클라우드 컴퓨팅의 활성화를 위한 법적 제문제(Ⅰ)
- 개인정보보호 관련 쟁점 -

정 원 준*

1. 개 요

스마트 혁명은 일상생활 전반에 상당한 혁신과 편리성을 가져왔지만, 막대한 규모의 데이터 유통으로 인한 역기능 방지를 위해 개인정보의 보호가 강력히 요구되고 있다. 정보보호의 중요성이 강조되고 있는 사물인터넷(IoT), 클라우드 컴퓨팅(Cloud Computing), 빅데이터(Big Data) 등 인터넷 신산업 분야에서도 개인정보보호를 강화하기 위한 법·제도 차원의 논의가 활발히 전개되고 있다.[1] 특히, 클라우드 컴퓨팅의

* 정보통신정책연구원 ICT산업연구실 연구원, (043)531-4009, visix@kisdi.re.kr

** 본고를 시작으로 총 5회에 걸쳐 클라우드 컴퓨팅 서비스의 활성화를 위한 법적 문제들을 통합적으로 살펴보고자 한다. "① 개인정보보호 관련 쟁점, ② 저작권 관련 쟁점, ③ 서비스의 계속성 보장 관련 쟁점, ④ 사법관할권 관련 쟁점, ⑤ 클라우드법 개정안의 주요 내용 및 문제점"을 부제로 하여 순차적으로 게재하면서, 클라우드 컴퓨팅과 관련한 현행 법제 동향 및 법적 쟁점들을 전반적으로 검토하는데 의의를 두겠다.

1) 「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법')」등 국내의 정보보호법제는 "수집·이용 목적의 고지, 개인정보 이용내용 통보제도, 개인정보 유출 통보 및 신고제도, 주민등록번호 처리제한, 법정손해배상제도, 과징금 확대 등" 개인정보의 강화 일변도로 법률 개정이 이루어지고 있다. 또한 최근에는 카드사(국민·롯데·농협)의 대규모 개인정보 유

경우 IT 자원을 활용하여 개인정보를 저장·유통·보관하는 서비스로서 높은 수준의 보안체계를 갖추고 리스크를 조절할 수 있는 관리 수단을 제공하는 등 정보보안이 매우 중요한 분야이다. 하지만 지나친 정보보호는 데이터 활용을 기반으로 하는 클라우드 서비스를 비롯한 각종 ICT 융합산업의 발전을 저해하는 장애요소로 작용할 수 있다. 또한 산업 발전의 초기 단계에 있는 클라우드 컴퓨팅 분야에서는 오히려 산업 진흥을 저해하고 운신의 폭을 제약하는 일일 수 있다. 최종이용자의 개인정보가 서비스의 대상이 되는 사업의 경우, 정보보호의 규율 강화가 곧바로 영업 활동 제한으로 이어질 수 있기 때문이다. 따라서 클라우드 컴퓨팅 산업의 활성화를 위해 개인정보의 '보호'와 '활용'이라는 측면이 적절히 균형을 이룰 수 있도록 조화로운 법체계 방향이 구축될 필요가 있다.

이에 본고에서는 앞으로 게재하게 될 연속적인 법적 논의의 전제로서 '클라우드 컴퓨팅의 개관'을 간단히 정리하고, 이어서 '국내외 정보보호법제의 현황'과 '개인정보 취급위탁자의 책임 문제 및 개인정보의 국외이전'에 관한 법적 쟁점을 검토하도록 하겠다.

2. 클라우드 컴퓨팅의 개관

(1) 클라우드 컴퓨팅의 개념 및 특징

2008년을 전후로 인터넷상 허가된 컴퓨팅 자원을 활용할 수 있는 다양한 서비스가 출현하면서, 그 일환으로 클라우드 컴퓨팅[2] 서비스가 개시되었다. 엄밀히 말하면, '클라우드'는 인터넷 그 자체를 의미하는 것은 아니고, 온라인상의 컴퓨팅 자원을 의미한

출사태로 인해 개인정보보호 및 보안관리가 사회적 문제로 대두됨에 따라 개인정보처리자가 주민등록번호를 암호화하는 것을 의무화 하도록 하는 개인정보보호법 개정안(법률 제12504호, 2016. 1. 1 시행)이 확정되기도 하였다.

