당한 경쟁을 할 수 없도록 공공조달업무가 불법적으로 방해했다며 소송을 제기하였다. 이에 법원은 구글에 유리한 임시처분 결정을 내렸으며, 미 내무성의 공공 조달업무가 독점거래법 위반이므로 업무 기준을 변경하라고 판결했다. 마이크로 소프트 측의 부정행위나 정직하지 않은 행위에 대한 문제는 없었음에도 불구하고, 판결은 미 내무성에서 마이크로소프트 비즈니스 생산성 온라인 서비스 클라우드컴퓨팅 솔루션과 이메일 시스템을 몰아내는 결과를 가져왔다. 판결의도는 락인(Rock-in ; 기존 시스템에서 기술전환을 하지 못하는 상태)효과를 피하고, 가치분 없이 공정 경쟁구조의 방해물을 제거하며, 내무부 이메일 시스템의 최종 이전에 대한 발의와, 마이크로소프트의 ‘구조적 락인’ 달성, 그리고 구글이 경쟁할 수 있는 기회비용 등이다. 법원은 공공조달에서 마이크로소프트를 선호함으로써 인해 생산된 네트워크 효과에서 비롯된 경쟁과 그 대상들에게 돌아갈 수 있는 손해를 고려했다.³⁵⁾

한편, 클라우드컴퓨팅에 관련한 경쟁 이슈에 대해서 ITU는 2016년에 발표한 보고서에서 IoT 관련 규제 변화를 예상하고 여러 기준에 따라 정리하고 있다. 이 보고서에서는 라이선싱과 스펙트럼 관리, 스윙칭과 로밍, 접속과 넘버링, 경쟁, 개인정보보호와 보안의 5가지 분야로 구분하여 기준을 제시하고 있으나³⁶⁾ 이 보고서와 관련이 있는 경쟁, 개인정보와 보안 분야만을 소개하면 아래와 같다.

35) ITU, 「GSR 2012 Discussion Paper Demystifying Regulation in the Cloud : Opportunities and Challenges for Cloud Computing」, 2012. 10. 19, p.8.

36) ITU, 「Trends in Telecommunication Reform 2016」, 2016, p.91.

<표-2> 잠재적 IoT 규제 기준³⁷⁾

경쟁	<ul style="list-style-type: none"> - 경쟁 및 소비자 법을 통해 정보의 상호운용성을 향상시키고 개인 정보에 쉽게 접근할 수 있는 권한을 사용자에게 부여 - 글로벌 표준화를 지원하고 거대한 사물통신(M2M) 경쟁을 위해 원격으로 제공된 공용정보관리시스템(SIMs)의 배포
개인정보 보호와 보안	<ul style="list-style-type: none"> - IoT 시스템을 위한 하드웨어 및 소프트웨어 보안과 개인정보 보호 메커니즘의 R&D, 특히 자원이 부족한 신생기업 그리고 개인기업을 위해 이 기능을 보다 쉽게 개발하기 위한 R&D - IoT 개인정보의 사용과 수집의 동의서 확보의 투명성 개선을 위한 새로운 메커니즘 개발을 위한 기업 인센티브 - 조직구축과 IoT시스템의 환경설정을 통한 대규모 개인정보의 사용 영향평가 - IoT시스템에서의 정보 최소화와 목적제한 원칙에 관한 글로벌 개인정보 규제기관의 적용을 기반으로 한 추가지침의 개발 - 통신 및 기타 규제기관(개인정보보호, 정보보호 기구 등) 간의 더 많은 협력

출처 : ITU, 「Trends in Telecommunication Reform 2016」, p.91

규제기관은 시장의 효율성과 공공의 이익증진을 위하여 IoT의 개발과 적용을 장려하는 역할을 할 수 있다는 것을 설명하면서 특히, 경쟁규제기관은 시장경쟁과 신속한 혁신을 촉진하기 위한 지배적 지위 남용의 조사와 경쟁 모니터링이 필요하다고 하였다.³⁸⁾ 또한, 규제기관은 IoT 개인정보보호와 보안 쟁점들에 대한 특별한 주의를 통하여 공공의 신뢰와 기술적용을 장려할 수 있도록 해야 함을 강조하였다.³⁹⁾

37) 이 표는 ITU, 「Trends in Telecommunication Reform 2016」, p.91의 표 중 일부를 발췌하여 정리한 것임.

38) ITU, 「Trends in Telecommunication Reform 2016」, p.92.

39) *Id.*

많은 통신규제기관이 네트워크 보안에 관한 책임을 가지고 있지만, 신뢰할 만한 IoT 개발 촉진을 위해서는 국가의 개인정보보호 및 소비자보호 규제당국과 더 많은 협력이 필요한 영역이라는 것이다.⁴⁰⁾

이러한 논의와 관련하여 개별 국가의 소비자보호법 분야에 대해서도 클라우드와 같이 이전의 제품이나 서비스로부터 디지털 정보나 서비스로 바뀌어가는 사회적 분위기를 반영하기 위해서 이를 개선하거나 조정되어야 할 필요가 있는 것으로 지적되었다. 소비자보호법을 통하여 시장개방이 가능하도록 하고 경쟁방식이 유지되는 것이 가능하게 한다. 또한, 소셜 네트워크와 같은 역할을 하는 클라우드 서비스들은 많은 이용자들이 사회와 경제활동에 활용하게 될 것이며, 많은 이용자들이 사용하게 되는 새로운 데이터 취급방식으로서 서비스 개발자 및 시장 개발자들이 인식하게 될 것이다.⁴¹⁾

이러한 인식에 따라 발생할 수 있는 여러 가지 문제들에서 소비자의 이익을 보호하기 위하여 소비자 보호당국이 개입해야 한다는 주장이 있다.⁴²⁾ 이에 대한 예시를 보면 영국의 광고자율심의기구(특정 사용자가 서비스를 이용할 수 없도록 서버수용력이 제한된 상황에서 클라우드를 호스팅하는 제공자가 '무제한 패키지'라고 허위 광고한 경우 제공자에게 불리한 판결을 내린 바가 있다.⁴³⁾ 이와 비슷하게, 한 웹 호스팅 회사는 3개월 이내 3번의 중대한 네트워크 문제가 발생한 것을 소비자에게 명확하게 밝히지 않고 '99.99 가동시간 보장'이라고 주장한 것에 대하여 허위 광고한 것으로 판결이 났다.⁴⁴⁾ 반면, 프랑스 법원은 페이스북 사용자가 페이스북 표준용어규정에 적힌 분쟁처리

40) *Id.* p.93

41) ITU, 「GSR 2012 Discussion Paper Demystifying Regulation in the Cloud : Opportunities and Challenges for Cloud Computing」, 2012. 10. 19, p.7

42) *Id.*

43) *Id.*

44) *Id.*

조항에 따를 의무가 없는 것으로 판결을 내렸는데, 이 표준용어규정에서는 모든 법적 분쟁이 미국의 산타클라라 카운티에 위치한 주법원 혹은 연방법원에서만 제기될 수 있다고 적혀 있었다. 프랑스 법원은 이러한 조항이 강제권을 가지기엔 사용자들에게 충분히 인지되거나 이해되지 않았으며, 이는 프랑스 민사소송 절차법에 어긋난다고 설명했다.⁴⁵⁾

3. 정보보안에 관한 검토

(1) 표준화 논의

클라우드컴퓨팅에 대한 해킹 등 불법적인 파괴나 변형, 허가되지 않은 정보의 공개나 접근에 대해 적절한 보안조치를 사전에 시행해야 한다는 점은 주지된 사항이다. 다만, 적절한 보안조치의 수준을 상정하는 기준이 국가별로 달라질 수 있다. 이러한 문제를 해결하기 위하여 국제표준화기구의 ISO27001⁴⁶⁾을 사용하도록 하고, 우리나라 기업의 경우에도 이 표준을 획득하여 사용하고 있다.⁴⁷⁾ 그럼에도 불구하고 현재 사용되고 있는 국제표준이 클라우드컴퓨팅의 보안을 확보하는 적절한 수준의 보안조치에 해당하는지에 대해서는 해당 수준에 미치지 못한다는 분석이 있다.⁴⁸⁾

45) *Id*

46) 국제표준화기구 (ISO : International Organization for Standardization) 및 국제전기기술위원회 (IEC : International Electrotechnical Commission)에서 제정한 정보보호 관리체계에 대한 국제 표준이자 인증이다. 정보보호정책, 보안정책, 위협관리 등 정보보안 관련 11개 영역, 133개 통제항목에 대한 심사와 검증을 통과해야 인증을 얻을 수 있다.(한경 경제용어사전,

<http://terms.naver.com/entry.nhn?docId=2075491&cid=42107&categoryId=42107> 2016. 8. 17. 최종접속)

47) 우리나라 기업의 ISO27001 획득에 관한 기사 참조

(http://news.inews24.com/php/news_view.php?g_serial=970491&g_menu=020800&rrf=nv 2016. 8. 17 최종접속)

48) ITU, 「Privacy in Cloud Computing」, 2012. 3, p.12.

<표-3> 클라우드컴퓨팅 보안 및 개인정보 이슈

구 분	내 용
Governance	클라우드 환경에서 정책, 절차 및 표준과 관련된 거버넌스 수립 뿐 아니라 설계, 구현, 테스트, 사용 및 서비스 적용, 모니터링에 대한 통제 도구 마련
Compliance	개인정보보호에 대한 법과 규제 준수
Trust	서비스 제공자는 보안과 개인정보보호에 대하여 높은 수준의 통제 및 절차의 투명성을 제공
Architecture	클라우드 서비스에 대한 소프트웨어 및 하드웨어 전체에 대한 구성요소와 관련된 보안 및 개인정보보호 통제 기술
Identity and Access Management	민감한 정보와 개인정보 접근에 대한 인증, 접근통제를 위한 보호조치
Software Isolation	클라우드 환경의 가상화 및 소프트웨어 격리
Data Protection	클라우드 서비스 제공자의 데이터 관리에 대한 적합성
Availability	서비스 거부 공격, 장애, 자연재해, 취약점 등에 대하여 서비스 가용성 보장을 위한 방안
Incident Response	클라우드 사업자는 침해사고 확인, 분석, 대응, 데이터 수집 및 보존 등에 대한 절차 마련

출처 : 유우영 · 임종인, “클라우드컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구”, 정보보호학회논문집 제22권 제2호, 2012. 4, 339쪽.

이러한 문제에 관하여 ITU 전권 회의(International Telecommunication Union Plenipotentiary Conference) 결의130에서는 정보와 소통기술의 이용에 관한 보안과 기밀성 유지를 위해 ITU가 하는 역할 강화에 대한

문제를 다루었다. 여기에는 스팸, 맬웨어(malware) 등 개인 정보보호와 프라이버시와 관련한 문제의 해결 방법과 안정성이 포함되며 클라우드 솔루션의 정보처리 상호운용성을 개선하기 위해서는 필수적으로 표준을 정해야만 한다고 주장하였다.⁴⁹⁾

세계표준협력회의(Global Standards Collaboration ; GSC)는 국가 간 표준화가 아닌 범세계적 표준화를 위해 GSC 용어와 용어의 정의, 구성과 과정의 표준화가 국가나 지역 단위의 우려를 동일하게 반영하고 의미 있는 대화를 하기 위해 필수적이라고 결론지었다. 덧붙여 이러한 표준화 과정은 일관성 있고 효율적인 연구영역을 포함 할 필요가 있고, 개인정보보호법 범위 내에 있는 활동들에도 표준규정을 적용해야 한다고 설명하고 있다.⁵⁰⁾

기본적으로 클라우드컴퓨팅 서비스는 이용자의 이용편의를 위하여 쉽게 구성되어야 한다. 클라우드컴퓨팅 서비스 공급자와 서비스 개발자가 개입되어 있는 경우에도 이용의 편의성이 도모되어야 함은 다르지 않다. 따라서 표준방식의 도입은 클라우드컴퓨팅의 광범위한 구성원들 간 상호운용이 용이하도록 하는 하나의 해결책이 될 수 있을 것이다.

그러나 이와 같은 문제점의 인식에도 불구하고 클라우드컴퓨팅의 개별적인 표준지침은 개발되어 있지 않은 상황이다.

다만 2010년 4월 이후 ITU에서 ‘통신 영역에서의 클라우드컴퓨팅 보안 가이드라인(Security guideline for cloud computing in telecommunication area)’, ‘클라우드 기반의 원격통신 서비스 환경의 체제와 보안에 필요한 요건들(Security requirements and framework of cloud based telecommunication service environment)’, ‘통신조직을 위한 개인정보 관리 지침(Guideline for management of personally identifiable information

49) ITU, 「Privacy in Cloud Computing」, 2012. 3, p.10

50) *Id.*

for telecommunication organizations)’ 등의 작업이 진행되고 있으므로 이를 기대해 볼 만 하다.⁵¹⁾

(2) 보안의무와 방법

데이터 보안의 의무를 지는 주체에 대한 검토도 필요할 것이다. 클라우드컴퓨팅의 보안문제 발생시에 위반통지 의무는 기본적으로 제공자에게 있다. 즉, 제공자는 관련 국내 규제기관에 이를 통지할 의무를 가지며(부문적이던 수직적이던) 클라우드 사용자가 보안상의 중대한 위반으로 인해 사용자 데이터 보안에 직·간접적인 영향을 주는 경우에 한하여 사용자 또한 동일한 의무를 가진다.⁵²⁾

따라서 클라우드 서비스를 위한 개인정보에 접근할 수 있는 취급자를 가장 최소한으로 유지하도록 하고 그 과정에서 데이터 관리자와 처리과정에 연루된 모든 이들에게는 개인정보 기밀성을 유지할 의무가 주어지는 것으로 판단하여야 한다.

또한, 클라우드에 저장된 정보는 클라우드 내의 정보처리 암호화를 통해 높은 수준의 보안이 보장되어야 한다. 암호화는 정보의 기밀성을 보장하는 것으로 보안 전문가들로부터 인정받는 매우 기본적인 방식이다.⁵³⁾

보안에 관한 조직으로 클라우드 보안연합(Cloud Security Alliance ; CSA)이 있는데, 여기에서는 클라우드컴퓨팅의 보안에 관한 모범사례를 홍보하고 교육하는 업무를 하고 있으며, CSA 내에 9개의 연구그룹을 두고 각 분야별 해결 지침을 제공하고 있다. 특히, 정보관리와 보안, 데이터 센터 운영과 사고대응 등의 그룹의 지침은 향후 클라우드컴퓨팅에 관한 보안지침 수립에 많은 참고가 될 수 있을 것이다.⁵⁴⁾

51) ITU, 「Privacy in Cloud Computing」, 2012. 3, p.14.

52) ITU, 「GSR 2012 Discussion Paper Demystifying Regulation in the Cloud : Opportunities and Challenges for Cloud Computing」, 2012. 10. 19, p.16.

53) ITU, 「Privacy in Cloud Computing」, 2012. 3, p.13.

54) ITU, 「Privacy in Cloud Computing」, 2012. 3, p.16 참조.

클라우드와 관련하여 클라우드 서비스 제공자들이 도입하고 따를만한 기존의 보안기준에는 정보보안시스템을 위한 ISO/IEC 27001나 SAS7078 같이 외부감사와 증명을 요구하는 것들이 있다. ITU-T에서는 연구조직17이 지난 2010년 4월부터 클라우드 보안과 관련하여 계정관리를 포함한 다양한 분야에서의 필요조건과 지침들을 개발하기 위해 연구해왔다. 여기에서는 각국의 규제기관에서 요청된 감사권이나 책임실행이 클라우드 환경에 내포되어야 할 필요성을 포함하여, 회계서비스 부문이나, 정보보호당국처럼 그에 준하는 부문을 모두 포함하여 모든 클라우드 사용자가 대상이 되는 규제에 대한 것을 다루고 있다.⁵⁵⁾

그 밖에도 개인정보 보호를 위하여 우선적으로 개인정보 보안에 관한 위기평가 기준을 수립하는 방안을 고려할 수 있을 것이며, 기본적으로는 수집되는 정보가 최소한으로 하고 특히 민감한 개인정보의 경우 보안을 더욱 강조하여야 할 것이다.

제 3 절 우리나라의 클라우드컴퓨팅 정보보호 관련 법제

1. 클라우드컴퓨팅법의 개인정보 관련 입법

「클라우드컴퓨팅법」 제4조(다른 법률과의 관계)에서 “이 법은 클라우드컴퓨팅의 발전과 이용 촉진 및 이용자 보호에 관하여 다른 법률에 우선하여 적용하여야 한다. 다만, 개인정보 보호에 관하여는 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등 관련 법률에서 정하는 바에 따른다”고 규정하여 클라우드컴퓨팅에 있어서도 개인정보 보호에 관해서는 기존의 개인정보에 관한 일반법에 해당하는 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 규정이 적용됨을 밝히고 있다.

55) ITU, 「GSR 2012 Discussion Paper Demystifying Regulation in the Cloud : Opportunities and Challenges for Cloud Computing」, 2012. 10. 19, p.14

이와 같이 규정함으로서 중복적인 입법을 방지하고자 하였으며, 유사한 규제를 내용으로 하는 조문이 여러 법에 존재하여 적용상의 우선순위의 논란도 사전에 예방되도록 하였다. 따라서 「클라우드컴퓨팅법」내에 개인정보보호에 관한 조문은 많이 포함되어 있지 않다.

한편, 국내의 정보보호 관련 법제에서는 외국계 클라우드 관련 정보보호 규정을 두고 있지 않으며,⁵⁶⁾ 「클라우드컴퓨팅법」에서도 해외 서버에 대한 정보보호 규정을 별도로 두지 않고 있다.

이와 관련하여 기존의 개인정보 관련 국외이전에 관한 사항은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제24조의2, 제25조, 제63조에 따라 제3자에게 업무를 위탁하거나 국외 이전시에는 이용자의 동의를 받고 별도의 보호조치를 하도록 규정하였다.

「클라우드컴퓨팅법」

제26조(이용자 보호 등을 위한 정보 공개) ① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

② 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제2호에 따른 정보통신서비스를 말한다. 이하 제3항에서 같다)를 이용하는 자는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제3호에 따른 정보통신서비스 제공자를 말한다. 이하 제3항에서 같다)에게 클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

③ 미래창조과학부장관은 이용자 또는 정보통신서비스 이용자의 보호를 위하여 필요하다고 인정하는 경우에는 클라우드컴퓨팅서비스 제공자 또는 정보통신서비스 제공자에게 제1항 및 제2항에 따른 정보를 공개하도록 권고할 수 있다.

④ 미래창조과학부장관이 제3항에 따라 정보를 공개하도록 권고하려는 경우에는 미리 방송통신위원회의 의견을 들어야 한다.

56) 박종수, 위의 논문, 58쪽.

다만 「클라우드컴퓨팅법」 제26조에서 위와 같이 규정하여 이용자 정보가 저장되는 국가의 명칭을 공개될 수 있는 근거규정을 마련하였을 뿐, 강행규정으로 이를 강제하고 있는 것도 아니다.

개인정보와 관련한 분쟁이 발생하였을 경우 데이터에 대한 통제권의 행사를 위해서나 재판관할권과 관련한 문제까지도 데이터 저장의 위치와 관련된다.⁵⁷⁾

그 밖에 계약 종료시의 개인정보 파기에 대해서는 제27조 제3항부터 제6항까지에서 규정하고 있다.

「클라우드컴퓨팅법」

제27조(이용자 정보의 보호)

(생략)

③ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.

④ 클라우드컴퓨팅서비스 제공자는 사업을 종료하려는 경우에는 그 이용자에게 사업 종료 사실을 알리고 사업 종료일 전까지 이용자 정보를 반환하여야 하며 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 사업 종료일 전까지 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.