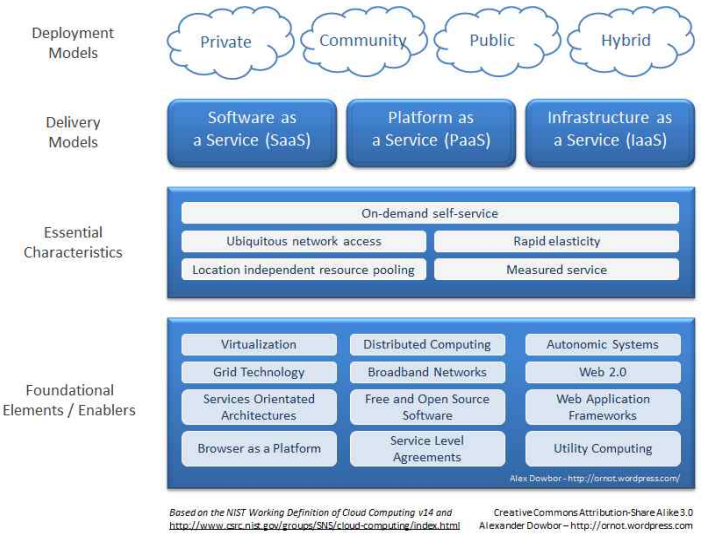
2) '클라우드 컴퓨팅'은 인터넷 초기 시절부터 사용되던 용어로서 네트워크로 연결된 컴퓨팅 자원 집단을 하나의 구름(Cloud)으로 표현한 것이다. 하지만 최근에는 가상화(Virtualization) 기술, 그리드 컴퓨팅(Grid Computing), 고속 데이터 전송 등 기술적 요인이 접목되면서, 지리적·물리적으로 분산된 전산 자원을 이용자가 원하는 위치에서 쉽게 접근할 수 있는 발전적인 형태의 서비스를 제공하고 있다.

다. '클라우드 컴퓨팅'이라는 용어는 온라인에서 소프트웨어 및 처리장치를 이용하게 된 새로운 시대의 도래와 지난 20년간의 기존 인터넷상 컴퓨팅을 구분시켜 준다는 점에서 의미가 있다(Christopher Barnatt, 2010).

미국국립표준기술원(NIST)의 정의에 따르면, 클라우드 컴퓨팅 개념은 "① 최소한의 관리나 서비스 제공자의 작업만으로 신속하게 제공·배포될 수 있고, ② 요구에 따라 변경될 수 있으며, ③ 컴퓨팅 자원들(네트워크·서버·스토리지·어플리케이션·서비스…)의 공유된 집합에, ④ 언제, 어디서나, 편리하게, 수요에 따라 네트워크를 통해 접속 가능하도록 하는 ⑤ 컴퓨팅 모델"로 이해할 수 있다.[3)]

클라우드 컴퓨팅의 종류로는 클라우드 인프라의 위치와 운영 기준에 따른 분류로서 '배치모델(Deployment Model)'과 사용자가 클라우드 컴퓨팅 서비스에 접근할 수 있는 형태에 따른 분류로서 '서비스 모델(Delivery Model)'로 구분된다(〔그림 1〕).

〔그림 1〕 클라우드 컴퓨팅의 종류 및 특성



자료: NIST 홈페이지(http://www.nist.gov/)

3) NIST 홈페이지(http://www.nist.gov/)내 자료 참조.
(http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).

배치모델은 클라우드의 이용 목적 및 시스템의 위치에 따른 분류로서 Public Cloud, Private Cloud, Hybrid Cloud, Hybrid Cloud, Community Cloud, Community Cloud로 구분할 수 있다. 서비스모델의 경우에는 사용자가 클라우드 컴퓨팅 서비스에 접근할 수 있는 형태에 따른 분류로서 IaaS(Infrastructure as a service), PaaS (Platform as a service), SaaS(Software as a Service)로 구분할 수 있다(보다 자세한 내용은 〈표 1〉 참조).

〈표 1〉 클라우드 컴퓨팅 서비스 유형별 특징

구분		주요 특징
배치 모델	Public Cloud (공용클라우드)	• 누구든지 이용하도록 구현되는 것으로 일반 이용자 또는 대기업에게 사용량에 따라 과금하는 형태로 제공되는 서비스 • 퍼블릭 클라우드의 인프라는 서비스를 판매한 업체가 소유
	Private Cloud (개인클라우드)	• 특정 조직 내부에서 클라우드 컴퓨팅 사용 환경을 제공하여 폐쇄적으로 구현하는 서비스 • 프라이빗 클라우드 인프라는 해당기관 또는 제3자에 의해 관리할 수 있으며, 영역 내/영역 외에 사용자가 조직에 포함되는 여부에 따라 권한 할당이 가능함
	Hybrid Cloud (혼합클라우드)	• 퍼블릭 클라우드와 프라이빗 클라우드의 혼재된 형태로 중요자료는 프라이빗 클라우드에 보관하고, 부분적으로 퍼블릭 클라우드를 활용하는 형태로 운영 • 데이터와 애플리케이션의 이동을 가능하게 하는 표준기술로 하나로 묶거나 2개 이상의 클라우드를 통합함
	Community Cloud (커뮤니티클라우드)	• 비슷한 환경의 기관 및 단체들이 공통으로 사용하기 위한 목적으로 만들어진 서비스 • 분산되어 있는 관계사항(목적·정책·보안요구사항·협약…)을 공유함
서비스 모델	IaaS	• 서버, 프로세서, 네트워크, 스토리지 등 인프라스트럭쳐를 가상화 환경으로 만들어 필요에 따라 인프라 자원을 사용할 수 있도록 하는 서비스
	PaaS	• 이용자가 애플리케이션을 개발·테스트·구축할 수 있는 통합된 플랫폼을 제공하는 서비스로서, 이용자는 PaaS를 통해 새로운 애플리케이션을 개발하기도 하고, 다른 SaaS 서비스를 제공하기도 함

구분		주요 특징
서비스 모델	PaaS	• 사용자는 클라우드 인프라, 네트워크, 서버, 운영체제, 스토리지에 대한 관리/제어 권한 없지만 사용자가 구성한 애플리케이션과 호스팅한 애플리케이션 시스템 환경의 구성 및 관리 권한을 가질 수 있음
	SaaS	• 일정관리, 주소록, CRM용 프로그램, 오피스 프로그램 등 다양한 소프트웨어를 웹을 통해 임대해 사용할 수 있도록 제공하는 서비스 • 사용자에게 서비스의 환경 설정만 제한적으로 제공될 뿐 클라우드 인프라 등에 대한 관리 및 제어가 불가능

자료: 이창범(2010), 노병규·김형종(2012), Barrie Sosinsky(2011) 등을 토대로 재구성

(2) 클라우드 컴퓨팅의 장단점

클라우드 컴퓨팅은 기존 인터넷 기반의 컴퓨팅에 비해 경제성과 효율성 측면에서 주목할 만하다. 이용자 입장에서는 자신이 필요로 하는 컴퓨팅 인프라를 직접 소유할 필요가 없으므로, 자체의 인프라 장비(서버·네트워크…)나 소프트웨어를 구입할 필요가 없다는 점에서 비용이 절감된다. 또한 최소한의 용량으로 인터넷 사용이 가능한 곳이면 언제라도 서비스 제공자가 구축해 놓은 서버나 소프트웨어 등을 사용할 수 있다.[4] 국가적 차원에서는 탄소 배출량 감소, 에너지 사용전력 감소와 같은 그린 IT로서의 효과를 위해 클라우드 기술 도입을 강조하고 있으며, 기업 차원에서는 ICT 자원의 높은 활용률, 전력 및 비용 절감, 운영비용 절감, 장애복구의 편리성 및 비즈니스 연속성 등 다양한 이점이 제공된다.[5]