⑤ 제3항 및 제4항에도 불구하고 클라우드컴퓨팅서비스 제공자와 이용자 간의 계약으로 특별히 다르게 정한 경우에는 그에 따른다.

⑥ 제3항 및 제4항에 따른 이용자 정보의 반환 및 파기의 방법·시기, 계약 종료 및 사업 종료 사실의 통지 방법 등에 필요한 사항은 대통령령으로 정한다.

57) 유우영·임종인, “클라우드컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구”, 정보보호학회논문집 제22권 제2호, 2012. 4, 343쪽.

한편, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 ‘정보통신망법’이라 함)」 제63조에서는 국외이전 개인정보의 보호에 관하여 이용자의 사전 동의를 받도록 하고 있으며, 이 법을 위반하는 내용으로 국제계약을 체결하지 못하도록 하고 있다.

이와 함께 「정보통신망법 시행령」 제67조 제1항에서는 개인정보 국외 이전시 보호조치로 「정보통신망법」 제15조에 따른 개인정보보호를 위한 기술적·관리적 조치, 개인정보 침해에 대한 고충처리 및 분쟁 해결에 관한 사항, 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치를 정하고 있으며, 같은 조 제2항에서 정보통신서비스 제공자들은 제1항에서 정한 사항을 개인정보를 국외에서 이전받는 자와 미리 협의하고, 이를 계약내용 등에 반영하도록 정하고 있다.

그리고 같은 법 제62조 국제협력 조항에서는 정부가 개인정보의 국가간 이전 및 개인정보의 보호에 관련된 업무를 추진할 때 다른 국가 또는 국제기구와 상호 협력하여야 한다고 규정하고 있다.

그런데 이와 유사한 취지의 규정이 「개인정보 보호법」에서도 규정되고 있는데, 제17조 제3항에서 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다고 규정하고 있다. 또한, 같은 법 제14조 제2항에서는 정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하도록 규정하고 있다.

2. 클라우드컴퓨팅 보안 관련 입법

「클라우드컴퓨팅법」에서 보안에 관한 규정으로는 제23조의 신뢰성 향상에 관한 규정을 들 수 있는데, 여기에서는 클라우드컴퓨팅 서비스 제공자는 클라우드컴퓨팅 서비스의 품질·성능 및 정보보호 수준을 향상시키기 위하여 노력하여야 한다고 하였으며, 미래창조과학부장은 클라우드컴퓨팅 서비스의 품질·성능에 관한 기준 및 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함한다)을 정하여 고시하고,⁵⁸⁾ 클라우드컴퓨팅 서비스 제공자에게 그 기준을 지킬 것을 권고할 수 있다고 규정하고 있다(「클라우드컴퓨팅법」 제23조 제1항, 제2항).

뒤에서 설명하는 표준계약서나 개인정보의 해외이전규제에 관한 조문과 마찬가지로 보안 관련 조문에 해당하는 제23조에 대해서도 역시 권고규정으로 입법한 것은 이 법의 성격과 산업의 발전에 오히려 부작용을 끼치는 것은 아닌지, 지나친 사업자 입장을 고려한 입법은 아닌지 재검토해 볼 필요가 있을 것이다.

그 밖에 「클라우드컴퓨팅법」 같은 조에서는 미래창조과학부장이 제23조 제2항에 따라 클라우드컴퓨팅 서비스의 품질·성능에 관한 기준을 고시하려는 경우에는 미리 방송통신위원회의 의견을 들어야 한다고 정하고 있는데(클라우드컴퓨팅법 제23조 제3항) 이는 클라우드컴퓨팅이 어느 한 부처의 업무 영역이 아니라 정보통신분야에 널리 적용되기 때문인 것으로 판단된다. 다만, 업무협의를 거치는 등의 보다 적극적인 협조의 형태로 규정되지 않고 의견을 듣는 수준으로 규정한 것에는 아쉬움이 남는다.

58) 2016년 4월 4일 미래창조과학부 고시로 「클라우드컴퓨팅서비스 정보보호에 관한 기준」이 제정되었다. 모두 8개 조문으로 구성되어 있으며, 제3조부터 제6조까지는 각 정보보호 조치에 따른 구체적인 세부 기준을 별표로 규정하고 있다.

한편, 클라우드컴퓨팅의 기술이나 서비스의 표준화에 관련한 규정으로 「정보통신 진흥 및 융합 활성화 등에 관한 특별법(이하 ‘정보통신융합법’이라 함)」 제16조의 ‘기술·서비스 등의 표준화’ 규정을 볼 수 있다. 이 규정에서는 미래창조과학부장관이 정보통신 진흥 및 융합 활성화를 위하여 정보통신융합등 기술·서비스 등의 표준화에 관하여 ① 신규 정보통신융합등 기술·서비스 등 관련 표준의 제정·개정 및 폐지와 그 보급, ② 신규 정보통신융합등 기술·서비스 등 관련 국내외 표준의 조사·연구개발, ③ 그 밖에 신규 정보통신융합등 기술·서비스 등의 표준화에 필요한 사항에 해당하는 사업을 추진할 수 있도록 하였다. 또한, 미래창조과학부장관은 민간부문에서 추진하는 정보통신융합등 기술·서비스 등의 표준화 사업에 대한 지원을 할 수 있도록 하였다(제16조 제2항).

제 4 절 소결 : 시사점

클라우드컴퓨팅 관련 개인정보의 보호와 보안 관련 EU에서의 규제 추이는 기존의 EU의 정보보호지침에서 유럽연합 밖에서 정보를 수집, 처리 및 저장하는 것을 원칙적으로 금지⁵⁹⁾하는 조치를 취하고 있는 것과는 다른 형태로 나타나고 있다. 이는 앞서 설명한 클라우드컴퓨팅의 특성인 인터넷을 기반으로 자유로운 정보의 이용, 서비스 제공을 고려한다면 당연한 결과이다. 우리나라의 경우에도 동일한 문제를 안고 있다. 클라우드컴퓨팅의 특성에 비추어보아도 우리나라 영토 내에서만 서버를 두도록 하여 제한하는 것은 불가능한 것이다.

EU의 경우 회원국 내에서의 규제수준 평준화를 위해 이미 오랫동안 그 작업을 하여왔기 때문에, 여러 국가의 규제수준의 평준화가 선결문제로 제시되고 있는 클라우드컴퓨팅의 경우에도 EU의 움직임을 고려하는 것은 유의미할 것으로 판단된다.

59) 박종수, 앞의 논문, 63쪽.

따라서 앞에서 클라우드컴퓨팅에 관한 EU의 규제동향을 검토하였는데, 가장 핵심적인 사항은 유럽연합 회원국들도 회원국 시민의 개인정보 역외이전을 원칙적으로 금지하고 있으나, EU 집행위원회가 개인정보 보호수준이 적정하다고 판정한 국가의 기업에 한하여 역외이전을 허용하고 있다는 것이다.⁶⁰⁾

EU의 이러한 정책에 따라 2015년 우리 정부는 우리나라 기업들이 EU 회원국에서 영업활동에 필요한 개인정보를 국내로 전송하여 처리해야 할 경우, EU 회원국과 사전에 국외이전 계약을 체결하고 회원국별 감독기구의 규제심사를 거쳐야 하는 불편과 경제적 손해를 해소하고자 EU 집행위원회에 「EU 개인정보 보호수준 적정성 평가」⁶¹⁾를 신청할 예정이라고 밝히고 있다.⁶²⁾

우리나라가 「EU 개인정보 보호수준 적정성 평가」 승인을 받으면 EU에 진출한 국내 기업들은 개인정보 보호와 관련해 EU 기업과 동일한 조건에서 영업 활동이 가능해지고, 추가 절차 없이 EU 시민의 개인정보를 우리나라로 이전하여 활용할 수 있게 되는 것이며,⁶³⁾ 이를 통하여 개인정보의 역외 이전을 특성으로 하는 클라우드컴퓨팅 산업에도 긍정적인 영향을 미칠 것으로 전망된다.

60) 행정자치부 보도자료, 2015. 12. 15. 1쪽.

(http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_0000000008&nttId=47865), 2016. 8. 3. 최종방문.

61) 이 평가는 OECD의 개인정보원칙을 반영하여 EU에서 제정한 개인정보보호지침에 따른 평가를 말하는 것이며, 우리나라의 개인정보보호법은 이미 OECD의 기준을 충족하고 있다. 행정자치부 보도자료, 2015. 12. 15. 4쪽 참조.

(http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_0000000008&nttId=47865), 2016. 8. 3. 최종방문.

62) 행정자치부 보도자료, 2015. 12. 15. 1-2쪽.

(http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_0000000008&nttId=47865), 2016. 8. 3. 최종방문.

63) 행정자치부 보도자료, 2015. 12. 15. 2쪽.

(http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_0000000008&nttId=47865), 2016. 8. 3. 최종방문.

이러한 제도를 반대로 적용해 보는 것은 어떤가. 클라우드컴퓨팅에 관해서는 우리나라가 최초의 입법을 하는 등 제도적 정비가 빠른 상황이고, IT분야에서는 가장 빠른 발전 속도를 보이고 있다고 본다면 우리나라에서도 EU에서와 같은 개인정보 보호수준의 적정성에 관한 구체적인 기준을 세우고 이를 충족하는 법제를 갖춘 국가에 대해서만 우리 국민의 개인정보를 이전, 활용이 가능하도록 하는 방안을 고려해 볼 수 있을 것이다.

또한, 다른 측면에서 보면, 우리나라의 「클라우드컴퓨팅법」의 개인정보, 보안 관련 규정에서는 개인정보 관리주체인 서비스 제공자의 정보나 개인정보의 저장위치 등에 대한 이용자의 알 권리를 보호하기 위한 취지의 규정을 두고 있으나 이들 조문은 선언적 규정으로 권고적인 성격을 가지는 것에 그치고 있다.