하지만 클라우드 컴퓨팅은 데이터의 중앙 집중 현상으로 인해 오히려 정보 누출의 위험이 증가하며, 데이터가 도처의 디바이스 및 저장 공간에 분산되어 저장되므로 보안의 커버리지가 광범위하다. 따라서 개인이 직접 데이터를 통제한다는 것은 사실상 불가능해지고, 이로 인해 사업자는 자신의 지배하에 민감정보, 개인정보 등을 통제할 수 있는 위치에 놓이게 된다. 여기에서 개인정보가 침해될 위험성이 발생한다.

4) 이창범(2011)
5) 임용재 외(2013)

3. 클라우드 컴퓨팅과 관련 정보보호법제의 현황 및 법적 쟁점

(1) 클라우드 컴퓨팅 관련 정보보호법제의 현황

1) 국내 현황

현재 국내법상 클라우드 컴퓨팅을 직접 규율하는 법률은 없지만, 클라우드 컴퓨팅 사업자는 정보통신망, 시스템 등을 사용하는 정보통신서비스 제공자로서 정보통신망법이 적용된다. 동법에서는 "개인정보의 이용제한(제24조), 개인정보의 제공 동의등(제24조의2), 개인정보의 취급위탁(제25조), 개인정보의 누출등의 통지·신고(제27조의3), 개인정보의 누설금지(제28조의2), 개인정보의 파기(제29조) 등" 클라우드 컴퓨팅의 서비스에 적용될 수 있는 정보보호 관련 조항들을 명문으로 규정하고 있다. 동법에서 특별히 규율하고 있지 않는 사항은 개인정보에 관한 일반법으로서 개인정보보호법이 적용된다. 다만, 정보통신망법이 정보통신서비스 제공자를 대상으로 하는 반면, 개인정보보호법은 공공·민간분야의 모든 개인정보처리자를 적용대상으로 한다는 점에서 차이가 있다. 그밖에 해당 서비스가 개인위치정보를 활용하거나 위치정보사업자·위치기반사업자가 서비스를 제공하는 경우에는 위치정보보호법이 적용된다. 참고로 현재 국회에 계류 중인 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」과 「클라우드 컴퓨팅 산업 진흥법」에서는 클라우드 컴퓨팅 관련 사업자의 인허가제도를 별도로 마련하고 있지 않기 때문에 법제정 이후에도 일반적인 개인정보법제가 적용될 것으로 보인다.

2) 해외 현황

해외의 법제를 살펴보아도 클라우드 컴퓨팅과 관련하여 직접적으로 규율하는 법률은 존재하지 않는다. 다만, 몇몇 국가에서 우리의 법체계와 마찬가지로 일반법으로서 정보보호와 관련한 법률을 두고 있다. 국가별로 살펴보면, 일반법이 없는 미국의 경우 정보보호를 엄격하게 강조하고 있지 않지만, 의료·금융 등의 개별 영역에서 개인정보를 보호하는 개별 법률을 두고 있다. 하지만 영국·독일·일본의 경우에는 데이터 및 개인정보의 보호에 관한 일반법 뿐 만 아니라 개별적인 법률도 마련하고 있다.[6] 해외 주요

국들의 ICT와 관련된 정보보호법제의 핵심적인 내용은 다음과 같이 요약해볼 수 있다.