클라우드 서비스 제공자가 이용자에게 데이터가 저장되는 위치를 고지하도록 한 것은 이미 입법되어 있다. 다만, 데이터가 저장될 수 있는 위치가 여러 곳이고, 이 중 선택하여 자신의 데이터를 저장할 수 있는 경우에 이용자가 자신의 데이터를 저장할 위치를 선택할 수 있도록 정보를 제공하고 결정권을 행사할 수 있도록 하여야 한다.

물론 이 경우 해당 서버가 위치하고 있는 국가의 개인정보 처리에 관한 기본적인 조건들을 사전에 비교할 수 있도록 제공한 후 결정할 수 있도록 하면 더욱 바람직할 것이다.

이 경우 이용자는 정보보호의 법제 수준이 국가별로 다르기 때문에 자신의 정보를 어느 국가의 서버에 저장하여 서비스를 이용할 것인지 결정할 수 있게 될 것이다.

한편, 선진국과 개발도상국의 기술의 차이뿐만 아니라 개인정보·보안에 관한 수준의 차이로 인한 문제도 있는데, 이를 ITU의 ‘커넥트 2020 어젠다’에서는 디지털 격차로 표현하고 정보의 접근성을 높이도록 해마다 목표치를 제시하고 있다.⁶⁴⁾

64) 이에 관한 상세는 별첨한 참고자료 ‘커넥트 2020 어젠다’ 참조.

이와 유사한 취지로 Business Software Alliance가 2012년 2월에 발표한 보고서에서도, 개인 정보보호를 위한 적절한 법에 관련하여 개발도상국과 선진국가 사이에 큰 차이가 있음을 설명하고 있다.⁶⁵⁾

이 보고서는 선진국가들 간에도 국외로의 개인 정보 이동에 방해가 되는 정보보호 규제로 인한 갈등이 있다는 것을 강조했다. 예를 들자면, 몇 선진국가들은 국가 내 로컬기업에게만 클라우드 서비스 조항을 제한하는 것을 고려하고 있다. 국제적인 접근은 복합적인 정보 보호 제도의 합의와 제공자들 위한 비즈니스 법과 시민들을 위한 보호법의 조화를 위해 꼭 필요한 접근이다. 국가 정책에 국제적인 수준의 조정이 없다면, 정보이동과 국가간의 자유로운 소프트웨어 서비스 이동이라는 클라우드의 큰 이점과 효율성이 이루질 수 없을 것이다.⁶⁶⁾

결국 이상에서의 논의를 종합하면, 이제 클라우드컴퓨팅을 포함한 정보통신 분야의 발전은 어느 한 국가 내에서 개발·발전되는 것을 전제로 할 수 없기 때문에 국가별 기술이나 보안의 수준뿐만 아니라 이를 운영하는 법제도의 평준화, 개발도상국의 접근성 향상이 필수적인 상황이며, 이에 관한 국가간의 지속적인 논의와 제도로의 수렴이 요구된다 할 수 있다.

따라서 어느 한 국가만의 선제적인 입법 보다는 공통적인 대응이 더욱 강하게 요구된다 할 수 있으므로 우리나라의 경우에도 국내의 입법 정비에 치중하기 보다는 다른 국가와의 법제도 평준화 특히, 우리나라 보다 정보통신 수준이 하위에 있으나 우리 국민이나 기업의 접근·교류 빈도가 높은 국가와의 법제도 수준의 조화 또는 필요한 경우 우리나라의 지원 노력이 필요할 것이다.

65) <http://cloudscorecard.bsa.org/2012/>;ITU, 「Privacy in Cloud Computing」, 2012. 3, p.8. 재인용

66) <http://cloudscorecard.bsa.org/2012/>;ITU, 「Privacy in Cloud Computing」, 2012. 3, p.8. 재인용

제 3 장 클라우드컴퓨팅 계약 관련 이용자 보호

제 1 절 쟁점 검토

일반적으로 클라우드컴퓨팅 사용자들은 클라우드컴퓨팅 계약과 관련한 사안들 중 직간접적 책임과 안정성에 대한 불이행, 데이터 보전, 신뢰성 또는 서비스에 대한 연속성, 서비스에 문제가 생겨 꺼지거나 데이터가 사라졌을 때 복원, 공급자와의 계약 체결 이후에 발생하는 일방적인 계약 수정, 계약 만료와 그것에 따른 영향, 데이터 저장의 제약 등 여러 가지 문제들에 대해 우려한다.

클라우드컴퓨팅은 서비스 제공에 관한 계약을 체결하여 이용하게 될 것인데, 이와 관련하여 서비스 제공자와 이용자 간에 위와 같은 문제가 발생하게 될 여지가 있다는 것은 일반 계약들에서 나타난 기존의 문제에 비추어 보면 예상이 가능하다.

그런데, 국가별 계약법제에 따르는 기존 규제 환경은 클라우드 기반 서비스에 적합하지 않을 수 있다는 문제가 있다.

클라우드컴퓨팅 서비스의 지역 제한이 없기 때문에 다양한 국가의 이용자가 있을 것이고 이들 이용자는 각 국가별 계약법제를 인식의 기반으로 하여 클라우드컴퓨팅 서비스를 이용하게 될 것이다. 따라서 클라우드컴퓨팅 서비스 제공자의 경우에도 여러 국가의 법을 적용 받아 운영해야 하는 경우가 발생할 수 있다. 이 경우 각 국가별 계약 관련 법제의 차이로 인한 법 적용 문제가 발생할 수 있는데 계약 용어의 사용이나 계약조건의 해석 등에 관련한 문제가 이에 해당 될 것이다.

한편, 클라우드컴퓨팅 서비스 제공자가 동일한 계약 용어를 사용하여 청약하는 경우에도 국가별 계약법제의 차이로 인하여 계약을 체결한 이용자의 법 이해가 다르게 작용하는 문제가 발생할 수도 있다.

따라서 클라우드 계약과 서비스 수준협약을 고려할 필요가 있다. 빠르게 성장하고 다양화 되어가는 시장에서, 클라우드 서비스에서 사용되는 용어는 관계당사자간에 해결해야 될 문제로 검토될 수도 있는 반면, 소비자가 관여되는 경우에는 서비스의 질, 정보 이동성, 혹은 정보의 소유권 등 소비자가 고려하는 핵심사안을 다루는 표준 조항 사용에 대한 충분한 고려가 요구된다.⁶⁷⁾

이와 같이 소비자와 기업들이 클라우드컴퓨팅 서비스 활용에서 나타날 수 있는 다른 문제는 계약의 불명확성이나 클라우드서비스 제공자와의 불균형성에 기반한다. 클라우드 환경에서의 개인정보보호와 함께 계약법 적용을 위한 법제 개선도 클라우드 서비스 활성화를 위한 큰 문제라 할 수 있다.

따라서 여기서는 클라우드컴퓨팅 계약 관련 논의동향을 검토하고 간략한 시사점을 제시해 보도록 한다.

제 2 절 계약 관련 논의동향

1. 현대 디지털 계약 원칙의 제시

EU 집행위원회에서는 「유럽 공통매매법(Common European Sales Law)」에 대한 제안서에서 디지털 아젠다 하의 신뢰성 구축과 관련하여 통일되지 못한 규정으로 계약을 하여 발생하는 어려움을 설명하고 있다.⁶⁸⁾

EU에서는 기존 EU 의회의 규칙 등을 통하여 클라우드 서비스 이용자들을 보호하기는 하지만, 특히 계약법에 관한 질문이 발생하였을

67) ITU, 「GSR 2012 Discussion Paper Demystifying Regulation in the Cloud : Opportunities and Challenges for Cloud Computing」, 2012. 10. 19, p.16

68) EUROPEAN COMMISSION, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Unleashing the Potential of Cloud Computing in Europe”, 2012. 9. 27 p.11

때 민사 및 상사의 문제와 관련하여, 적용가능 한 법이나 관할을 포함하여 EU 회원국 국민들의 권리를 알기 어렵다.⁶⁹⁾

이를 개선하기 위하여 EU 집행위원회는 단일 시장을 강화하기 위해 매매 관련 법제, 보험계약 관련 법제 및 클라우드컴퓨팅 계약의 영역에서 여러 계획을 제안하고 있다.

이러한 논의를 바탕으로 하여 2015년 9월 12일 “디지털 콘텐츠 제공 계약 고려사항에 관한 유럽의회와 이사회의 지침(이하 ‘제안서’라 함)”이 제안되었다.⁷⁰⁾ 이를 일명 “현대 디지털 계약 원칙(Modern digital contract rules)”이라고 설명하고 있다.⁷¹⁾

이 제안의 목적으로는 유럽이라는 디지털 단일 시장의 빠른 성장을 위해 계약법 관련 국경의 장벽을 제거하여 법적 복잡성과 불확실성을 제거하고 소비자의 권리보장 및 통일적인 규칙제공에 따른 소비자의 신뢰 증진을 제시하고 있다.⁷²⁾

이하에서는 EU에서 클라우드컴퓨팅을 포함하는 디지털 콘텐츠 제공 계약 관련 규제 개선 등 제도개선을 위한 논의 사항을 정리한다.

2. 디지털 콘텐츠 제공 계약 관련 고려사항

디지털 콘텐츠 제공 계약시의 고려사항을 정리한 EU의 제안서는 총 24개의 조문으로 구성되어 있다.⁷³⁾

69) *Id* p.11

70) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content(<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015PC0634&from=EN>), (2016. 7. 27. 최종방문)

71) http://ec.europa.eu/justice/newsroom/contract/news/151209_en.htm(2016. 7. 27 최종방문)

72) <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015PC0634&from=EN>, (2016. 7. 27. 최종방문)

73) 이 지침은 유럽 연합(EU)의 공식 저널을 통해 게시된 20일 이후에 발효한다고 명시되어 있다(Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of

<표-4> 제안서의 구성

조문	제목
제1조	목적
제2조	정의
제3조	범위
제4조	조화의 수준
제5조	디지털 콘텐츠의 제공
제6조	디지털 콘텐츠 계약의 준수
제7조	디지털 콘텐츠의 통합
제8조	제3자의 권리
제9조	입증책임
제10조	제공자의 책임
제11조	제공실패의 처리
제12조	계약이행이 불충분한 경우의 처리
제13조	계약의 종료
제14조	피해에 대한 권리
제15조	디지털 콘텐츠의 수정
제16조	장기계약 종료시의 권리
제17조	배상청구권
제18조	시행
제19조	구속력
제20조	다른 지침의 개정
제21조	지침 관련 변경

digital content Art.23).