〈표 2〉 주요국의 ICT 영역 정보보호법제 현황

국가	법률명	주요 내용
미국	ECPA (Electronic Communications Privacy Act of 1986)	• 전기통신 기록에 불법적으로 접근하거나 보유하고 있는 정보를 허가 없이 공개하는 것을 예방하기 위해 제정
	HIPPA (Health Insurance Portability and Accountability Act of 1996)	• 전자적 형태의 개인 의료정보보호를 의무화하여 의료기관이 정보보호를 위한 정책을 작성하고 시행할 것을 요구하고 있음
영국	Data Protection Law	• 데이터 등록기관 및 등록관을 두어 데이터 등록제를 운영하고 있으나, 사실상 허가제로서 ICT 활용이 증대됨에 따라 규제가 불가능하다는 인식발생
	Privacy and Electronic Communications (EC Directive)	• EU의 전자통신부문 프라이버시지침(2002/58/EC)을 반영하여 제정한 규칙으로서 쿠키 거부권, 개인정보보호, 트래픽정보 처리기준, 위치정보 처리기준 등을 규정하고 있음
독일	Telecommunication Act	• 2004년 제정한 법률로 정부기관의 기밀누설 방지, 데이터 안정성 확보 및 네트워크 침해 방지 등을 위해 정보통신사업자는 고객정보를 정부가 접근 가능하도록 할 의무를 규정하고 있음
	Federal Data Protection Act(BDSG)	• 개인정보의 정의규정을 비롯하여 제3국으로의 정보이전, 민감정보의 수집 등에 대한 내용을 포함하고 있으며, 2003년 EU 개인정보보호지침을 반영하기 위해 개정됨
일본	고도 정보통신 네트워크 사회 형성 기본법	• 네트워크 안정 및 신뢰성을 비롯하여 개인정보보호에 관한 기본적인 방침을 규율하고 있음
	특정 전기통신서비스제공자의 손해배상 책임 제한 및 발신자 정보의 개시에 관한 법률	• 2001년 제정된 법률로서 인터넷 상에서 송수신되는 정보에 의해 피해를 받은 경우 전기통신서비스제공자 등에 대한 배상책임에 대한 기준 등을 규정하고 있음

6) 참고로 EU의 경우에는 「정보보호지침(The Data Protection Directive(95/46/EC))」을 두고 있어 이에 따라 개별국가에서 입법을 하도록 하고 있으며, 최근 2012년에는 「일반정보보호법(General Data Protection Regulation)」을 제정하여 시행을 앞두고 있다. 후자의 경우에는 전자와 달리 법적 기속력을 발휘하게 된다.

(2) 클라우드 컴퓨팅 관련 법적 쟁점

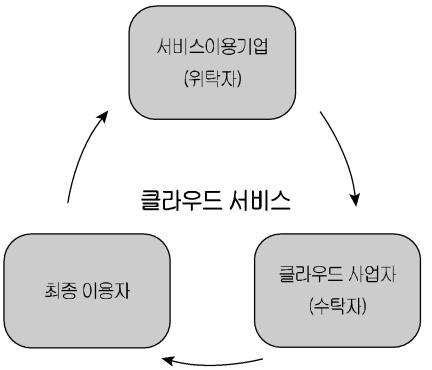
1) 개인정보의 취급위탁에 대한 위탁자의 관리 · 감독 책임 문제

클라우드 서비스를 이용하려는 기업이 클라우드 컴퓨팅 사업자와 IT업무 관련 위탁계약을 체결한 경우, 업무 중에 서비스가 중단되거나 데이터의 유출 및 훼손 등의 손해가 발생할 때 서비스이용기업은 최종이용자인 고객들을 상대로 계약상책임 혹은 불법행위책임을 질 수 있다. 〔그림 2〕와 같은 형태의 계약에서 서비스이용기업은 위탁자로서 정보통신망법상의 수탁자에 대한 관리·감독 의무를 가진다(정보통신망법 제25조 제4항). 또한 서비스이용기업은 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 법을 위반하여 이용자에게 손해를 발생시킬 경우 정보통신서비스제공자등의 소속 직원으로 보아 동조상의 책임을 지게 된다(동조 제5항). 이와 같은 개인정보 취급에 대한 위탁자의 관리·감독 의무 등의 책임은 클라우드 서비스를 이용하는 기업의 입장에서는 부담으로 작용할 수 있다. 다만, 최근 법개정을 통해[7] "이용자 편의 증진 등을 위하는 경우"를 조문에 추가하여 해당 경우에는 고지절차 및 동의절차를 생략할 수 있도록 하고 있다(동조 제2항).