제22조	검토
제23조	발효일
제24조	어드레스

출처 : EUROPEAN COMMISSION, "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content", 2015. 9. 12, P.31-46의 내용을 발췌·정리함

이 제안서 제6조에서는 디지털 계약 준수를 위하여 ① 서비스의 양, 품질, 기간 및 버전이 계약 내용과 같아야 하고, 사전계약 정보를 포함하는 계약의 필수 부분에 기능성, 상호운용성, 접근성, 연속성, 보안과 같은 다른 성능 특성을 보유해야한다. 그리고 ② 계약에 명시된 지시사항과 고객지원 사항에 따라 제공되어야 하며, ③ 계약 명시된 업데이트를 하여야 한다고 정하고 있다(Art.1(a)-(d)).

계약의 적합성에 대한 입증책임은 제공자에게 있으며(Art.9 1), 소비자는 디지털 환경을 결정하기 위해 제공자에게 협력할 의무를 진다(Art.9 3). 다만 소비자가 협력하지 못하는 경우, 계약의 비적합성에 대한 입증 책임은 소비자에 있다고 하였다(Art.9 3).

디지털 콘텐츠 제공 실패시의 처리에 관해서는 제공자가 제5조에 따라 디지털 콘텐츠를 제공하지 못한 경우 소비자는 제13조에 규정한 바와 같이 즉시 계약을 해지할 권리를 가지는 것으로 규정하고 있으며(Art.11), 소비자는 제공자에게 계약을 해지할 것을 통지하여 계약해지의 권리를 행사할 수 있다고 하였다(Art 13). 우선, 소비자가 계약을 종료할 때, 공급자는 해지통보를 받은 이후 14일 이내에 어떠한 경우라도 소비자에게 배상한다(Art.13 2(a)). 이 경우 공급자는 소비자로부터 제공받은 콘텐츠와 소비자가 생산 또는 발생시킨 다른 데이터를 소비자에게 제공하여야 하며, 소비자는 합리적인 시간 동안 데이터

포맷 등을 통해 비용 지급이나 불편함이 없이 콘텐츠를 회수할 자격을 갖는다(Art 13 2(c)).

소비자와 생산 또는 데이터 공급자에 의해 유지된 정도까지 디지털 콘텐츠의 소비자의 사용을 통해 생성된 다른 데이터가 제공하는 모든 콘텐츠를 검색하는 기술적 수단으로 소비자를 제공해야한다. 소비자는 적절한 시간 및 일반적으로 사용되는 데이터 포맷에 상당한 불편 없이 무료로 콘텐츠를 검색하는 권리를 갖는다.

제14조에서 손해배상청구권에 대한 사항을 정하고 있는데, 제공자는 계약의 불충분한 이행이나 콘텐츠 공급의 실패에 대하여 디지털 환경에서의 소비자의 어떠한 경제적 손해도 책임을 진다. 이를 위하여 회원국은 소비자의 손해배상청구권 행사에 대한 상세한 규정을 마련하여야한다.

또한, 제15조 계약의 수정에 관해서 디지털 콘텐츠 제공기간이 계약에 규정되어 있는 경우 기능, 상호운용성, 접근성, 연속성 및 보안과 같은 디지털 콘텐츠의 주요 기능을 수정할 수 있는데, 이 경우 계약으로 규정되어야 하고, 소비자는 영구적인 매체로 수정을 사전에 합리적으로 통지하도록 하였다. 또한, 소비자는 통지 접수로부터 30일 이내에 비용 지불 없이 계약을 해지할 수 있도록 보장하고 있다.

제16조에서는 장기계약의 종료에 관한 권리를 규정하였는데, 불확정한 기간이나 최초 계약 기간 또는 갱신주기가 12개월을 초과하는 경우의 디지털 콘텐츠 제공을 위한 계약에서 소비자는 첫 번째 12개월 기간의 만료 후 계약을 언제든지 해지할 권리를 가진다는 것이다.

마지막으로 제18조 시행에 관한 규정에서 이 지침을 준수하기 위해 회원국들은 공공기관이나 그 대리인, 소비자단체, 정당한 전문기관이 국내법에 의해 결정, 법원으로의 이전, 또는 법에 따른 조치를 취할 수 있도록 하여야 한다고 규정하고 있다.

3. 모델계약 용어 사용 등 계약 표준화

앞서 설명한 클라우드컴퓨팅을 포함한 디지털 계약의 특징이라 할 수 있는 탈지역기반의 계약체결에 따라 발생하는 어려움을 개선하기 위하여 EU에서는 모델 계약용어를 개발하는 방법이 제안되었다. 이미 이용자와 제공자들은 자율규제 협정이나 표준화를 요구해왔고, 소비자와 소규모 기업들에 대한 계약은 유럽 모델 계약 용어와 조건은 클라우드 서비스의 투명하고 공정한 계약을 위해 필요하게 될 것이다. 또한, 모델 계약 용어를 확립하고 보급하는 것은 잠재적 소비자에게 신뢰도를 높여 클라우드컴퓨팅의 정착을 촉진시킬 것이라고 전망하였다.⁷⁴⁾

계약용어와 관련된 적절한 제도는 디지털 계약의 중요한 문제인 데이터 보호에 큰 도움이 될 수 있다. 개인정보가 유럽연합과 EEA 외부로 전송 될 경우에도 보안을 유지하는 것을 보증하게 되는데 즉, 국제적인 데이터 전송 및 설정을 관리하는 표준계약조항을 통해 클라우드 기업이 채택하도록 하는 것이다.⁷⁵⁾

이를 위하여 EU 집행위원회는 클라우드 제공자와 사용자들 간의 서비스 단계 동의서에 사용하는 유럽 모델 계약용어를 개발하고 소비자와 소규모 기업을 위하여 「유럽 공통매매법(Common European Sales Law)」에 모델용어와 조건이 포함되도록 하겠다고 밝히고 있다. 핵심적인 모델 계약용어 및 조건에 관한 표준지침을 정하여 디지털 콘텐츠에 관한 클라우드 서비스 분야에서 사용될 실용적인 계약용어들을 제공하려는 것이다.⁷⁶⁾

74) EUROPEAN COMMISSION, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Unleashing the Potential of Cloud Computing in Europe”, 2012. 9. 27 p.12

75) *Id*

76) *Id* p.12-13

절차적으로는 EU 집행위원회가 전문가 집단을 구성하여, 소비자와 소규모 기업을 위해 기존 「유럽 공통매매법」을 벗어나는 클라우드 관련 이슈들에 관한 안전하고 공정한 계약 용어와 조건을 마련하고자 하였다.⁷⁷⁾

또한, 제3국으로 개인정보가 이동되는 경우에 적용가능 한 표준계약 조항을 검토하고, 클라우드 서비스를 위해 필요한 경우 국가 정보보호 기관에게 법적 구속력이 있는 기업 규칙을 승인을 요청하는 방식으로 참여를 유도하고 있다.⁷⁸⁾

이러한 표준계약의 도입방법으로 표준서비스약관의 사용을 고려해 볼 수 있는데, 서비스제공자의 약관을 통해 서비스이용계약을 체결하게 되는 경우 서비스제공자 측의 책임을 과도하게 제한하는 면책약관에 대해서는 이용자 보호 측면에서 검토할 필요가 있다.⁷⁹⁾

제 3 절 우리나라의 클라우드컴퓨팅 계약 관련 법제

1. 클라우드컴퓨팅법의 계약 관련 입법

「클라우드컴퓨팅법」에서 클라우드컴퓨팅의 계약체결에 관해서는 제 24조에 표준계약서에 관한 조문을 두고 있을 뿐이다.⁸⁰⁾

77) *Id.* p.13

78) *Id.*

79) 박영규, 앞의 논문, 123쪽.

80) 「클라우드컴퓨팅법」제18조 제2항에서 “대기업인 클라우드컴퓨팅서비스 제공자는 중소기업인 클라우드컴퓨팅서비스 제공자에게 합리적인 이유 없이 그 지위를 이용하여 불공정한 계약을 강요하거나 부당한 이익을 취득하여서는 아니 된다”고 규정한 것은 대기업과 중소기업이라는 클라우드컴퓨팅 서비스 제공자 간의 계약에 관한 규정이므로 이용자 관련 계약 규정에는 포함되지 않는다.

「클라우드컴퓨팅법」

제24조(표준계약서) ① 미래창조과학부장관은 이용자를 보호하고 공정한 거래질서를 확립하기 위하여 공정거래위원회와 협의를 거쳐 클라우드컴퓨팅 서비스 관련 표준계약서를 제정·개정하고, 클라우드컴퓨팅서비스 제공자에게 그 사용을 권고할 수 있다. 이 경우 클라우드컴퓨팅서비스 제공자, 이용자 등의 의견을 들을 수 있다.

② 미래창조과학부장관이 제1항에 따라 표준계약서를 제정·개정하려는 경우에는 미리 방송통신위원회의 의견을 들어야 한다.

이 법에서는 클라우드컴퓨팅 서비스 이용자와 제공하는 자에 관해서 제2조 제4호에서 정의하고 있으나, 클라우드컴퓨팅 서비스 제공자에 관해서는 직접정의 하는 방식이 아닌, 제2조 제3호의 클라우드컴퓨팅 서비스를 제공하는 자로 정의하고 있어 이 법 시행령 제3조에서 규정한 “1. 서버, 저장장치, 네트워크 등을 제공하는 서비스 2. 응용프로그램 등 소프트웨어를 제공하는 서비스 3. 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스 4. 그 밖에 제1호부터 제3호까지의 서비스를 둘 이상 복합하는 서비스”를 제공하는 자가 클라우드컴퓨팅 서비스 제공자에 해당하게 된다.

2. 약관규제법의 계약 관련 입법

「약관규제법」제2조 제1호에서 약관이란 “그 명칭이나 형태 또는 범위에 상관없이 계약의 한쪽 당사자가 여러 명의 상대방과 계약을 체결하기 위하여 일정한 형식으로 미리 마련한 계약의 내용”으로 규정하고 있기 때문에 클라우드컴퓨팅의 서비스 계약도 여기에 해당되는 것으로 볼 수 있다.

「약관규제법」의 표준약관에 대해서는 제19조의3에서 정하고 있는데, 여기에서 표준약관은 사업자 등이 사전에 공정거래위원회에 약관에

관한 심사를 청구하여 정할 수 있으며, 공정거래위원회는 이에 따라 심사하거나 제정·개정된 표준약관을 공시(公示)하고 사업자 및 사업자단체에 표준약관을 사용할 것을 권장할 수 있다고 규정하였다.

이러한 규정은 표준약관에 관한 일반적인 사항으로 클라우드컴퓨팅의 서비스 계약에 대해서도 동일하게 적용될 것이고 그 밖에 이 법에서 클라우드컴퓨팅 서비스 계약에서 특히 고려하여야 할 사항은 없는 것으로 보인다.

다만, 「클라우드컴퓨팅법」 제24조에서는 클라우드컴퓨팅의 표준계약서를 공정거래위원회와 협의를 거쳐 미래창조과학부 장관이 제정·개정하도록 정하고 있는 점에 특징이 있다.

외국 사업자와의 클라우드컴퓨팅 서비스 계약에 있어서 「약관규제법」을 적용할 수 있을 것인지에 대해서는 이 법에서 별도로 정하고 있는 사항이 없다.

「독점규제 및 공정거래에 관한 법률」의 경우 제2조의2에서 국외행위에 대한 적용 규정을 두고, “이 법은 국외에서 이루어진 행위라도 국내시장에 영향을 미치는 경우에는 적용한다”고 명시적으로 규정하고 있는 것과 달리, 「약관규제법」의 경우 이러한 규정이 없어, 역외적용에 대한 해석이 불분명한 문제가 있다.

또한, 「약관규제법」이나, 「클라우드컴퓨팅법」에서도 별도의 적용범위를 설정하거나, 사업자의 범위(외국사업자 포함여부)에 대해 명확한 규정을 두고 있지 않다.

제 4 절 소결 : 시사점

클라우드컴퓨팅 계약 관련 국제적 논의동향을 요약하면 크게 새로운 디지털계약 원칙의 등장과 서비스계약시 표준용어(표준계약서, 서비스 수준협약)의 사용으로 정리된다.

새로운 디지털계약 원칙의 경우 우리나라에서도 새로이 고려해 보아야 할 사항이라 할 수 있다.

클라우드컴퓨팅 서비스 계약에 관한 사항뿐만 아니라 현대 사회에서 발생하는 수많은 인터넷 기반 계약환경에 적합한 계약의 원칙이 새로이 제시될 필요가 있다는 것에 공감한다.

현재는 「전자상거래 등에서의 소비자보호에 관한 법률」을 통해 주로 인터넷 계약 환경에서의 소비자보호를 도모하고 있으나, 앞서 살펴 본 탈지역기반이라는 인터넷 계약 환경의 특성을 이 법 역시 반영하고 있지 못하다.

클라우드컴퓨팅을 비롯한 인터넷 계약 환경의 소비자 보호를 위한 적극적인 입법이 필요한 시점이라 판단된다.

이에 관하여 앞에서 설명한 「독점규제 및 공정거래에 관한 법률」의 입법례와 같이 해외기업과의 계약의 경우에도 국내시장이나 우리국민에게 영향을 미치는 경우의 국내법 적용을 명시하는 방안을 고려할 필요가 있다.

이 경우 그 입법의 위치는 「약관규제법」에서 규정하도록 하여 단지 클라우드컴퓨팅이 아닌 일반적인 인터넷 환경의 계약에 적용되도록 하는 방안을 고려하는 것이 「클라우드컴퓨팅법」등 정보통신 관련 법에 입법하는 것보다 바람직할 것이라 판단된다. 왜냐하면, 법의 집행 가능성을 고려하기 위해서이다.

「독점규제 및 공정거래에 관한 법률」의 경우 공정거래위원회가 그 관할 정부부처로서 이미 기업의 영업활동 관련 우리법의 역외적용에 관한 법의 집행 실적이 다수 있으며, 인터넷 환경의 계약도 ‘계약’, ‘약관’, ‘기업활동’의 영역에 속하는 것이므로 같이 법을 집행하는 것이 보다 전문적인 집행이 가능할 것으로 판단되기 때문이다.

한편, 다른 검토사항으로 정보의 국외이전에 관한 사전적인 계약체결 및 규제심사에 관한 사항이 있다.

전술한 바와 같이, 우리나라 기업들이 EU 회원국에서 영업활동에 필요한 개인정보를 국내로 전송하여 처리해야 할 경우, EU 회원국과 사전에 국외이전 계약을 체결하고 회원국별 감독기구의 규제심사를 거쳐야 한다.⁸¹⁾

이러한 절차에 관해서 이미 우리 정부에서 보다 간소하게 진행할 수 있도록 여러 정책적인 방안을 고려하고 있을 것이나, 우리나라에서 영업활동을 영위하는 해외기업이 자국으로 개인정보를 전송하여 처리하여야 할 경우에 대한 처리방안 등에 대해서도 고려해야 할 것이다.

다음으로 클라우드컴퓨팅 계약 등 인터넷 환경에서 체결하게 되는 계약에서 사용되는 용어의 표준화, 표준계약의 사용에 관해 고려해야 한다.

앞서 설명한 EU의 모델용어 사용에 관한 움직임은 우리나라 법제에도 중요한 시사점을 주는 것으로 보인다. 표준계약 등으로 계약을 정형화, 표준화하는 노력과 함께 사용하는 용어의 표준화를 통하여 어느 나라의 이용자라도 동일한 이해가 가능하도록 하고, 피해를 예방할 수 있다면, 해당 산업의 활성화 측면에서나 이용자 보호의 측면에서 모두 긍정적인 역할을 할 수 있을 것이라 기대된다.

이와 관련하여 앞서 설명한 미래창조과학부 고시 「클라우드컴퓨팅 서비스 정보보호에 관한 기준」을 보면, 제2조 제5호에서 “서비스수준 협약이라 함은 서비스 제공자가 서비스 가입자와 합의를 통하여 사전에 정의된 수준의 서비스를 제공하기로 맺는 협약”으로 정의하고 있으나 이후 이 고시에서 서비스수준협약에 대해 언급하고 규정은 없다. 정의 규정에서 정하는 사항은 이후 본칙에서 필요한 사항을 정하는 것인데, 이와 같이 정의규정에서만 용어를 정의한 형태는 일반적이지 않은 것으로 향후 보완될 것이라 판단된다.

81) 행정자치부 보도자료, “국내 개인정보 보호 수준, 국제적 기준에 맞춘다 - 국제기준을 적용한 개인정보 보호법 개정 추진 -”, 2015. 12. 15, 1쪽.

또한, 「클라우드컴퓨팅법」에서 표준계약서를 사용하도록 권고하는 규정은 2012년 방송통신위원회의 입법안에서는 ‘정부가 수행하는 정보보호 인증제도’를 포함하도록 했던 것에서 완화된 것으로 설명되고 있는데,⁸²⁾ 향후에는 이 인증제도를 통한 신뢰성 보완의 방안도 재검토해 볼 수 있을 것이다.⁸³⁾

82) 오길영, “클라우드컴퓨팅 발전 및 이용자보호에 관한 법률안’의 검토와 비판”, 2014, 11, 268쪽.

83) 다만, 이와 유사한 취지로 이미 「정보통신융합법」에서 ‘기술·서비스 등의 품질 인증’에 관하여 규정하고 있으므로 중복입법 여부에 대한 검토는 필요하다. 이 법 제17조 제1항에서 미래창조과학부장관은 정보통신융합등 기술·서비스 등의 편의성·안정성·신뢰성·확장성 등에 관한 인증기준(이하 “품질기준”이라 한다)을 정하여 고시할 수 있도록 하고, 제2항에서 미래창조과학부장관은 정보통신융합등 기술·서비스 등의 품질이 제1항에 따라 고시한 품질기준에 적합한지를 인증할 수 있도록 하고 있다.

제 4 장 결 론

클라우드 서비스에 대한 불확실성은 개인정보의 보호, 보안, 서비스 제공, 이용자 보호 등 다양한 측면에서의 보완이 지속적으로 요청되고 있으며, 이에 대한 규제와 보완 또한 요청되는 분야라 할 수 있다.

또한, 클라우드컴퓨팅에 관한 여러 가지 서비스의 확대가능성과 탈지역기반을 서비스의 특성으로 한다는 점에서 우리나라에서 이미 이에 관한 「클라우드컴퓨팅법」이 입법된 이후에도 계속 논의가 진행될 수밖에 없는 것이며, 국제적인 논의의 수용과 평준화가 보다 강조되고 있는 것으로 판단된다.

이와 같은 고민들은 최근에 생겨난 새로운 통신기술들의 등장에 따라 겪었던 경험들을 그대로 되풀이 하는 듯이 보인다.

PC의 등장과 인터넷의 접근성 확대, 모바일 컴퓨터의 보급 등으로 새로운 기술을 어떤 유형으로 구분할 것인지, 이를 통한 계약을 기존의 어떤 계약 유형으로 보고 규제해야 할 것인지 고민하는 기존의 모습과 닮아 있다.

그런데, 클라우드컴퓨팅 관련 법제에 관한 선행연구들과 외국의 논의 동향을 검토하면서 클라우드컴퓨팅 관련 법적인 논의가 처음 시작된 2010년 이후 「클라우드컴퓨팅법」이 제정된 이후까지 큰 쟁점사항은 동일하다는 것을 알게 되었다. 그리고 그 쟁점에 대하여 국내의 입법이 있는 후에도 명확히 해결되지 못하고 있었다.

그 사유로는 큰 쟁점이 정보의 역외이동과 정보가 여러 디바이스와 도처의 저장공간에 분산되어 저장되는 것으로 인한 준거법의 적용문제,⁸⁴⁾ 외국 사업자를 포함하는 클라우드컴퓨팅 서비스 제공자와 이용자의 계약문제(이용자의 보호를 위한 표준계약서 사용 등)이기 때문이

84) 클라우드컴퓨팅 계약의 준거법 적용에 대해서는 박영규, 앞의 논문, 203쪽 이하 참조.

고 더 근본적으로는 이를 규율하기 위해서는 어느 한 국가의 입법으로는 개선될 수 없기 때문이다. 결국 클라우드컴퓨팅 관련 기술의 발전은 날로 가속화 다양화되고 있는 반면, 법제적인 접근은 이 속도를 따라가지 못하는 것이다.

「클라우드컴퓨팅법」의 경우 클라우드컴퓨팅 관련 산업을 발전시키기 위하여 기존의 정보통신 관련 많은 입법과 구분하여 개별 입법을 하였는데, 사실상 그 내용에서는 클라우드컴퓨팅 산업을 발전시키기 위한 특별한 조문이 입법되기 보다는 다른 정보보호 법률과 유사한 내용의 정보보호에 관한 사항과 보안에 관한 사항이 주를 이루고 있는 한계가 있다.⁸⁵⁾

최근 클라우드컴퓨팅 관련 규제개선 방안이 발표되었으나 기존의 클라우드컴퓨팅의 탈지역기반 등 관련 쟁점들에 대한 실질적인 해결이 아닌 국내에서의 금융, 의료, 교육분야에 클라우드컴퓨팅을 활성화하기 위한 고시 정비 등의 내용이 담겨져 있다.⁸⁶⁾

정보의 자유로운 이동을 특성으로 하는 클라우드컴퓨팅의 법제가 제대로 정착, 발전하기 위해서는 국가별 정보통신 기술의 평준화만큼이나 정보통신 관련 법제 수준의 평준화가 요구되는 것이다.

따라서 클라우드컴퓨팅 관련 법제야말로 여러 국가의 법제가 충분히 논의되고 각 국가에 반영할 수 있도록 지침이 정해지는 국제기구의 지침 제정 등의 결과에 주목해야 할 것이다.

한편, 개인정보보호는 인간에게 가장 핵심적인 권리이며 이 권리에 관해서는 세계인권선언문과 국제정치와 시민권리서약문에 기록되어 있다.⁸⁷⁾ 한편, 유럽에서는 유럽연합 기초 권리 헌장(2000)에 의하여 리

85) 우리나라는 이미 정보보호에 관한 법률이 촘촘히 입법되어 있기 때문에 클라우드컴퓨팅에 관한 개별 법에서 이 내용을 추가적으로 규정해야 했는지에 대해서는 의문이 있다.

86) 미래창조과학부, “제4차 산업혁명의 핵심동력, ICT 융합 신산업 활성화를 위한 규제혁신 방안 발표” 2016. 5. 18, 3쪽 참조.

87) http://www.un.org/documents/instruments/docs_en.asp?type=conven ; ITU, 「Privacy in

스본 조약(2009년 12월에 시행)과 유럽연합 법에 의해 합병되었다. EU 95/46/EC 지침과 인터넷 프라이버시, 정보 보유를 포함한 전자 소통지침인 2002/58/EC는 개인 프라이버시와 개인 정보 활용을 포괄하는 주요 유럽 법률들이다.⁸⁸⁾ 그런데 이후 유럽의 27개 국가들은 1995년 EU의 공식 지령을 저마다 다르게 시행했으며 그 결과로 인해 집행에 어려움을 겪었다.⁸⁹⁾ 클라우드컴퓨팅 서비스에서 개인정보보호는 더욱 복잡한 문제로 나타날 수 있으므로 개인정보보호에 관한 초기 논의와 제도도입이 있었을 때와 같은 어려움이 다시 나타나지 않도록 주의할 필요가 있다. 예컨대, 각국의 클라우드컴퓨팅에 관한 제도가 화합되지 못하고, 정보의 위치에 좌우되며 이해관계자들 사이의 책임 소재가 불분명할 때, 클라우드에 법적 체계를 적용하는 것은 쉽지 않은 일이 될 것이다.

보안의 문제에 있어서도 점점 방대해지는 클라우드컴퓨팅 서비스에서의 정보집적과 처리는 해커들이나 클라우드컴퓨팅 서비스 제공자로 하여금 정치적 또는 상업적 동기를 부여한다. 클라우드컴퓨팅의 특수성에 따라 정보보안에 대한 지속적이고 강력한 장려정책이 필요하다. 이는 이견이 없을 것이다. 예컨대, 클라우드서비스 제공자는 저장된 개인정보에 대한 암호화 의무적으로 하도록 하여 권한이 없는 서버로의 진입이나, 개인정보 복사, 유출, 또는 처리를 예방하도록 하여야 할 것이다.

Cloud Computing», 2012. 3, p.7. 재인용

88) ITU, 「Privacy in Cloud Computing», 2012. 3, p.7.

89) *Id.* p.7.

참 고 문 헌

□ 국내문헌

- 관계부처 합동, “K-ICT 클라우드컴퓨팅 활성화 계획(안)”, 2015. 11. 10.
- 미래창조과학부, “제4차 산업혁명의 핵심동력, ICT 융합 신산업 활성화를 위한 규제혁신 방안 발표” 2016. 5. 18.
- 박영규, “클라우드컴퓨팅의 법적 문제에 관한 고찰”, 법조(Vol.671), 2012. 8.
- 박종수, “클라우드컴퓨팅과 정보보호”, 법제연구 제46호, 2014.
- 오길영, “‘클라우드컴퓨팅 발전 및 이용자보호에 관한 법률안’의 검토와 비판”, 2014, 11.
- 유우영·임종인, “클라우드컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구”, 정보보호학회논문집 제22권 제2호, 2012. 4.
- 이인용, “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률안 검토 보고서”, 국회 미래창조과학방송통신위원회, 2013. 12.
- 행정자치부 보도자료, “국내 개인정보 보호 수준, 국제적 기준에 맞춘다 - 국제기준을 적용한 개인정보 보호법 개정 추진 -”, 2015. 12. 15.

□ 외국문헌

EUROPEAN COMMISSION, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,

참 고 문 헌

THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Unleashing the Potential of Cloud Computing in Europe”, 2012. 9. 27.

ITU, 「Privacy in Cloud Computing」, 2012. 3.

ITU, 「GSR 2012 Discussion Paper Demystifying Regulation in the Cloud : Opportunities and Challenges for Cloud Computing」, 2012. 10. 19.

ITU, 「Trends in Telecommunication Reform 2016」, 2016.

□ 인터넷 자료

<http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=001&aid=0007230052>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>

http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm

http://ec.europa.eu/justice/newsroom/contract/news/151209_en.htm

http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000_000000008&nttId=47865

http://www.dt.co.kr/contents.html?article_no=2016042702109960813013

<https://itunews.itu.int/En/3414-Regulation-in-the-cloud.note.aspx>

<http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw44&artId=1186502>

<https://itunews.itu.int/En/3414-Regulation-in-the-cloud.note.aspx>

<http://terms.naver.com/entry.nhn?docId=20154&cid=43659&categoryId=43659>

[http://terms.naver.com/entry.nhn?docId=20139&cid=43659&categoryId=43659,](http://terms.naver.com/entry.nhn?docId=20139&cid=43659&categoryId=43659)

[http://terms.naver.com/entry.nhn?docId=20155&cid=43659&categoryId=43659,](http://terms.naver.com/entry.nhn?docId=20155&cid=43659&categoryId=43659)

<http://terms.naver.com/entry.nhn?docId=2075491&cid=42107&categoryId=42107>

http://news.inews24.com/php/news_view.php?g_serial=970491&g_menu=020800&rrf=nv

http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000_000000008&nttId=47865

<http://cloudscorecard.bsa.org/2012/>

<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015PC0634&from= EN>

참 고 자 료

<참고자료>

결의안 제 200호 (Busan, 2014)

글로벌 전기통신/정보 및 통신기술 발전을 위한 커넥트 2020 의제

국제전기통신연합 전권회의(부산, 2014)는 아래 각 호를 상기하고,

- a) ITU 규약 제 1조에 기재된 동맹의 목적과
- b) 유엔 새천년 개발 목표(MDG) 달성을 위한 ITU 및 그 회원국의 공약
- c) 2015년까지 달성할 제네바 실행계획의 목표를 증진함에 있어 전기통신/정보통신기술(ICT)의 접근 및 이용을 개선하기 위해 글로벌 준거점의 역할을 수행하고 있는 세계정보사회정상회담(WISIS)이 정한 목표
- d) 이해관계자의 협력 강화 및 지속을 장려하고 이와 관련하여 ITU가 주도하는 커넥트 월드 사업을 환영하는 튀니스 정보사회 의제 제 98조

아래 각 호를 고려하고

- a) 유엔 전기통신/ICT 전문기관이자 유엔 개발 체제에 따라 관련 사업을 시행하는 실무 기관인 동맹의 이중 책임
- b) 2015 이후 개발 의제와 지속가능한 발전 목표(SDG)를 위한 유엔 체제 전반의 준비와 MDG 달성을 위한 노력

아래 각 호를 지적하고

대한민국 부산(2014)에서 개최된 각료회의에서 채택되고 “커넥트 2020” 의제 하에 전기통신/ICT 부문의 발전을 위해 공유되는 글로벌 비전에 반영된 지속가능한 발전을 달성하는 향후 전기통신/ICT의 역할에 관한 부산선언

아래 각 호를 인정하고

- a) 유엔총회(UNGA)에서 결의안 제 55/2호로 채택하고 신기술, 특히 ICT의 편익을 인정하는 유엔 새천년선언의 원칙
- b) WSIS 결과 문서- 제네바 실행계획(2003) 및 튀니스 의제(2005)
- c) WSIS+10 검토 프로세스, 특히 WSIS+10 고위직 행사의 결과 문서 - WSIS 결과의 실행에 관한 WSIS+10 성명 및 2015 이후 WSIS에 대한 WSIS+10 비전
- d) WSIS를 배경으로 설립된 커넥트 월드 글로벌 복합 이해관계자 사업 하에 개최된 커넥트 시리즈 정상회담(커넥트 아프리카, 커넥트 CIS, 커넥트 아메리카, 커넥트 아랍, 커넥트 아시아태평양)의 성과
- e) 세계전기통신개발회의(WTDC-14)에서 채택한 두바이선언과 두바이 실행계획, 본 회의의 결의안 제 30호, 37호, 50호(Rev. Dubai, 2014)뿐 아니라 제 135호, 139호, 140호(Rev. Busan, 2014)를 비롯한 관련 WTDC-14 결의안
- f) 2015-2019년 동맹의 전략 체계를 채택하고 전략 목적과 관련 대상 및 목표를 정한 본 회의의 결의안 제 71호(Rev. Busan, 2014)
아울러 아래 각 호를 인정하여
 - a) 전기통신/ICT는 지속가능한 사회와 경제, 환경 성장 및 발전을 촉진하는 핵심 동인이다.
 - b) 현재의 업적을 지속하고 개발에 사용되는 ICT를 진흥 및 지원하기 위한 노력을 강화해야 할 필요성
 - c) 결의안 제 71호(Rev. Busan, 2014), 제 1 부속서에 확인한 대로 급속하게 발전하는 전기통신/ICT 환경의 글로벌 과제
아래와 같이 결의한다.

- 1 “전기통신/ICT”가 모든 이에게 지속가능한 사회와 경제, 환경 성장 및 발전을 실현 및 촉진하는 상호접속 세계를 통해 강화되는 정보사회"를 예상하는 의제 “커넥트 2020” 하에 전기통신/ICT 부분의 발전을 위해 공유되는 글로벌 비전을 지지한다.
- 2 하기에 상술되는 상위 4대 전략 목적과 본 결의안 부속서에 상술되는 각 목표를 지지하고 모든 이해관계자와 주체가 협력하여 커넥트 2020 의제를 실행할 것을 고취 및 촉구한다:
 - 제 1 목적: 성장 - 전기통신/ICT의 접근 및 이용 증대를 실현 및 증진한다.
 - 제 2 목적: 통합 - 디지털 격차를 해소하고 모든 이에게 광대역을 제공한다.
 - 제 3 목적: 지속가능성 - 전기통신/ICT 발전으로 인한 과제를 관리한다.
 - 제 4 목적: 혁신과 협력 - 전기통신/ICT 환경의 변화를 주도, 개선하고 이에 적응한다.
- 3 유엔 사무총장과 협력하여 2015 이후 개발 의제에 대한 지속적 논의에 적극적으로 참여하고 MDG와 2015 이후 개발 의제 SDG를 달성하는 핵심 동인이라는 전기통신/ICT의 중요한 역할을 보장하며 경제와 사회, 환경 차원의 지속가능한 발전을 균형 있게 통합하는 2015 이후 유엔 개발 의제에서 전기통신/ICT의 중요성을 보장하는데 일조할 것을 회원국에 촉구한다.

사무총장에 아래와 같이 지시한다.

- 1 특히 ITU 세계 전기통신/ICT 지표 데이터베이스와 개발 ICT 측정 파트너십의 데이터를 활용하여 커넥터 2020 의제의 달성 경과를 모니터한다.
- 2 커넥트 2020 의제에 기여하는 국가와 지역, 국제 사업에 관한 정보를 배포하고 지식과 모범사례를 공유한다.

참고 자료

- 3 커넥트 2020 의제에 따라 ITU의 책임에 할당된 WSIS 실행 방침의 이행을 촉진한다.
- 4 ITU 이사회에 통합 연례 경과 보고서를 제출한다.
- 5 모든 이해당사자, 특히 USGA와 유엔 개발 프로그램, 경제사회이사회에 본 결의안을 통지하여 결의안 이행에 협력을 구한다.
- 6 본 결의안 3번 결의와 관련하여 회원국의 적극적 참여를 지속적으로 지원한다.

국장에게 아래와 같이 지시한다.

커넥트 2020 의제에 기여하는 결의안 제 71호(Rev. Busan, 2014), 제 2 부속서에 포함되는 2016-2019 동맹 전략 계획에 부연되는 각 부문의 업무 목표 및 성과 달성의 경과를 보고한다.

전기통신개발국장에게 아래와 같이 지시한다.

글로벌 전기통신/ITC 목표의 달성을 위한 경과에 대한 비교 분석을 측정 및 제공하는 지표 및 통계의 수집과 제공, 배포를 공조하고 연례 정보사회 측정 보고서의 일환으로 경과를 보고한다.

이사회에 아래와 같이 지시한다.

- 1 커넥트 2020 의제의 달성을 위해 성취되는 연례 경과를 검토한다.
- 2 커넥터 2020 의제 달성의 경과 평가를 차기 전권회의에 발표한다.

회원국에 아래와 같이 권고한다.

- 1 커넥트 2020 의제의 이행에 적극적으로 참여하고 국가, 지역 국제 사업에 기여한다.
- 2 모든 기타 이해관계자에게 커넥트 2020 의제에 기여 및 협력하도록 권고한다.
- 3 커넥트 2020 의제 달성의 경과를 모니터 하는데 적절한 데이터와 통계를 제공한다.

- 4 커넥트 2020 의제의 달성을 위한 국가의 경과를 보고하고 커넥트 2020 의제에 기여하는 국가 및 지역 사업에 관한 정보를 수집 및 배포하는 데이터베이스에 기여한다.
- 5 UNGA가 정한 절차에 따라 2015 이후 개발 의제에 관한 논의에 적극적으로 참여한다.
- 6 ICT가 전체 SDG 달성을 위한 중요한 톨로 인정을 받아 2015 이후 개발 의제의 중심이 되도록 한다.
- 7 커넥트 2020 의제에 기여하는 결의안 제 71호(Rev. Busan, 2014) 제 2 부속서에 포함되는 2016-2019 동맹 전략 계획에 부연되는 ITU의 업무에 기여한다.

회원국과 준회원, 학계에 아래와 같이 권고한다.

커넥트 2020 의제 이행에 적극적 역할을 맡는다.

모든 이해관계자에게 아래와 같이 권고한다.

자체 사업과 경험, 자격, 전문지식을 이용하여 글로벌 전기통신/ICT 개발을 위한 커넥트 2020 의제의 성공적 실행에 기여한다.

결의안 제 200호 부속서 (Busan, 2014)

커넥트 2020: 글로벌 전기통신/정보사회기술 목적 및 목표

제 1 목적: 성장 - 전기통신/ICT의 접근 및 이용 증대를 실현 및 증진한다.

- 목표 1.1: 2020년까지 전세계 가구 가운데 55퍼센트가 인터넷을 이용한다.
- 목표 1.2: 2020년까지 전세계 개인 가운데 60퍼센트가 인터넷을 이용한다.
- 목표 1.3: 2020년까지 전세계 전기통신/ICT의 비용을 40퍼센트 이상 절감한다.

제 2 목적: 통합 - 디지털 격차를 해소하고 모든 이에게 광대역을 제공한다.

- 목표 2.1.A: 2020년까지 개도국 가구 가운데 50퍼센트가 인터넷을 이용한다.
- 목표 2.1.B: 2020년까지 최빈국(LDC) 가구 가운데 15퍼센트가 인터넷을 이용한다.
- 목표 2.2.A: 2020년까지 개도국 개인 가운데 50퍼센트가 인터넷을 이용한다.
- 목표 2.2.B: 2020년까지 최빈국(LDC) 개인 가운데 20퍼센트가 인터넷을 이용한다.
- 목표 2.3.A: 2020년까지 선진국과 개도국의 적정성 격차를 1) 40퍼센트 감소해야 한다.
- 목표 2.3.B: 2020년까지 개도국 및 경제전환국 광대역 서비스 비용

1. 여기에는 최빈국과 개발 소도국, 내륙 개도국, 경제전환국이 포함된다.

을 월평균 소득의 5퍼센트 이내로 해야 한다.

- 목표 2.4: 2020년까지 전세계 농촌 인구의 90퍼센트에 광대역서비스를 보급해야 한다.
- 목표 2.5.A: 2020년까지 인터넷 이용자의 성평등을 달성해야 한다.
- 목표 2.5.B: 2020년까지 장애인이 접근할 수 있는 전기통신/ICT를 실현하는 환경을 확립해야 한다.

제 3 목적: 지속가능성 - 전기통신/ICT 발전으로 인한 과제를 관리한다.

- 목표 3.1: 2020년까지 사이버보안 대응을 40퍼센트 개선해야 한다.
- 목표 3.2: 2020년까지 중복 전자폐기물 용량을 50퍼센트 감축해야 한다.
- 목표 3.3: 2020년까지 전기통신/ICT 부문에서 생성되는 온실가스 배출량을 기기당 30퍼센트까지 감축해야 한다.

제 4 목적: 혁신과 협력 - 전기통신/ICT 환경의 변화를 주도, 개선하고 이에 적응한다.

- 목표 4.1: 혁신에 기여하는 전기통신/ICT 환경
- 목표 4.2: 전기통신/ICT 환경에 속한 이해관계자의 효과적 협력