하지만 클라우드 서비스의 경우, 일반적인 IT업무 위탁계약과는 다르게 위탁자가 도처에 분산되어 있는 서버 및 데이터 센터를 관리·감독하는 것이 현실적으로 어렵다고 보인다. 따라서 클라우드 컴퓨팅의 경우에는 동 조항의 적용을 완화하여 해석하거나, 예외 규정을 추가적으로 제정하는 방안을 고려해 볼 필요가 있다.

7) 정보통신망법 제25조(개인정보의 취급위탁) ② 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 〈개정 2014. 5. 28〉

〔그림 2〕 클라우드 컴퓨팅 서비스의 위탁관계



2) 개인정보의 국외 이전에 따른 법적 쟁점

전 세계적으로 상당한 규모의 이용자를 확보하고 있는 MS(Azure), 아마존 웹서비스(AWS), 구글(Docs)등 해외 서비스를 이용할 경우, 클라우드 사업자가 해외에 관련 서버 또는 전산센터를 두고 있어 사실상 국내법의 적용이 어렵게 된다. 이러한 현실적 한계가 노정됨에 따라 정보 유출 사건이 해외에서 발생할 경우 국내 이용자들의 개인정보가 침해될 수 있다는 우려가 발생한다.

이 같은 문제는 EU 법체계 하에서도 동일하다. 「EU 개인정보보호지침」[8]은 EU 영역 외에서 정보를 수집, 처리 및 저장하는 것을 원칙적으로 금지하고 있다. 다만, 예외적으로 정보보호수준의 적절성이 확정된 경우에는 정보보호 관련 조항을 적용할 수 있다(EU 개인정보보호지침 제25조·제26조). 여기에서 개인정보를 국외로 이전하기 위해서는 상대국가의 법이 자국법보다 더 개인정보를 보호하거나 계약 체결에 의해 개인정보보호를 위한 안전장치(Safe Harbor)를 확보해야 한다. EU집행위원회는 캐나다, 스위스, 아르헨티나 등 몇몇 국가들은 적절한 정보보호수준을 확보한 것으로 판단하여 EU 회원국과 동일하게 법적용이 가능하다. 그런데 미국의 경우 정보보호의 정

8) '개인정보보호지침(Directive 95/46/EC)'은 회원국 간에 개인정보의 자유로운 유통이 제한 또는 방해되지 않도록 하는 것을 목적으로 제정한 지침으로서 개별 국가에서 입법을 하는데 있어 기준이 되는 지침이다.

도가 낮기 때문에 EU는 미국과 일정 원칙을 준수하는 프라이버시 정책을 공개하도록 하는 Safe Harbor 협정[9]을 채택하여 이를 준수하는 기업은 적절한 보호 조치를 취한 것으로 간주하여 이러한 문제를 해결하고 있다.

독일의 경우에도 클라우드 제공자의 거주지가 EU 내에 존재하고 당해 정보가 EU 내에서 처리되는 경우에 한하여 정보보호의 주체로서 보호받을 수 있다(독일 연방정보보호법 제3조 제8항). 예컨대, 미국에 주된 사무소를 두고 있는 클라우드 제공사업자는 독일에 클라우드 컴퓨팅 제공 사업지를 두고 있다고 하더라도 미국의 정보보호 법제가 적용된다. 독일 연방정보보호법은 정보의 국외 이전은 특별히 정당성을 요구하고 있으며, 이에 따라 정보의 수취인은 적절한 정보보호 수준을 담보하여야 한다(독일 연방정보보호법 제4조 제2항·제3항). 독일 연방정보보호법은 안전하지 않은 제3국의 서비스제공자는 제3자로 간주하여(연방정보보호법 제3조 제8항 제3문), 이러한 제3자의 경우에는 이에 상응하는 동의가 존재하는 경우에만 허용된다.[10]

이와 같이 자국 내 영역에 법 적용이 미치는 속지주의의 원칙을 적용하므로 해외로 이전 되는 개인정보의 경우에는 해외법제의 정보보호 정도에 따라 보호받지 못하는 법적 불안정성이 발생한다. 따라서 이러한 해외 이전 정보에 대한 보호 미비는 자국 이익을 심각하게 침해할 수 있으며, 정보 침해자의 우회적인 침해양태를 유발할 수 있다.

EU와 미국 간의 정보이전에 관한 이슈는 우리 법제에도 시사하는 바가 크다고 할 수 있다. 정보통신망법 제63조는 개인정보의 국외 이전과 관련하여 이용자의 개인정보에 관하여 국외로 이전하려면 이용자의 동의를 받아야 하며, 제63조 제3항의 각 호[11]의 사항을 이용자에게 고지하도록 하고 있다. 현행법상 단순히 데이터센터 등을

9) 세이프하버 원칙은 "① 정보 수집 시 통지, ② 개인의 정보 수집 기피 선택권 보장, ③ 명시적인 동의 없이 수집된 정보의 이전 금지, ④ 수집된 정보의 보안, ⑤수집된 정보의 온전성, ⑥ 수집된 정보에 대한 개인의 열람권 보장, ⑦ 상기원칙의 집행"을 제시하고 있다(윤혜선, 2013).

10) 박종수(2014).

11) 정보통신망법 제63조(국외 이전 개인정보의 보호) ③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.
1. 이전되는 개인정보 항목

물리적으로 해외에 두는 것을 개인정보의 국외이전으로 해석할 수 있는지 해석상 논란이 있다.[12] 이러한 부분을 입법적으로 명확히 하여 해결할 필요가 있다.

4. 결 어

2011년 제정·시행된 개인정보보호법을 비롯하여 정보통신망법, 위치정보법 등 정보보호에 관한 개별 법률들은 개인정보의 보호 일변도로 법률을 개정하고 제도를 확충해왔다. 예를 들어, 법정손해배상제도, 주민등록번호의 수집 금지 원칙, 개인정보 유출 통지제도 등을 추가적으로 도입하면서, 개인정보의 수집, 이용, 제공, 관리 등이 더욱 어렵게 되었다. 하지만 IoT, 빅데이터, 클라우드 등의 인터넷 신산업들은 개인정보의 활용이 없이는 서비스 개시가 어렵다는 점에서 개인정보의 '보호'와 '활용'의 측면이 상충된다. 정보보호에 대한 엄격한 법·제도 규율은 신생기업들에게는 시장에 대한 진입장벽으로 작용하게 될 것이고, 이러한 엄격한 규제환경에서는 국내 기업이 Facebook, Twitter 등과 같이 글로벌 기업으로 성장하기 어렵게 된다.

따라서 현행 법체계하에서 정보 활용 산업을 활성화기 위한 입법론적 방안으로 정보통신망법 등에서 규정하고 있는 예외 조항"[13]을 근거로 타 법률에 개인정보의 수집 및 활용을 완화하는 관련 조항을 신설하는 방안이 있다. 하지만 정보보호에 대한 규율의 약화는 이용자들의 개인정보자기결정권(데이터 통제권) 침해로 이어질 수 있다는 점에서 정보 유출 및 침해발생 시 강력한 이용자 구제책이 수반되어야 한다. 이를 위해 손해배상청구권, 과징금제도[14]등 개인정보침해에 대한 처벌 규정의 강화를 강구해

---

2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

12) 이창범(2010)

13) 여기서 '예외조항'이라 함은 "타 법률에 규정이 있는 경우 예외적으로 고지 및 동의절차 등을 면제하도록 하는 조항"을 말한다. 예를 들어, 정보통신망법 제22조 제2항 제3호에서는 타 법률에 특별한 규정이 있는 경우 동의 없이 개인정보를 수집·이용할 수 있다는 조문을 두고 있다.

볼 만하다. 이를테면, 법정손해배상제도[15]의 도입에서 나아가 징벌적 손해배상제도[16]를 도입하거나, 집단소송제도를 보완하는 것이다. 이러한 손해담보 수단의 보장을 통해 기업의 입장에서는 막대한 손해배상금 및 과징금에 대한 우려로 자율적으로 정보보호 시스템을 구축할 것이고, 최종이용자인 피해자 입장에서는 징벌적 손해배상을 통해 고의침해를 예방하는 등 손해전보에 대한 구제수단이 확보된다. 이와 같은 법체계로의 전환을 통해 클라우드 컴퓨팅 산업의 활성화를 지원하고, 동시에 이용자의 손해를 강력히 담보하는 것이 가능할 것이다.

이상에서 살펴본 바와 같이 개인정보에 관한 법적 미제들로 인해 성장가치가 높은 정보산업의 발전이 저해되는 상황이 발생해서는 안 될 것이다. 특히, 클라우드 컴퓨팅의 경우 정보의 국외 이전 문제와도 결부되어 있는 만큼, 국가 간 정보보호 수준을 조율하고 공조체제를 형성하는 데에도 국가적 차원에서의 노력이 필요하다.

---

14) 기존 정보통신망법상 과징금 제도는 제64조의3 제1항의 각 호에 해당하는 위반행위가 있는 경우 관련 매출액의 100분의 1이하의 과징금을 부과하도록 하고, 단서 구문에서 동조 동항 제6호(제2호 내지 제5호의 조치를 취하지 아니하여 이용자 개인정보를 분실·도난·누출·변조 또는 훼손한 경우)에 해당하는 경우 기술적·관리적 보호조치 미비와 유출사고와의 인과관계의 입증을 통해 1억 이하의 금액을 부과할 수 있도록 규정하였다. 하지만 2014년 11월 29일부로 시행되는 개정안(법률 제12681호)에서는 단서를 삭제하고, 개인정보 위반행위가 있을 경우 일률적으로 관련 매출액의 100분의 3 범위내로 과징금의 한도 금액을 확대하였다.

15) 개인정보의 유출로 인한 손해액 산정의 경우 구체적인 손해액을 입증하는 것이 어렵기 때문에 개인정보 유출로 인한 손해액을 입증하지 않더라도 최대 300만원의 범위 내에서 손해배상청구가 가능하도록 하는 '법정손해배상제도'를 도입하였다. 이러한 제도의 도입으로 인해 위자료 명목으로 20만원 내외의 소단위 금액만을 구제받았던 피해자들이 적극적인 구체조치를 취할 수 있게 되었다. 민법상 손해배상청구권이 존재함에도 이와 같이 별도의 손해배상제도를 도입하는 것은 계약을 통해 손해배상을 무마시키는 것을 방지할 수 있다는 점 때문이다.

16) '징벌적 손해배상제도'는 가해자가 악의적으로 불법행위를 한 경우(고의침해) 징벌을 목적으로 실제 손해액을 넘는 금액으로 가액하여 배상하도록 하는 제도이다.

참고문헌

Barrie Sosinsky (2011). Cloud Computing Bible 757, John Wiley & Sons Inc.

Christopher Barnatt (2010). *A Brief to Cloud Computing*, Robinson Publishing.

노병규·김형종 (2012), "클라우드 컴퓨팅 동향 및 정보보호 이슈", 「PM Issue Report」, 2012-제1권 이슈3, 한국방송통신전파진흥원.

박종수 (2014), "클라우드 컴퓨팅과 정보보호", 「법제연구」, 제46호.

방송통신위원회 (2012), "민간 부문의 클라우드 도입 실무 가이드라인 - 퍼블릭·프라이빗 클라우드를 중심으로".

유우영·임종인 (2012), "클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구", 정보보호학회논문지, 제22권 제2호.

윤혜선 (2013), "클라우드 컴퓨팅 환경에서 개인정보 보호에 제기되는 도전", 「경제규제와 법」, 제6권 제1호.

이창범 (2010), "클라우드 컴퓨팅의 안전한 이용과 활성화를 위한 법적 과제", 「정보보호학회지」, 제20권 제2호.

임용재·백선경·정성인·원희선 (2013), "스마트인터넷 서비스를 위한 클라우드와 빅데이터", 「PM Issue Report」, 2013-제3권 이슈1, 한국방송통신전파진흥원.

http://www.nist.gov/

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf