클라우드 컴퓨팅과 정보보호

박 종 수*

차 례

* 고려대학교 법학전문대학원 교수, 법학박사.
접수일자 : 2014. 5. 30. / 심사일자 : 2014. 6. 20. / 게재확정일자 : 2014. 6. 25.

Ⅰ. 서 론

최근 인터넷 신산업이라 하면 빅데이터, 사물인터넷(IoT)와 더불어 클라우드 컴퓨팅을 떠올리게 된다. 클라우드 컴퓨팅 또는 클라우드 서비스란 ICT기술의 발전에 따라 가상화 기법이 실용화되어 가상의 공간에 정보를 저장하고 원하는 시기에 원하는 정보를 편리하게 이용할 수 있도록 하는 인터넷 서비스를 의미한다고 정의할 수 있다. 더욱이 스마트 혁명의 도래에 따라 마침내 온라인으로 저장된 문서나 정보를 인터넷에 연결될 수 있는 거의 모든 기기(단말)를 통해 전세계 어디에서나 접근할 수 있는 세상이 되었다. 아이디, 비밀번호 등 접속정보만 입력하면 동료나 친지들도 언제나 클라우드 정보(Cloud-Daten)에 접근할 수 있다. 이처럼 정보를 클라우드에 저장할 수 있다는 것은 기업이나 일반 사인들에게는 매우 매력적인 대상이 아닐 수 없다.

그러나 클라우드 컴퓨팅에 있어서 개인관련 정보처리와 관련해서는 아직 충분히 해결되지 못한 법적 및 기술적 문제들이 제기되고 있다. 그 중의 하나가 정보보호(Datenschutz)의 문제이다. 이러한 새로운 형태의 정보처리 방식은 점점 더 애용될 수밖에 없기 때문에 이 문제에 대하여 적절히 대응하기 위해서는 점차 발전하는 클라우드 컴퓨팅에 대하여 국내 정보보호 법제를 적용함에 있어서 아무런 문제는 없는지 검토하여야 할 것이며, 특히 클라우드 컴퓨팅의 제공과 이용은 흔히 국경을 넘어 이루어지는 성향을 보이고 있는바, 그러한 국제적 클라우드 컴퓨팅 이용시의 정보보호 문제와 그 해결책에 대한 고민도 필요한 시기이다.

이하에서는 이러한 문제의식을 바탕으로 최근의 ICT트렌드로서의 클라우드 컴퓨팅의 의의를 살펴보고(Ⅱ.), 국내 정보보호법제를 개관하여 클라우드 컴퓨팅에 적용가능한 정보보호법제의 내용을 살펴보고(Ⅲ.) 국제적 클라우드 컴퓨팅 이용시의 정보보호에 관한 독일 및 유럽연합의 사례를 살펴봄으로써(Ⅳ.) 향후 제도개선을 위한 법제개선의 방향을 제시(Ⅴ.)하는 것을 목표로 삼고자 한다.

Ⅱ. 새로운 ICT 트랜드로서의 클라우드 컴퓨팅 - 기회와 위험

1. 클라우드 컴퓨팅의 개념

오늘날과 같은 다양한 소프트웨어와 하드웨어 솔루션들 그리고 가상화 기술의 이용가능성은 ICT산업이 효과적으로 그리고 탄력적으로 구축될 수 있도록 해 줄 수 있는 많은 새로운 가능성을 제공한다. 클라우드 컴퓨팅이 그 하나이다.[1)]

그런데 클라우드 컴퓨팅이란 무엇인가? 이것이 과연 구름과 관련이 있는가? '클라우드'라는 표현은 인터넷에 대한 은유적 표현으로, 통신망-위치(Topologie)를 묘사할 때 인터넷을 구름(클라우드)으로 설명하는 것에 근거하고 있다. 구름의 모습은 가령 형태는 없으나, 그렇다고 해서 포착될 수 없는 것은 아님을 의미한다. 그러나 구름의 모습은 모든 통신망 묘사에서 필요한데, 왜냐하면 오늘날에는 통신망이 대부분 인터넷을 통하여 외부세계와 연결되기 때문이다. 아직도 구름을 이용하여 이러한 인프라 구조의 복잡성을 묘사하곤 한다. 이 경우 예를 들어 서버, 데스크탑, 응용프로그램 또는 메모리(Speicherplatz) 등의 자원들은 클라우드 컴퓨팅 제공업체에 역동적으로 확장(스케일링)이 가능한 그리고 대부분 가상화된 자원들의 형식으로 존재하고 있으며, 인터넷을 통해서 서비스로 제공된다. 그 접속은 웹브라우저를 이용한 인터넷을 통하여 이루어지며, 그 이용자에게는 어떤 특별한 지식도 요구하지 않는다.

IBM에 의한 클라우드 컴퓨팅의 개념정의에 의하면 클라우드 컴퓨팅은 데이터처리를 위한 두드러진 패러다임의 변화로서, 이 경우 데이터와 서비스는 극도로 확장(스케일링)이 가능한 중앙컴퓨팅센터에 존재하며, 인터넷에 연결되어 있는 단말기를 통해서 언제나 접속될 수 있다. 극도로 확장이 가능한 컴퓨팅서비스가 응용프로그램의 경우에도 또 그 응용 자체를 위해 호스팅(Hosten)하는 경우에도 제공된다. 따라서 구름의 형식으로 인터넷을 나타내는 이 상징은 그 체재의 중요한 구성요소를 이루는 것임을 알 수 있다.

---

1) Nägele/Jacobs, Rechtsfragen des Cloud Computing, ZUM 2010, 281.

2. 클라우드 컴퓨팅의 유형

클라우드 컴퓨팅은 다음과 같이 몇 가지로 유형화해볼 수 있다.

(1) 서비스로서의 소프트웨어(SaaS)

이는 하나의 호스트를 통해 - 중앙에서 관리되고, 보통 인터넷을 거쳐서 접속되는 - 응용프로그램들을 사용할 수 있게 해 준다. 따라서 그 응용을 관리하는 것은 온전히(komplett) 제공업체 자신을 통해서 넘겨받게 되는 것이지, 이용자를 통해서 넘겨받게 되는 것이 아니다. 이에 대한 하나의 예로 세일즈포스(Salesforce)를 들 수 있다.

(2) 서비스로서의 플랫폼(PaaS)

이는 클라우드 컴퓨팅을 토대로 하여 실행플랫폼뿐 아니라 개발플랫폼도 제공한다. 따라서 응용프로그램의 개발과 옮겨 보내기(Rollout)는 그 기반이 되는 복잡한 하드웨어와 소프트웨어에 대한 비용이나 복잡함을 들이지 않고도 간단하게 실행될 수 있다.

(3) 서비스로서의 인프라구조(IaaS, 서버·데스크탑·스토리지)

이 모델은 "서비스로서의 모든 것"을 제공하고 있으며, 서버, 통신망구성요소들, 메모리, CPU, 메모리와 전산센터(Rechenzentrum) 등을 포함한다. 이 경우 전형적인 특성들로는 그 필요에 상응하는 자원들의 역동적인 확장성, 다양한 비용, 위임자의 능력(더 많은 고객들이 인프라구조자원들을 함께 사용한다)과 매우 작은 규모의 단체들까지도 이용할 수 있는 산업-인프라구조 등이 있다.[2)]

3. 클라우드 컴퓨팅의 장점과 단점 - 기회와 위험

세계 Public 클라우드 시장은 2012년 373억불[3)]에서 2017년 1072억불로

2) 이상 클라우드 컴퓨팅의 유형에 대해서는 Nägele/Jacobs, Rechtsfragen des Cloud Computing, ZUM 2010, 282.

성장할 것으로 전망된다. 비교하여 국내의 경우는 2012년 3.4억불에서 2017년 11.7억불로 성장할 것으로 기대된다. 클라우드 컴퓨팅은 빅데이터나 IoT와 접목되어 다양한 융합 신산업을 촉발시킬 수 있는 촉매제의 역할을 할 수 있을 것으로 기대되고 있다.[4)]

클라우드 컴퓨팅의 가장 중요한 경제적 장점은 유연하고 수요 지향적인 제공과 이용자를 위해 즉시 필요한 IT 설비의 이용가능성이다. 즉, 최고부하 시점이 아닌 때에는(in Nebenzeiten) 최고부하 시점(in Spitzenzeiten)에서와 같이 많은 연산처리능력과 소프트웨어가 항시 준비되어 있어야만 하는 것은 아니다. 이와 비교하여 보면 대부분의 기업들은 지속적으로 변동하는 노동자 수에 근거하여 소프트웨어 할당량(Softwarekontingente)과 이에 상응하는 라이선스들을 매번 정확히 필수적 수요에 상응하는 노동자 총수에 지속적으로 맞추어 준비할 수 없고, 따라서 대부분의 기업들은 신중함과 법적안정성을 근거로 대개 라이선스를 더 많이 받는 상태이다. 클라우드 컴퓨팅은 또한 이와 같은 관점에서 프로젝트 지향적인 구체적인 서비스의 제공이 요구될 수도 있기 때문에 수요 기반적 사용 가능성을 통하여 법적안정성, 보다 높은 유연성과 보다 낮은 비용을 가능하게 한다. 특히 클라우드 컴퓨팅 방식의 ICT 어플리케이션들의 외주를 통해, 최종 소비자로서 어플리케이션에 관련된 영업 리스크가 클라우드 제공자에게 이양되고 또한 하드웨어와 소프트웨어를 기다리는 소비가 줄게 된다. 또한 클라우드 컴퓨팅에서는 새로운 소프트웨어 버전의 구매와 이와 관련된 기존 시스템과의 통합 및 적응의 문제가 사라지게 된다.[5)]

그러나 클라우드 컴퓨팅에는 장점만 있는 것은 아니다. 클라우드 솔루션의 단점으로서 무엇보다 데이터저장과 관련한 충분히 투명하지 못한 안전성 문제 및 서비스의 안정성, 비용과 관련하여 발생 가능한 부정적 효과와 어플리케이션의 통합과 관련된 문제점 및 클라우드간의 연계작동(호환성)과 관련된 문제점이 거론된다. 또한 데이터와 프로세스에 대한

3) PWC, Cloud Computing, Navigation in der Wolke, 2012, S. 15 f.

4) 이인용, 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률안(정부제출) 검토보고서, 6쪽 이하.

5) Thilo Weichert, Cloud Computing und Datenschutz, DuD 2010, 679 f.

통제의 상실이 종종 보안기술적 문제로 간주되기도 한다.[6]

상기와 같은 장점이 많음에도 불구하고 기업들이 선뜻 클라우드 솔루션을 도입하지 못하는 주된 이유는 정보보호 및 보안의 문제라고 한다. 클라우드를 장미빛으로만 보게 되면 이는 마치 기회의 땅처럼 여겨질 수 있다. 그러나 그러한 기회만 있는 것이 아니라 여러 가지 위험요소가 내재하고 있음을 유의하여야 한다.[7]

최근 국내적으로는 KB, 농협, 롯데 등 카드사의 개인정보 유출사태가 벌어지면서 개인정보의 보호 및 보안관련 제도가 대폭 강화되는 기폭제가 된 바 있다. 이는 한편으로는 개인정보의 보호가 강화된다는 측면이 있기는 하지만 개인정보를 활용하거나 이용하여야만 하는 산업의 측면에서는 재앙과도 같은 일이었다. 높은 보안 수준과 위험관리 수단을 제공하는 것이 클라우드 컴퓨팅의 도입 및 발전을 위한 전제조건이 되는 것은 분명하다. 그러나 너무 높은 수준의 정보보호 강조는 자칫 발전의 초기에 있는 클라우드 산업의 운신을 지나치게 제약할 가능성이 있다. 향후 정보보호법제의 발전방향을 논함에 있어서 짚고 넘어가야 할 관점이라고 생각한다.

Ⅲ. 클라우드 관련 정보보호법제의 내용과 문제점

1. 국내 정보보호법제의 체계 - 일반법과 개별법의 구도

(1) 헌법적 가치로서의 정보보호

정보, 그 중에서도 개인 관련 정보(개인정보)는 헌법상의 기본권인 사생활의 보호에 근거한다. 헌법재판소는 개인은 자신에 관한 정보가 언제 누구에세 어느 범위까지 알려지고 또 이용되도록 할 것인지를 스스로 결정할 수 있는 권리, 즉 '개인정보자기결정권'을 가진다고 판시한 바 있다.[8]

---

6) Nägele/Jacobs, Rechtsfragen des Cloud Computing, ZUM 2010, 283.

7) Aufsichtsstelle Datenschutz Basel-Landschaft, Merkblatt "Cloud Computing", 2012.

① 개인정보자기결정권의 의의

개인정보자기결정권이란 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 헌법재판소는 개인정보자기결정권의 보호 대상이 되는 개인정보는 “개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다”고 하여 개인정보의 범위를 비교적 넓게 파악하고 있다.[9] 아울러 이러한 “개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다”고 하여 개인정보주체의 보호 범위도 그에 상응하여 넓게 파악하고 있다.[10]

② 개인정보자기결정권의 헌법상 근거

개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려하는 입장도 있을 수 있다.

그러나 헌법재판소는 개인정보자기결정권으로 보호하려는 내용을 위각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하

8) 류지태/박종수, 행정법신론, 2011, 435쪽.

9) 헌법재판소 2005. 5. 26. 선고 99헌마513 결정.

10) 헌법재판소 2005. 5. 26. 선고 99헌마513 결정. 이는 현대사회에서 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 된 상황에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치라고 판단한 것으로 이해할 수 있다.

다고 보아 그 헌법적 근거를 굳이 어느 한 두개에 국한시키는 것은 바람직하지 않다고 보고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 한다고 보고 있다.[11)]

(2) 정보보호법 체계 개관

현행 정보보호법 체계는 일반법인 「개인정보보호법」과 특별법인 개별 영역별 정보보호 법제로 나누어 볼 수 있다.

먼저 개인정보보호 일반에 대해서는 안전행정부 소관의 『개인정보보호법』이 규율하고 있다. 동법은 개인정보처리자가 정보주체의 개인정보를 처리하는 것에 대하여 적용하는바, 여기서 '처리'란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말하며, '개인정보처리자'란 업무를 목적으로 개인정보파일[12)]을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다. 개인정보보호법은 온라인 및 오프라인 사업자, 근로자, 비영리단체(동창회, 협회 등) 및 공공기관 등 넓은 범위를 적용대상으로 포함한다. 특히 수집에 대해서는 수집 목적 등 고지, 사전동의 획득 후 수집, 주민등록번호의 수집 제한 등을 규정하고 있으며, 이용/제공에 대해서는 목적 외 이용 및 동의 없는 제3자 제공 금지 등을 규정하고 있다. 개인정보에 관한 일반행정의 집행은 안전행정부가 맡아 수행하지만, 개인정보보호에 관한 사항(정책)의 심의·의결은 대통령 소속의 개인정보보호위원회가 담당한다.

이와 달리 정보통신, 금융, 의료, 교육 분야 등에는 해당 개별 영역별로 정보보호에 대하여 규정하는 법체계가 별도로 존재하고 있는바, 정보통신 분야에는 대표적으로 방송통신위원회 소관 법률로서 『정보통신망 이용촉

11) 헌법재판소 2005. 5. 26. 선고 99헌마513 결정.

12) "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.

진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”이라 한다)과 「위치정보의 보호 및 이용 등에 관한 법률」(이하 “위치정보법”이라 한다)이 있다. 정보통신망법은 정보통신서비스제공자가 개인정보를 수집하는 경우를 적용범위로 하며, 따라서 정보통신서비스제공자를 적용대상으로 한다. 위치정보법은 위치정보사업 및 위치기반서비스사업을 영위하는 자가 개인위치정보를 수집하는 것을 적용범위로 하며 따라서 위치정보사업자 및 위치기반서비스사업자를 적용대상으로 한다.

이상의 정보통신 분야 정보보호법제의 체계와 내용을 도표로 정리하면 다음과 같다.

구분	법령	조문별 주요내용	소관부처
일반법	개인정보 보호법	**제3장 개인정보의 처리** 제15조(개인정보의 수집·이용) 제16조(개인정보의 수집 제한) 제17조(개인정보의 제공) 제18조(개인정보의 이용·제공 제한)[13] 제19조(개인정보를 제공받은 자의 이용·제공 제한) 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) 제21조(개인정보의 파기) 제22조(동의를 받는 방법) 제23조(민감정보의 처리 제한) 제24조(고유식별정보의 처리 제한) 제24조의2(주민등록번호 처리의 제한) 제26조(업무위탁에 따른 개인정보의 처리 제한) 제27조(영업양도에 따른 개인정보의 이전 제한) 제5장 정보주체의 권리 보장 제35조(개인정보의 열람) 제36조(개인정보의 정정·삭제) 제37조(개인정보의 처리정지 등) 제38조(권리행사의 방법 및 절차) 제39조(손해배상책임)	안전행정부 개인정보보호 위원회
특별법	정보통신망법	**제4장 개인정보의 보호** 제22조(개인정보의 수집·이용 동의 등)	방송통신위원회

		제23조(개인정보의 수집 제한 등) 제23조의2(주민등록번호의 사용 제한) 제23조의3(본인확인기관의 지정 등) 제23조의4(본인확인업무의 정지 및 지정취소) 제24조(개인정보의 이용 제한) 제24조의2(개인정보의 제공 동의 등) 제25조(개인정보의 취급위탁) 제26조(영업의 양수 등에 따른 개인정보의 이전) 제26조의2(동의를 받는 방법) 제27조(개인정보 관리책임자의 지정) 제27조의2(개인정보 취급방침의 공개) 제27조의3(개인정보 누출등의 통지·신고) 제28조(개인정보의 보호조치) 제28조의2(개인정보의 누설금지) 제29조(개인정보의 파기) 제30조(이용자의 권리 등) 제30조의2(개인정보 이용내역의 통지) 제31조(법정대리인의 권리) 제32조(손해배상) 제32조의2(법정손해배상의 청구)	
	위치정보법	**제3장 위치정보의 보호** 제15조(위치정보의 수집 등의 금지) 제16조(위치정보의 보호조치 등) 제17조(위치정보의 누설 등의 금지) 제18조(개인위치정보의 수집) 제19조(개인위치정보의 이용 또는 제공) 제20조(위치정보사업자의 개인위치정보 제공 등) 제21조(개인위치정보 등의 이용·제공의 제한 등) 제22조(사업의 양도 등의 통지) 제23조(개인위치정보의 파기 등) 제24조(개인위치정보주체의 권리 등) 제25조(법정대리인의 권리) 제26조(8세 이하의 아동 등의 보호를 위한 위치정보 이용) 제27조(손해배당) 제28조(분쟁의 조정 등)	

이상 위 표에서 보는 바와 같이 정보통신망법과 위치정보법은 각각 정보통신 분야의 특별법으로서 동일 사항에 대하여 「개인정보보호법」과 상충된 내용이 있을 시에는 일반법인 「개인정보보호법」에 대하여 우선 적용하는 관계에 있다. 「개인정보보호법」 제6조에서도 “개인정보보호에 관하여는 다른 법률에서 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다”고 하여 이를 명확히 하고 있다.

위 표에서 개관해보는 바와 관련하여 분명하게 알 수 있는 것은 정보보호 추진체계가 안전행정부 및 개인정보보호위원회와 방송통신위원회로 이원화되어 있다는 것이다. 이는 통일적인 추진체계 내지 콘트롤타워가 부재하다는 지적과 함께 정보보호정책의 추진에 있어서도 효율성이 떨어질 수 있다는 지적을 충분히 설득력 있게 보이게 한다. 클라우드만 보더라도 오늘날 정보보호 문제는 「개인정보보호법」이 공공과 민간을 모두 아우르는 범위를 적용대상으로 하는 바와 마찬가지로 단순히 전자정부의 카테고리속에서만 파악할 수는 없다. ICT분야의 전문규제기관이 아울러 정보보호 규제를 함께 관장하도록 함으로써 규제의 통일성과 효율성을 동시에 추구하도록 제도화하는 것이 중장기적으로는 바람직하다고 판단된다.

2. 국내 정보보호법제의 주요 내용

앞에서 정보보호법제의 틀을 표로 정리하여 보았지만 그 주요한 최근 내용을 정보통신망법을 중심으로 정리해보면 아래와 같다.

(1) 개인정보 수집 원칙

정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 원칙적으로 ① 개인정보의 수집·이용 목적, ② 수집하는 개인정보의 항목, ③ 개인정보의 보유·이용 기간 등 모든 사항을 이용자에게 알리고 동의를 받아야 한다(제22조).

---

13) 2013. 8. 6. 조문제목이 개정되어 2014.8.7. 이후로는 “제18조(개인정보의 목적 외 이용·제공 제한)”으로 변경된다.

그러나 이러한 원칙에 대하여 예외적으로 일정한 경우에는 동의 없이 이용자의 개인정보를 수집·이용할 수 있도록 하고 있다. 그러한 경우로 제22조 제2항에서 열거하고 있는 사항은 ① 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우, ② 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우, ③ 이 법 또는 다른 법률에 특별한 규정이 있는 경우 등이다. 2007년 법 개정 전 제22조 제2항은 “정보통신서비스 제공자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 각 호의 사항을 이용자에게 고지하거나 정보통신서비스이용약관에 명시하여야 한다”고 규정하고 있었다. 현행 법은 원칙과 예외의 체계를 갖추어 동의 없이 개인정보를 수집·이용할 수 있는 경우를 명시하여 규정하였다는 점에서 과거 보호 위주의 규정체계에서 활용 및 이용의 측면을 향하여 방향을 약간 선회하였다는 점에서 그 의미를 평가할 수 있을 것 같다.

(2) 민감정보의 수집·사용 제한

정보통신망법 제23조에 의하면 정보통신서비스 제공자는 사상, 신념, 가족 및 친인척관계, 학력·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조 제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다. 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 범위에서 최소한의 개인정보만 수집하여야 하며 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.

한편 민감정보 중 주민등록번호에 대해서는 정보통신서비스 제공자는 ① 본인확인기관으로 지정받은 경우, ② 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우, ③ 영업상 목적을 위하여 이용자의 주민등록

번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우가 아니면 이용자의 주민등록번호를 수집·이용할 수 없다(제23조의2). 또한 ②와 ③에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법을 제공하여야 한다. 주민등록번호와 관련해서 개정전 제23조의2는 “① 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신망을 통하여 회원으로 가입할 경우에 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다. ② 제1항에 해당하는 정보통신서비스 제공자는 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택하게 할 수 있다”고 규정하고 있었으나 주민등록번호의 남용이 심각한 사회문제로 대두되는 점을 반영하여 원칙적 사용금지로 방향을 선회한 것이다.

주민등록번호에 대해서는 일반법인 「개인정보보호법」에서도 관련 규정을 두고 있는데, 2014년 8월 7일부터 시행되는 개정 「개인정보보호법」제24조의2는 “개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다”고 규정하면서 그 각 호로서 ① 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우, ② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우, ③ 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우를 규정하고 있다. 나아가 실효성 확보를 위하여 주민등록번호 유출 등의 경우에는 5억원 이하의 과징금을 부과할 수 있도록 하였고(「개인정보보호법」 제34조의2 제1항), 안전행정부장관의 징계권고 대상에 개인정보처리자의 대표자(CEO) 및 책임 있는 임원이 포함됨을 명시하였다(「개인정보보호법」 제65조 제2항).

(3) 개인정보 이용내역 통지제도

정보통신망법 제30조의2에 따르면 일정한 정보통신서비스 제공자등은

수집한 이용자 개인정보의 이용내역을 주기적으로 이용자에게 통지하여야 한다. 구체적인 정보의 종류, 통지 주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정하도록 하고 있는데, 수집대상은 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다)매출액이 100억원 이상인 정보통신서비스 제공자이며, 통지항목은 ① 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목, ② 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제, ③ 법 제25조에 따른 개인정보 취급위탁을 받은 자 및 그 취급위탁을 하는 업무의 내용 등이다. 통지 주기 및 방법은 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 연 1회 이상 하도록 하고 있다.

(4) 개인정보 누출 통지·신고 제도

한편 정보통신망법 제27조의3에 따르면 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 "누출등"이라 한다) 사실을 안 때에는 지체 없이 ① 누출등이 된 개인정보 항목, ② 누출등이 발생한 시점, ③ 이용자가 취할 수 있는 조치, ④ 정보통신서비스 제공자등의 대응 조치, ⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 등의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

(5) 손해배상

정보통신망법 제32조에 의하면 “이용자는 정보통신서비스 제공자등이 이 장의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.”

고 하여 손해배상에 대하여 특별히 규정하고 있다. 이는 손해배상이 민사상 손해배상으로만 규율될 경우 손해배상에 관한 사항을 계약에 넣어 이용자의 손해배상청구권을 계약에 의하여 무력화하게 되는 것을 막기 위하여 법률규정으로 특별히 손해배상에 대하여 명문의 규정을 둔 것이다.

그런데 2014년 5월 28일 이러한 기존의 징벌적 손해배상에 더하여 이른바 법정손해배상제도가 추가로 신설되었다. 즉, 정보통신망법 제32조의2에 의하면 “이용자는 ① 정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우, ② 개인정보가 분실·도난·누출된 경우의 모두에 해당하는 경우에는 대통령령으로 정하는 기간 내에 정보통신서비스 제공자등에게 제32조에 따른 손해배상을 청구하는 대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다”고 규정한 것이다.

3. 클라우드 컴퓨팅에의 정보보호법의 적용 문제

앞서 살펴본 바와 같이 클라우드 컴퓨팅에 있어서 정보보호 이슈가 매우 중요한 것이라면 이상과 같은 정보보호법제가 클라우드 컴퓨팅에도 잘 적용될 수 있어야 할 것이다. 이때는 일반법인 「개인정보보호법」에 대한 특별법으로서 정보통신망법과 위치정보법이 있으므로 이 두 법이 클라우드 컴퓨팅에도 적용이 있는지 여부를 판단하면 될 것이다.

(1) 정보통신망법의 적용대상과 클라우드 컴퓨팅

앞서 정리한 바와 같이 정보통신망법의 적용대상은 정보통신서비스제공자이다. 이 법에서 정보통신서비스제공자란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. 클라우드 컴퓨팅에 있어서 인터넷을 통하여 가상의 공간에서 정보를 제공하거나 정보의 제공을 매개하는 자는 전기통신사업자일 수도 있고, 전기통신사업자의 전기통신역무를 이용하여 정보를 제공 또는 매개하

는 자일 수 있으므로 적용대상 면에서 클라우드 컴퓨팅에 정보통신망법을 적용하는 것은 큰 문제가 없어 보인다.

구체적으로는 다음과 같은 사업자군이 정보통신망법의 적용대상에 들어온다. 이러한 범주의 사업자가 클라우드를 제공하는 경우 정보보호 문제와 관련하여 정보통시망법의 적용대상이 되는 것이다.

- 전기통신사업법에 따른 전기통신사업자: 이에는 초고속인터넷사업자, 이동통신사업자 등 기간통신사업자(허가제), 국제전화서비스, 재판매사업자 등 별정통신사업자(등록제) 및 포털, 게임사이트, 온라인쇼핑몰사이트 등 부가통신사업자(신고제)가 포함된다.
- 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자: 이에는 웹호스팅업자, 커뮤니티 제공 사업자(미니홈피, 블로그 등), P2P사업자 등이 포함된다.
- 정보통신서비스 제공자로부터 개인정보를 제공받은 자:
- 방송법에 따른 방송사업자: 이에는 지상파, 종합유선방송, 위성방송, 방송채널사용, 공동체라디오방송, 중계유선방송, 음악유선방송, 전광판방송 및 전송망 등이 포함된다.

(2) 위치정보법의 적용대상과 클라우드 컴퓨팅

한편 위치정보법에서는 위치정보사업 및 위치기반서비스사업을 적용대상자로 하는바, 전자는 위치정보를 수집하여 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 것을 말하고, 후자는 위치정보를 이용한 서비스("위치기반서비스")를 제공하는 것을 사업으로 영위하는 것을 말하는 바, 클라우드에 제공되는 정보가 개인위치정보이거나 위치정보사업자 또는 위치기반서비스사업자가 클라우드 서비스를 제공하는 경우 개인위치정보의 제공 또는 매개를 하는 경우에는 해당 클라우드 서비스와 관련하여서는 위치정보법상의 정보보호 관련 규정이 적용되어야 할 것이다.

(3) 개인정보 및 개인위치정보 해당여부와 클라우드 컴퓨팅

그러나 정보보호법제의 적용가능성에 있어서 중요한 것은 처리되는 정

보가 개인정보 또는 개인위치정보에 해당하는지 여부이다. 개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다(정보통신망법 제2조 제6호). 「개인정보보호법」에서도 개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다(「개인정보보호법」 제2조 제1호).

한편 "개인위치정보"라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알수 있는 것을 포함한다)를 말하는데, 여기서 위치정보란 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 「전기통신사업법」 제2조제2호 및 제3호에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것을 말한다(위치정보법 제2조 제1호, 제2호).

이처럼 식별가능정보까지 포함하면 개인정보 또는 개인위치정보의 범위는 매우 넓혀지는 것인바, 익명의 정보처리가 정보보호법제상 허용될 수 있기 위해서는 따라서 재식별(Reidentifizierung)이 불가능한에서만 가능함을 알 수 있다.

(4) 국회 계류중인 클라우드법(안)의 경우

현재 국회에 제출되어 있는 정부제출 클라우드법(안)[14]이나 의원입법으로 제출된 클라우드법(안)[15]에서도 특별히 클라우드 컴퓨팅 사업자의 인허가제도를 별도로 상정하고 있지 아니하다. 따라서 클라우드를 제공하는 자이기만 하면 개인정보 또는 개인위치정보를 제공하거나 매개하는 한

14) 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(안): 정부제출, 2013. 10. 16.
15) 클라우드 컴퓨팅 산업 진흥법(안): 김도읍 의원 대표발의, 2013. 11. 27.

정보보호법제의 적용을 받게 되는 것이다.

정보보호의 문제에 대해서 위 법안들은 정부제출 클라우드법(안)에서만 법안 제21조 및 제27조에서 이용자 정보의 보호에 대하여 간략하게 규정하고 있을뿐, 의원발의 클라우드 컴퓨팅 산업 진흥법(안)에서는 정보보호에 관한 사항은 전혀 찾을 수 없다.

4. 평가 및 소결

이상 살펴 본 바에 의하면 클라우드 컴퓨팅은 정보보호와 관련하여 개인정보 또는 개인위치정보를 클라우드에 제공받거나 이를 매개하는 경우 충분히 정보보호법제의 적용대상이 될 수 있음을 알 수 있었다. 그러나 현행 클라우드 관련 정보보호법제는 기본적으로 국내에서의 클라우드 제공 및 이용에 관한 사항만을 적용대상으로 하고 있음을 알 수 있다. 그러나 클라우드 이용관계는 기본적으로 국경을 넘어 이루어지는 경향이 농후하기 때문에 그에 관한 법률관계에 대한 규율은 국내법에 의한 규율에만 국한할 수 없는 문제가 있다. 이는 비단 계약법에 관한 사항뿐 아니라 정보보호법제의 측면에서도 마찬가지이다. 오늘날 Naver, Daum, T-Cloud 등 국내 포털사업자 등이 운영하는 클라우드를 이용하는 사례도 늘어나고 있지만, Facebook, Google+, Dropbox & Co 등 이미 전세계적으로 지배적인 위치를 점하고 있는 미국계 클라우드 서비스의 이용자들이 기하급수적으로 늘어나고 있다. 그러나 이들 미국계 클라우드 제공자들의 서버에 있는 정보에 대해서는 우리 국민이 국내에서 사실상 전혀 정보보호를 누릴 수 없는 한계를 노정하고 있다. 국내 정보보호 관련 법제에서는 이러한 외국계 클라우드와 관련한 정보보호 관련 규정을 두고 있지 않기 때문이다.[16]

이러한 문제점은 최근 Microsoft가 새로이 출시한 클라우드 서비스인 Office 365와 관련하여 현실화된 바 있다. 즉, Microsoft 클라우드가 런던에서 공식 출범하던 날 한 언론인은 유럽 Office 365 이용자가 영국에 소

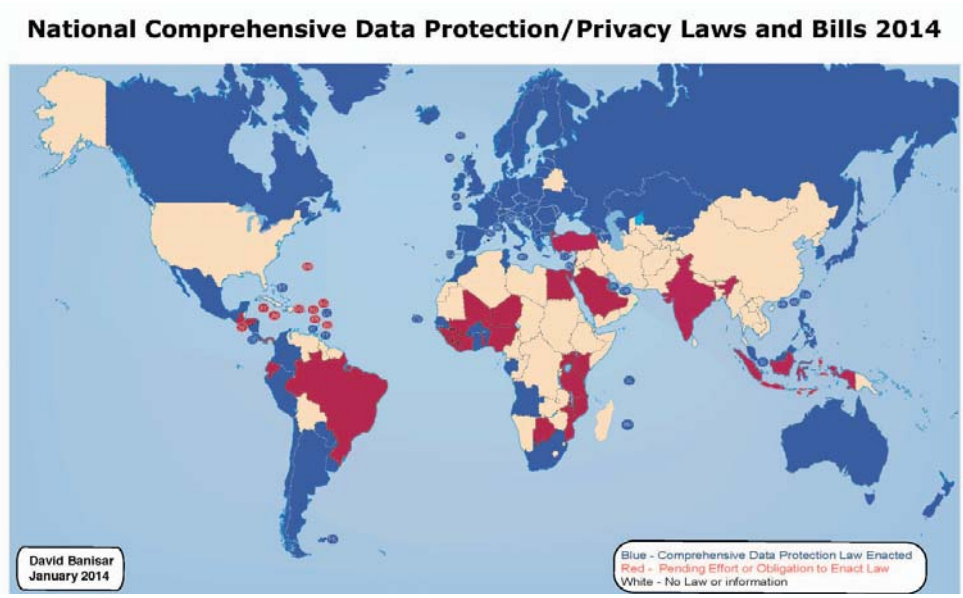
16) Jörg Oesterle, Cloud Computing: Datenschutz und transatlantische Misverständnisse, DAJV 2013, 170 f.

재하는 Microsoft 서버에 저장한 정보는 미국 행정당국(정보기관)의 접근으로부터 안전한가라는 결정적인 문제를 제기하였다. 이에 대하여 영국 Microsoft의 매니저인 Gordon Frazer는 공개적으로 놀라운 대답을 하였는바, “마이크로소프트는 그러한 보장을 할 수 없다”고 한 것이다.

이러한 상황은 비단 영국에서뿐 아니라 우리나라에서의 경우라도 동일한 문제가 제기되리라고 추단해본다. 그래서 이러한 문제를 조금이라도 개선하기 위해서는 비슷한 문제를 경험한 유럽연합에서의 경험을 참고하여 우리 제도에 반영할 수 있는 시사점을 찾아보는 노력이 필요하다고 본다.

Ⅲ. 국경을 넘는 클라우드 이용관계에 관한 법적용 문제

이하에서는 독일 및 유럽연합의 사례를 중심으로 국경을 넘는 클라우드 이용관계에 관한 법적용문제를 살펴보기로 한다. 이 문제는 아래 David Banisar가 2014년 1월 기준으로 정리한 그림[17]에서 보는 바와 같이 국가마다 정보보호수준이 다르다는 점을 전제로 한다. 그림에서 파란색으



17) http://ssrn.com/abstract=1951416.

로 표시된 국가들은 포괄적 정보보호법제가 유효하게 발효되고 있는 국가를 나타내며, 빨간색으로 표시된 국가들은 현재 정보보호법 제정을 위해 노력중인 국가를 나타내고, 흰색으로 표시된 국가들은 전혀 법제가 없거나 알 수 없는 국가를 표시한다.

클라우드 관련 정보보호에 관한 해외사례를 살펴봄에 있어서는 미국은 오히려 정보보호법제가 유럽연합이나 다른 나라보다 매우 미약하다. 그보다는 정보보호수준이 비교적 높고 정보보호법제가 체계화되어 있는 독일의 사례를 유럽연합을 중심으로 살펴보는 것이 정보보호 관련해서는 더 실천적인 결론을 얻어내기 수월할 것이다. 또한 정보보호수준이 높은 유럽연합이 클라우드 관련 지배적 위치에 있는 기업을 다수 가지고 있는 미국과의 국경을 넘는 클라우드 이용관계가 성립하는 것과 관련하여 정보보호 문제에 관심을 가지지 않을 수 없고, 따라서 Safe Harbor 협약을 체결하는 등 방안을 강구하고 있다. 이하에서는 이러한 일련의 상황을 검토함으로써 우리 법제를 위한 좋은 시사점을 도출해보기로 한다.

1. 독일의 정보보호법제

독일 연방헌법재판소는 1983년 12월 15일 있은 결정에서 정보보호를 ‘정보적 자기결정권(Recht auf informationelle Selbstbestimmung)’으로서 하나의 기본권으로 정의한 바 있다.[18]

독일에서는 인적 관련성(Personenbezug)을 갖는 정보, 즉 개인정보만이 연방정보보호법(Bundesdatenschutzgesetz, BDSG)의 적용을 받는다. 이에 따르면 개인정보란 “특정인 또는 특정가능한 인(人)의 인적 또는 물적 관계에 관한 개별적 언명(Einzelangabe)”을 말한다.[19] 그 밖의 다른 정보(예컨대 상품견본 등)에 대해서는 연방정보보호법은 적용되지 아니한다. 이러한 정보는 저작권법 등 다른 법과의 충돌을 야기하지 아니하는 한 타인의 시스템에서 저장되거나 처리될 수 있다. 클라우드 컴퓨팅에 있어서는, 개인 클라우드가 문제되지 않는 한, 대부분 타인의 시스템이 문제된다.

18) BVerfGE 65, 1 vom 15. 12. 1983.
19) 연방정보보호법 제3조 제1항.

정보가 타인의 시스템으로 이전되고 거기서 처리된다면 연방정보보호법 제11조에 따라 위탁(Auftrag)에 의하여 개인정보가 수집, 처리 또는 이용되는지 또는 이른바 기능이전(Funktionsübertragung)이 문제되는지 분명히 되어야 한다. 독일 정보보호법상 위탁정보처리와 기능이전이라는 두 가지 법개념은 서로 배척하는 관계이면서 또한 상이한 법효과를 가지고 있기도 하다.

이른바 '위탁정보처리(Auftragsdatenverarbeitung)'에 있어서는 정보보호법상 책임이 무제한적으로 위탁자에게 머물러 있게 된다. 이 경우 위탁자와 수탁자간에 문서에 의한 계약이 필수적으로 요구된다. 연방정보보호법 제11조 제2항은 위탁정보처리의 요건이 되는 10개 요소의 목록을 상세히 규정하고 있다. 즉, 위탁은 문서에 의하여 발해져야 하며 다음 각 호의 사항이 확정되어 있어야 한다.[20]

1. 위탁의 대상 및 기간
2. 예정된 정보 수집, 처리 또는 이용의 범위, 종류 및 목적, 정보의 종류 및 관련인의 범위
3. 법 제9조에 따른 기술적·조직적 조치
4. 정보의 정정, 삭제 및 저장
5. 제4항에 따른 수탁자의 의무, 특히 수탁자가 하여야 할 통제
6. 재위탁의 가능성
7. 위탁자의 통제권 및 관련한 수탁자의 수인의무와 협력의무
8. 수탁자나 그의 고용인에 의한 개인정보보호 관련 규정 또는 위탁에서 확정한 사항에 대한 위반의 고지
9. 위탁자의 수탁자에 대한 지시권한의 범위
10. 위탁종료에 따른 이전된 정보의 반환 및 수탁자에 저장된 정보의 삭제

위탁계약은 위에 열거된 10가지 사항을 포함하고 있어야 한다. 클라우드 제공자(Cloud-Anbieter)는 수탁자로서 클라우드 이용자(Cloud-Nutzer)의 지시에 따라야 하며 따라서 정보의 처리 및 이용과 관련하여 결정권이 없다. 반면에 위탁자는 정보처리의 시작 전 및 정기적으로 수탁자가 취

20) Johanna Schmidt-Bens, Cloud Computing Technologien und Datenschutz, 2012, S. 27 f.

한 기술적 및 조직적 조치의 준수를 확인하고 그 결과를 문서로 작성하여야 한다. 이처럼 이용권의 이전이 없기 때문에 결정권한은 전적으로 위탁자에게 있는 것이 위탁정보처리의 특징이다.

반면에 기능이전(Funktionsübertragung)에 있어서는 제3자에의 정보이전(Datenübermittlung)이 일어난다. 여기서 제3자란 책임 있는 주체 외의 모든 자연인 및 법인을 말한다[21] 정보에 대한 결정권 및 책임성 또한 위탁정보처리와 다른 중요한 구별기준이다.

이처럼 독일에서는 정보보호 관련 위탁정보처리와 기능이전을 구별하고 있기 때문에 클라우드 컴퓨팅 시스템을 양자 중 어디에 해당하는지 구별하기 위해서는 개별사안별 검토가 필수적이다. 그러나 일반적으로 하드웨어 및 소프트웨어의 서비스 기능을 갖춘 클라우드 컴퓨팅은 대부분의 사례에서 위탁정보처리의 영역에 속하는 것으로 보아도 무방할 것이다.[22]

2. EU 정보보호지침

유럽의 역사에 있어서 정보보호에 관한 최소한의 표준을 정립하기 위한 노력은 수차례 있었다. 1981년 그 첫 번째 시도로 유럽회의(Europarat)는 회원국들로 하여금 유럽정보보호협약(EuDSK)에 서명할 것을 요청하였다. 이 협약은 협약규정을 국내법에 반영하여야 할 의무를 포함하고 있었다(협약 제4조 제1항). 그러나 이 협약의 보호수준은 협약 제12조 제2항에서 보호수준을 가장 보호수준이 낮은 회원국에 맞추도록 하고 있었기 때문에 비교적 낮았다. 따라서 정보교환과 관련한 문제가 아직 완벽하게 해결될 수 없었고 이에 따라 유럽의회는 1982년 유럽집행위원회에 대하여 구속력 있는 정보보호지침을 제정할 것을 요구하였고, 그 첫 번째 초안이 1990년에 나왔다. 그런데 회원국들은 이 초안에 대하여 너무 높은 정보보호수준을 요구한다는 점에서 반발하였다. 그리하여 1992년에 두 번째 초안이 제출되었는바 이 초안은 1995년 10월 24일에 가서야 유럽연합 이사회를 통과하였다. 유럽연합 정보보호지침(95/46/EG)은 최초로 유럽연

21) 연방정보보호법 제3조 제8항.

22) Steffen Bothe, Datenschutz und Datensicherheit im Cloud Computing, 2012, S. 21 f.

합에 있어서의 정보보호에 관한 최소표준을 정립하였다. 회원국들에는 본 지침을 해당국가에 반영할 수 있도록 3년의 기간이 부여되었다(지침 제32조 제1항). 이렇게 해서 그때까지 상이했던 각 회원국들의 정보보호 법률을 높은 수준으로 맞출 수 있었다.

지침은 사적 및 공적 영역에서의 개인정보호의 처리를 규율한다. 지침 제2조에 따르면 지침은 개인정보의 자동화된 그리고 구조화된 수기의 수집에 대하여 적용된다. 따라서 챠트 형식의 카드는 포함되지만, 구조화되지 않은 서류는 포함되지 않는다. 지침 제7조(정보 처리의 허용성에 관한 원칙)에서는 요건들을 규정하고 있는데, 정보처리를 위해서 그 중 최소한 하나는 충족되어야 한다.[23]

- 처리에 대한 관련인의 동의(제7조 a),
- 관련인과 체결한 계약의 이행(제7조 b, c) 또는
- 책임 있는 자의 정당한 이익의 실현을 위한 처리, 단 관련인의 이익보다 초과하지 아니할 것.

지침은 1997년 ISDN지침(97/66/EG)[24]에 의하여 보완된 바 있지만, 통신 영역에서의 급격한 발전 때문에 이미 2002년에 재차 수정되지 않으면 안 되었다. 뒤이어 개인정보의 처리 및 전자적 커뮤니케이션에 있어서의 사적 영역의 보호에 관한 지침 2002/58/EG이 제정되었고 여기에 통신 영역에 특화한 정보보호 관련 규정이 포함되었다. 계속하여 2006년(2006/24/EG)과 2009년(2009/136/EG)를 통해 EU의 정보보호지침은 수정되어 오늘에 이르고 있다.[25]

3. 국경을 넘는 정보이전

EU 정보보호지침은 유럽연합 밖에서 정보를 수집, 처리 및 저장하는 것을 원칙적으로 금지한다. 독일식의 위탁정보처리는 클라우드 제공자의

23) Johanna Schmidt-Bens, Cloud Computing Technologien und Datenschutz, 2012, S. 42 f.
24) 개인정보의 처리에 있어서 자연인의 보호 및 자유로운 정보거래에 관한 지침.
25) Steffen Bothe, Datenschutz und Datensicherheit im Cloud Computing, 2012, S. 25 f.

거주지가 EU에 존재하고 또 당해 정보가 EU에서 처리되는 경우에 한하여 인정될 수 있다(연방정보보호법 제3조 제8항). 클라우드 제공자가 EU에 있는 전산센터를 이용하는 경우에도 그러한 바, 그의 회사 사무소가 어디에 위치해있는지는 상관 없다. 서버 또는 전산센터가 EU 밖에 있다면 EU의 정보보호표준은 적용되지 않는다. 그러나 해당 국가의 법에 따라 제공자에게 추가적인 의무, 예컨대 정보를 공적 기관에 재차 제출하도록 하는 의무가 부여되는 경우에는 가능하다. 이는 다음과 같은 사례가 해당할 것인바, EU 밖에 주된 사무소를 두고 있는 사업자가 클라우드 컴퓨팅 제공 사업지는 독일에 두고 있어 외국 정보보호법의 적용을 받는 경우이다. 개인정보를 EU로부터 EU밖으로 이전하는 것은 유보하에 허용된다(EU정보보호지침 제25조 및 제26조). 독일의 연방정보보호법에 따르면 정보의 이전은 특별한 정당성을 필요로 한다. 그에 따라 정보의 수취인은 적절한 정보보호 수준을 담보하여야 한다(연방정보보호법 제4b조 제2항, 제3항). 유럽집행위원회는 아르헨티나, 캐나다, 스위스 등 몇 개 국가들에 대하여 그와 같은 적절한 정보보호수준을 갖춘 것으로 인정하였다. 이러한 국가들에 대해서는 따라서 개인정보의 이전에 대하여 EU 회원국과 동일한 규정이 적용된다. 안전하지 않은 제3국의 서비스제공자는 정보보호법상 제3자로 간주된다(연방정보보호법 제3조 제8항 3문). 제3자에게의 정보이전은 그에 상응한 동의가 존재하는 한에서만 허용된다. 그러나 일반적으로는 관련인의 동의가 제대로 갖추어지지 못하고 있다고 한다.[26]

4. Safe Harbor 협정

미국은 일반적으로 독일이나 EU에서의 정보보호법제와 비견할만한 법률이나 규정을 갖추고 있지 못하다. 따라서 적절한 정보보호수준을 갖추고 있는 것으로 인정되는 나라의 명단에도 들지 못하고 있다. 그러나 미국은 가장 중요한 교역상대국 중의 하나이고, 개인정보가 미국으로 이전되는 것이 사실상 불가피한 면이 많고, 경제협력을 위해서는 정보의 이전

26) Johanna Schmidt-Bens, Cloud Computing Technologien und Datenschutz, 2012, S. 42 f.

이 오히려 장려되어야 할 측면도 있다. 이러한 이유에서 미국과 EU 사이에는 Safe Harbor 협정이 체결되어 있는바, 미국으로 이전되는 정보 관련 충분한 보호를 제공하기 위한 것이다. 이에 따라 미국기업은 독립연방행정청인 연방무역위원회(FTC)가 정한 7가지 Safe Harbor 원칙을 준수할 것을 스스로 의무지우는 경우 협약의 적용을 받을 수 있다.[27)]

1. 고지
   기업은 관련인에게 정보 수집·처리의 종류와 목적, 수취인, 제한과 이용 및 전송과 관련한 선택가능성 등을 고지하여야 한다.
2. 선택
   관련인은 자신의 정보가 제3자에게 재차 넘겨지는 경우 및 다른 목적을 위하여 사용되는 것에 대하여 이의를 제기할 가능성을 가져야 한다.
3. 제3자전송
   사업자가 정보를 제3자에게 재차 전송하는 것은 상기 제1 및 제2 원칙이 전제되는 경우에 한하여 허용된다.
4. 접속
   관련인은 자신에 대하여 저장된 정보를 열람하고, 경우에 따라서는 정정, 보충 또는 삭제할 수 있는 가능성을 가져야 한다. 그러나 그에 대한 비용이 비합리적으로 큰 경우에는 이에 대한 예외를 인정할 수 있다.
5. 보안
   기업은 정보의 일실, 변경, 파괴 및 남용으로부터 보호하기 위한 적절한 기술적 및 조직적 조치를 취해야 한다.
6. 정보통합성
   수집된 정보는 정확하며 완전하고 목적에 부합함이 담보되어야 한다.
7. 통제
   기업은 모든 Safe Harbor 원칙들의 충족을 담보할 수 있는 예방적 조치를 강구하여야 한다.

그밖에 이러한 7가지 원칙에 대하여 이를 보완하고 구체화하기 위한 미국 상무부의 15개 자주 묻는 질문(FAQ)이 있다. 기업에게는 Safe Harbor 협약에 참여할 2가지 가능성이 있다. 즉, Safe Harbor에 부합한 자

27) Steffen Bothe, Datenschutz und Datensicherheit im Cloud Computing, 2012, S. 27 f.

체 정보보호선언을 제출하거나 또는 자율규제적 정보보호프로그램에 가입할 수 있다. 이를 통해 인증받은 기업의 명단은 온라인으로 공시되어 있다.[28] 금융기관, 통신사업자, 항공사, 정육업자 등은 인증받을 수 없다.

클라우드 제공자가 유효한 Safe Harbor 인증을 받더라도 연방정보보호법 제11조 제2항에 따라 서면에 의한 합의를 해야 할 클라우드 이용자의 의무를 면제하는 것은 아니다.

Safe Harbor 협약은 현행 유럽법을 충족하도록 청구권을 고양시키는 역할을 하며 2000년 7월 26일 이래 유럽연합에 승인되어 있음에도 불구하고 인증에 대한 전면적이고 포괄적인 통제는 아직 없는 형편이다. 호주의 정보보호 전문가 Connolly는 이러한 Safe Harbor 협약을 연구하였는바, 그 결과 이러한 형태의 Safe Harbor 협약은 아무런 효용이 없다는 결론에 도달하였다. 왜냐하면 인증 받은 기업 중 많은 수가 Safe Harbor 원칙(특히 제7원칙)을 제대로 준수하지 않았거나 인증이 이미 유효기간이 지나서 효력을 상실했던 경우가 많았기 때문이다. 또한 어떤 경우는 심지어 미국 상무부에서 작성한 기업명단에 들어 있는 기업이 전혀 인증을 받지 않은 사례도 발견되었다고 한다. 제재조치가 행해지는 것은 극히 드물다고 한다. 2010년 4월 독일 비공공부분에서의 정보보호 규제기관 연합체의 뒤셀도르프 지부에서는 Safe Harbor 협약은 전혀 신뢰성을 제공해주지 못한다고 따갑게 지적하기도 하였다. 따라서 유럽 정보보호수준과 충돌하지 않기 위해서는 이용자는 기존의 계약상대방의 Safe Harbor 인증에도 불구하고 정보전문가를 위한 최소기준(특히 인증의 유효성 및 고지의무의 준수)을 심사하여야 한다. 독일 슐레시비히-홀슈타인 주 정보보호센터 소장인 Weichert는 Safe Harbor 도입 10주년에 즈음하여 “정보보호 시각에서 지금까지의 경험에 비추어 도출할 수 있는 유일한 결론은 Safe Harbor 협약을 즉시 폐기하여야 한다는 점이다”라고 비판적 입장을 피력하였다. 유럽 수준의 충분한 정보보호는 Safe Harbor 협약만에 의해서는 전혀 보장될 수 없다는 것이다.[29]

28) http://safeharbor.export.gov/list.aspx.

29) Steffen Bothe, Datenschutz und Datensicherheit im Cloud Computing, 2012, S. 28 f.

5. 정보의 국제적 이전과 정보보호법의 적용가능성

앞서 본 바와 같이 정보보호법은 처리될 정보가 개인정보일 때에만 적용된다. 익명의 정보처리는 재식별이 불가능한 한에서만 허용된다. 기술적 관점에서 클라우드 컴퓨팅에서는 독일 연방정보보호법 제11조에 따른 이른바 '위탁정보처리'가 문제된다. 그에 따라 클라우드 이용자는 (연방정보보호법 제3조 제7항, 유럽 정보보호지침 제2조 d에 따른 책임있는 주체로서) 정보처리의 방식과 종류에 대하여 책임이 있고, 따라서 클라우드 이용자는 정보의 통합성과 신뢰성을 보장하여야 한다. 나아가 클라우드 이용자는 위탁자로서 연방정보보호법 제11조가 정하는 계약 관련 전제조건을 충족하여야 한다. 클라우드 제공자는 수탁자로서 클라우드 이용자가 제시하는 바를 준수하여야 한다. 예외적인 경우에는 클라우드 제공자가 스스로 서비스급부를 제공하는 경우에는 클라우드 제공자도 책임있는 주체가 될 수 있다. 유럽연합 내에서 하는 정보처리는 기본적으로 허용되는 것으로 간주된다. 반면 유럽연합 밖의 클라우드는 일반적으로 허용되지 않는다. 다만 이에 대한 예외는 정보보호수준의 적절성이 확정된 경우에만 가능하다.

정보보호는 정보처리가 일어나는 장소에 연계하여야 한다. 만약 어느 주체가 독일에 거주지를 가지고 있으면 속지주의 원칙이 적용되어 이에 대하여는 독일 연방정보보호법이 적용된다. 유럽연합에서는 (유럽내) 국경을 넘는 정보거래에 있어서 거주지주의가 적용된다(지침 95/46/EG 제4조). 이는 정보수집 또는 정보처리에 책임 있는 주체가 그의 거주지를 갖는 나라의 법이 적용된다는 말이다. 즉, 사무소 소재지를 이탈리아에 갖는 회사에 대해서는 종전과 마찬가지로 이탈리아의 법이 적용되는 것이다.

정보보호법의 적용가능성이 문제되는 것은 정보처리가 이루어지는 장소가 (안전성이 희박한) 제3국일 때이다. 개인정보의 전송 및 처리는 당해 처리에 책임 있는 자가 사적영역과 기본권의 보호 및 그와 연관된 권리행사와 관련하여 충분한 보장을 제공할 수 있을 때이다(지침 95/46/EG 제26조 제2항). 이는 계약적으로는 예컨대 유럽연합 표준계약조항을 사용하거나 구속적 기업규칙인 BCR(Binding Corporate Rules)의 도움으로 실현

될 수 있을 것이다.[30]

적용법규의 불명확성은 법적 불안전성을 초래하고 이는 정보보호조치가 불충분하거나 전혀 행해지지 않는 상황도 초래할 수 있다. 이러한 이유에서 먼저 누가 개인정보의 처리에 대해 책임 있는 자인지 분명히 되어야 한다. 독일의 경우 이런 경우에는 제일 먼저 위탁정보처리의 기준들이 고려되어야 한다. 서비스가 전부 또는 일부 제3국에서 제공된다면 정보보호수준이 위탁자에 대해 적용되는 정보보호법이 요청하는 바에 상응하는지 명확히 되어야 한다.

이러한 독일법상의 해석들은 우리나라의 정보보호법제를 비교법적으로 검토할 때 국경을 넘어 정보가 거래되는 상황에서의 클라우드 이용관계에 있어서 법제도 마련의 필요성이 얼마나 큰 지를 잘 이해할 수 있다.

Ⅳ. 클라우드 산업발전을 위한 정보보호법제의 개선방향

이상의 검토내용을 바탕으로 이하에서는 현행 클라우드 관련 정보보호 법제의 발전을 위하여 필요한 개선사항을 몇 가지 필자가 보는 시각에 국한하여 제시해보고자 한다.

1. 과도한 정보수집의 제한 및 정보 개별화

2012년 이후 정보통신망법 등 정보보호를 규정하는 우리나라의 법제는 개인정보의 보호를 강화하는 방향 일변도로 발전해왔다. 수집·이용 목적의 이용자에의 고지, 주민등록번호의 원칙적 수집 금지, 개인정보 이용내역 통보 제도, 개인정보 누출 통보 및 신고제, 법정손해배상제도 등 면면이 모두 그러하다. 그러나 클라우드를 포함한 빅데이터와 IoT 등 새로운 유형의 ICT 산업의 발달을 위해서는 정보의 이용이 필수적이다. 그런데 현재 정보통신서비스 제공자 등이 수집하는 정보의 범위가 너무 넓다 보니 그 수집된 정보에 대하여 동일하게 엄격한 정보보호법을 적용하게 되

30) Johanna Schmidt-Bens, Cloud Computing Technologien und Datenschutz, 2012, S. 65 f.

면 정보의 이용 또는 활용 가능성은 막강한 정보보호법제의 벽에 가로막혀 현저히 떨어지기 마련이다. Twitter나 Facebook 같은 외국 사업자의 경우는 이름과 이메일주소, 생년월일 정도의 간단한 정보만 수집하여도 서비스제공이 가능하도록 하고 있기 때문에 정보보호 법제에 의하여 보호하여야 할 규제대상 정보의 범위가 매우 작고 따라서 산업의 입장에서 활용할 수 있는 정보의 범위는 상대적으로 우리나라의 경우보다 넓게 된다. 따라서 포털사업자 등 정보통신서비스 제공자가 수집하는 정보의 범위를 법으로 제한하거나 정보들을 개별화하여 부여되는 보호의 정도를 달리할 수 있다면 그 속에서 클라우드 등 산업이 활용하거나 이용할 수 있는 정보의 범위가 상대적으로 늘어남으로써 산업발전에 기여할 수 있으리라 생각된다.

2. 국경을 넘는 정보제공에 대한 법적 규율 도입

앞서 살펴본 바와 같이 클라우드 이용관계는 물리적 장벽이 없기 때문에 국경을 넘어 외국 사업자의 클라우드를 국내 이용자들이 사용하는 등 국경간 클라우드 이용관계가 성립되기 쉽고 그와 관련한 정보보호의 이슈도 제기될 수 있다. 특히 정보를 가지고 있는 클라우드 사업자가 국내 사업자이라면 국내 정보보호법제를 적용하여 규제할 수 있어 별다른 문제는 없다. 그러나 클라우드 사업자가 국외사업자이고 서버나 전산센터가 우리나라 국경내에 없다면 정보의 제3자 제공이나 목적외 사용 등을 규제하기 위하여 우리나라 정보보호법제를 역외에 적용하는 것이 사실상 불가능하여 정보보호의 사각지대가 나오기 쉽다. 가장 큰 문제는 우리나라와의 교역관계가 큰 미국과의 관계에서 정보보호수준이 (유럽연합과의 관계에서 보듯이) 상대적으로 우리나라보다 미국이 낮을 수 있고, 클라우스 서버나 전산센터가 우리나라가 아닌 미국에 위치해 있는 경우 우리 정보통신망법이나 위치정보법을 적용하여 해당 사업자로 하여금 기술적·조직적 조치나 시정조치 등을 명하는 것이 어렵다.

이에 대비하기 위해서는 해외 클라우드 사업자가 국내에 진출하려는 경우에 정보보호 대책을 마련하여 우리 규제기관에 제출하게 하고,[31] 서

버나 전산센터의 위치에 상관없이 우리나라 국민의 개인정보가 우리나라에서와 마찬가지의 개인정보보호수준을 누릴 수 있도록 양국간 보호수준이 높은 나라의 정보보호법제를 적용할 수 있는 근거를 마련하여야 할 것이다. 그러한 근거마련은 아마도 양국간의 양해각서 또는 협정체결을 통해 가능할 것이다. 앞서 살펴본 유럽연합의 사례에서는 미국과의 관계에서 Safe Harbor 협약을 체결하여 거기에 규정되어 있는 일정한 조치들을 이행하여 인증을 받도록 함으로써 정보보호수준을 끌어올리려는 시도를 하였다. 그러나 기본적으로 그러한 Safe Harbor 원칙들은 그 준수 여부가 사업자들의 자율에 맞겨져 있어서 사업자들의 자발적 준수가 없는 한 큰 위력을 발휘하기는 어려움을 알 수 있었다. 그렇다고 클라우드 사업자와 이용자간의 계약관계로 해결하도록 방치하는 것도 타당한 방법은 아니다. 정보보호 관련 국제협력의 차원에서 양국간에 정보보호 관련 협약을 체결하여 정보보호법제의 역외적용 문제, 정보보호수준의 균일화, 구체적인 제재조치의 절차와 방법 등을 정함으로써 속지주의의 한계를 넘어 정보보호의 실효성을 제대로 달성할 수 있는 장치를 적극적으로 마련하는 것이 필요하다.

3. 과도한 징벌제도의 완화

최근 카드사 정보유출사태 등 사고에 대한 경감심이 사회 전반에 퍼지고, 이에 따라 개인정보 유출사고를 막아야 한다는 공감대가 형성되는 것은 사실이다. 그러한 추세에 따라 기존에 있던 과징금 제도를 대폭 상향하고 손해배상과 관련해서도 법정손해배상제도가 추가로 생기는 등 해당 기업에 대한 징벌규정이 대폭 강화되었다. 그러나 징벌의 강화가 곧 필요로 하는 안전한 정보사회의 구현을 가져오는 것은 아니다. 오히려 과도하게 사업자들을 부담을 지움으로써 산업발전 발목을 잡는 것은 아닌지 우려될 여지가 있다. 따라서 징벌 일변도보다는 구체적이고 실체적인 제도면에서 수정 또는 보완을 함으로써 침해사고 등 정보 관련 위법이 줄어

31) Facebook이 독일에 진출할 때 이러한 조치를 독일정부가 공개적으로 요구한 사례가 있다.

들도록 하는 것이 바람직한 입법정책이 될 것이기 때문에 현재 강화되어 있는 규정들은 산업발전의 측면에서 향후 논의과정 중 또는 제도운영에 있어서 보완되거나 완화되는 것이 필요하다고 생각된다. 이는 과징금과 손해배상의 측면에서 각각 검토할 수 있다.

(1) 과징금 관련

개인정보 유출기업의 처벌강화 차원에서 정보통신망법 제64조의3이 개정되어 수탁자가 개인정보를 유출한 경우, 이용자의 개인정보를 분실, 도난, 누출, 변조 또는 훼손한 경우 법이 정한 일정한 조치를 하지 아니하는 경우 과징금을 기존 1억원 이내였던 것을 관련 매출액의 3% 이내에서 과징금을 부과할 수 있도록 대폭 강화되었다. 그런데 이 규정에 대한 보도자료에서 방송통신위원회는 개인정보 유출과 기술적·관리적 보호조치와 유출사고와의 인과관계를 입증하지 않더라도 관련 매출액의 3% 범위내에서 과징금을 부과할 수 있다고 해석함을 내비쳤다.

그러나 종래 정보통신망법상의 과징금은 기술적·관리적 보호조치와 개인정보 유출사고와의 인과관계가 있어야만 과징금을 부과할 수 있었던 점을 감안하면, 법리적으로 책임법적 원리를 포기하고 책임의 귀속을 무한정 확대할 수 있는 법해석을 해야 할 특별한 사정변화가 무엇인지 이해하기가 쉽지 않다. 과징금은 비록 형벌은 아니지만 행위에 대한 제재수단이라는 점에서 구성요건이 명확해야 하고 그에 해당하는지 여부를 판단함에 있어 행위결과를 행위자에게 객관적으로 귀속시키기 위해서는 원인행위와의 인과관계를 전제로 하는 것이 논리필연적이기 때문이다. 그리고 현재 법 제64조의3 제1항에는 어디에도 인과관계를 배제한다는 명문의 규정이 없음에도 불구하고 해석을 통해 인과관계 여부에 상관없이 과징금을 부과한다는 것은 법적 안정성을 해하고 사업자 등 관련인들에게 예측가능성과 수인가능성을 제한하여 법치국가원리에 부합하지 않는 결과를 가져올 가능성이 크다는 점에서 과징금 제도의 해석·운영상 인과관계에 근거하여 합리적으로 제한하여 현실화하는 것이 타당하다고 생각된다.

(2) 손해배상 관련

손해배상제도 관련해서는 민법상의 손해배상법리가 있음에도 불구하고 정보통신망법에서 손해배상에 대해서 별도의 규정을 둔 것은 사적자치와 계약내용을 통해 손해배상을 무력화하는 것을 방지하기 위한 것임을 앞서 살펴보았다. 그런데 이러한 기존의 손해배상규정에 더하여 이른바 '법정손해배상'제도가 추가로 신설되었다. 이는 기존의 정보통신망법 제32조에 의한 손해배상 대신에 정보통신서비스 제공자등이 고의 또는 과실로 규정을 위반한 경우 및 개인정보가 분실·도난·누출된 경우에 300만원 이하의 범위에서 손해배상을 청구할 수 있도록 하는 것이다(법 제32조의2). 이는 무과실 또는 무고의의 입증책임을 사실상 정보통신서비스 제공자에게 전환한 것으로 이 규정을 문언대로 해석하고 적용할 경우 유출사고 등 원인은 있지만 현실적으로 손해가 발생하지는 않은 경우에도 획일적으로 손해배상을 해야만 하는 상황이 배제되지 않을 것으로 보여 향후 제도운영과정에서 논란이 있을 것으로 생각된다. 종래 우리 대법원은 GS칼텍스 사건 등 몇몇 사례에서 정신적 손해 등을 인정할 만한 사유가 발견되지 않은 경우 손해배상을 인정하지 않은 사례가 있다.[32] 즉, 개인정보 누출 등 개인정보 법령위반에 있어서는 위법행위가 있더라도 손해 자체는 인정되지 않을 수 있는 경우가 존재하는데, 금번 도입된 법정손해배상제도하에서는 그러한 경우조차도 무조건 300만원 이하의 손해배상을 하여야 하는 상황이 존재할 수 있어 보인다. 그러나 법정손해배상제도는 위법행위로 인한 손해발생은 당연히 인정되나 손해액 입증이 어려울 경우 등에 제한하여 적용되는 것이 저작권법, 상표법 등 기존의 타법사례이며, 만약 법원이 정신적·재산적 손해가 발생할 가능성이 없거나 실제 손해가 발생하지 않은 경우에도 법정손해배상액 범위에서 손해배상을 인정한다면 정보통신서비스 제공자 입장에서는 예측가능성과 기대가능성을 배제하여 법적 안정성을 담보하지 못하는 환경을 직면하게 될 것이므로 관련 산업이 위축될 것은 불을 보듯 자명할 것이다. 따라서 법정손해배상제도에 있어서도 손해 발생 자체가 인정되기 어려운 경우에는 손해배상

32) 대법원 2012.12.26. 선고 2011다59834 판결.

책임을 묻지 않도록 제한하여 해석·운영하는 것이 반드시 필요하다고 생각되며, 향후 법개정 논의가 있을 때 입법적으로 보완하는 방안도 강구할 필요가 있다고 본다.

4. 자율규제 환경의 조성

보안침해사례에 대한 대응에 있어서는 보안과 해킹의 기술적 특성도 고려되는 것이 필요하다고 본다. 즉, 해커의 개인정보 침해 가능성을 사전적으로 100% 완벽히 차단한다는 것은 기술적으로도 사실상으로도 불가능하다. 정부의 규제의 칼로도 그러한 결과를 완벽하게 도출할 수도 없다. 그렇다면 규제일변도로 사업자들을 벼랑으로 몰기보다는 산업이 자율적으로 자정작용을 발휘하여 안전하고 깨끗한 정보사회가 이루어질 수 있도록 조장하고 이끄는 것이 필요할 것이다. 현재 정보통신망법에는 이미 자율규제의 씨앗은 뿌려져 있는 상태이고, 사업자들은 정부와 공동으로 개인정보보호를 위해 ISMS(Information Security Management System), PIMS(Personal Information Management System)와 같은 인증체계를 운영 중이며, 이에 대한 정부주관의 주기적인 점검도 시행되고 있어서 사업자들의 자율적 시정이 가능하고 또 바람직하기도 하다는 점에서 이러한 체제가 정상적으로 작동하도록 지속적으로 지원하고 유도하는 것이 필요하다고 본다.

Ⅴ. 요약 및 결어

이상 클라우드 컴퓨팅과 관련하여 특별히 정보보호 이슈를 정리하여 보았다. 현재 클라우드법(안)이 아직 국회에 계류중이지만 이들 법안은 주로 산업의 진흥을 중점으로 다루고 있고 정보보호 이슈에 대해서는 적극적으로 취급하고 있지 않다고 보여진다. 여전히 정보보호 관련해서는 개인정보보호법, 정보통신망법 및 위치정보법 등 기존의 정보보호법제를 클라우드 컴퓨팅에 여하히 적용할 수 있는지에 관심이 모아지게 될 것이다.

최근 카드사 정보유출사태를 기점으로 정보보호의 이슈가 강하게 드라

이브를 받게 되었고 그에 따라 보호 일변도의 논의가 급물살을 타게 되었고 그 때문에 산업의 측면은 물밑으로 수장된 듯한 분위기를 느낄 수 있다. 클라우드는 빅데이터 및 IoT와 더불어 정보에 밀접하게 기대어 발전할 수밖에 없는 신산업분야이다. 최근과 같은 보호 일변도의 상황에서는 이들 산업의 발전이란 사실상 기대할 수 없는 상황으로 나아갈 수밖에 없다. 우리의 정보보호법제가 비교적 정보보호수준이 높은 편이고 사전 동의 위주의 엄격한 제도로 체계화되어 있는 상황에서 사업자들에게 초기에 너무 많은 정보를 수집하게 방임하게 되면 활용 또는 이용의 범위가 너무 축소되게 되어 산업의 발전을 기약하기 어려운 상황이 될 수 있다. 따라서 수집되는 정보의 범위를 축소하도록 법제화하는 것이 현시점에서 필요한 처방이라고 본다. 아울러 기 수집된 정보 중에서도 어느 정도까지가 활용 또는 이용이 대상이 될 수 있는 것인지를 전향적으로 검토하는 작업도 필요한 시점이다. 최근 과징금과 손해배상제도가 대폭 강화되고 있으나, 제도의 운영에 있어서 가급적 비정상이 정상이 되도록 함으로써 법적 안정성을 꾀하고 산업의 안정적 발전을 지원하는 작은 움직임이 필요하다. 클라우드의 특성상 지역적 한계에 국한하여 논의할 경우 국경을 넘어 정보가 이전되는 현상을 정보보호법제로 정확히 규율되도록 하기 어려운 면이 있다. 우리 정보보호법제의 역외적용이 어려운 것이라면 해당 국가간 국제협력을 강화하고 관련 협약의 체결 등을 통해 양국간 같은 수준의 정보보호가 부여될 수 있는 환경을 조성하는 것도 필요하다.

이러한 작은 노력들이 결실을 이루면 우리의 정보산업도 유수의 다국적기업들 못지않게 발전할 수 있으리라 생각한다. 향후 학계나 실무계에서도 산업의 발전과 관련한 지속적인 논의와 관심을 기대해 본다.

참 고 문 헌

류지태/박종수, 행정법신론, 2011

정연덕, 클라우드 서비스와 개인 정보 보호의 문제점, 정보법학 제15권 제3호

홍성규, 인터넷을 통한 전자상거래 계약상의 법적 논점, 통상정보연구 제1권 제2호, 1999

이창범, 클라우드 컴퓨팅의 안전한 이용과 활성화를 위한 법적 과제, 정보보호학회지 제20권 제2호, 2010.4.

한국인터넷진흥원, 클라우드 서비스 정보보호 안내서, 2011

행정안전부, 뉴미디어 서비스 개인정보보호 가이드라인, 2012

Johanna Schmidt-Bens, Cloud Computing Technologien und Datenschutz, 2012

Aufsichtsstelle Datenschutz Basel-Landschaft, Merkblatt “Cloud Computing”, 2012.

Microsoft, Datenschutz in der Public Cloud: Microsoft Dynamics CRM Online, 2012

Steffen Bothe, Datenschutz und Datensicherheit im Cloud Computing, 2012

PWC, Cloud Computing, Navigation in der Wolke, 2012

Michael Winkelmann, Cloud Computing: Sicherheit und Datenschutz, Arbeitspapier für die Alcatel-Lucent Stiftung, 2010

Thilo Weichert, Cloud Computing und Datenschutz, DuD 2010, 679 f.

Nägele/Jacobs, Rechtsfragen des Cloud Computing, ZUM 2010, 281.

<국문초록>

클라우드 컴퓨팅은 최근의 ICT 생태계의 새로운 신산업으로서 IoT와 빅데이터와 더불어 중요한 핵심이슈로 떠오르고 있다. 클라우드와 관련해서는 많은 법적 이슈들이 있지만, 본 논문에서는 특별히 정보보호 이슈를 정리하여 보았다. 정보보호 관련해서는 개인정보보호법, 정보통신망법 및 위치정보법 등 기존의 정보보호법제를 중심으로 이를 클라우드 컴퓨팅에 여하히 적용할 수 있는지에 관심이 모아지게 될 것이다. 최근 카드사 정보유출사태를 기점으로 정보보호의 이슈가 강하게 드라이브를 받게 되었고 그에 따라 보호 일변도의 논의가 급물살을 타게 되었고 그 때문에 산업발전의 측면은 후순위로 밀린 듯한 분위기이다. 클라우드는 빅데이터 및 IoT와 더불어 정보에 밀접하게 기대어 발전할 수밖에 없는 신산업분야이다. 최근과 같은 보호 일변도의 상황에서는 이들 산업의 발전이란 사실상 기대할 수 없는 상황으로 나아갈 수밖에 없다. 우리의 정보보호법제가 비교적 보호수준이 높은 편이고 사전 동의 위주의 엄격한 제도로 체계화되어 있는 상황에서 사업자들에게 초기에 너무 많은 정보를 수집하게 방임하게 되면 활용 또는 이용의 범위가 너무 축소되게 되어 산업의 발전을 기약하기 어려운 상황이 될 수 있다. 따라서 수집되는 정보의 범위를 축소하도록 법제화하는 것이 현시점에서 필요한 처방이라고 본다. 최근 과징금과 손해배상제도가 대폭 강화되고 있으나, 제도의 운영에 있어서 가급적 비정상이 정상이 되도록 함으로써 법적 안정성을 꾀하고 산업의 안정적 발전을 지원하는 작은 움직임이 필요하다. 클라우드의 특성상 지역적 한계에 국한하여 논의할 경우 국경을 넘어 정보가 이전되는 현상을 정보보호법제로 정확히 규율되도록 하기 어려운 면이 있다. 우리 정보보호법제의 역외적용이 어려운 것이라면 해당 국가간 국제협력을 강화하고 관련 협약의 체결 등을 통해 양국간 같은 수준의 정보보호가 부여될 수 있는 환경을 조성하는 것도 필요하다.

주제어 : 클라우드 컴퓨팅, 정보보호, 보안, 인터넷, 정보통신

Cloud Computing and Protection of Personal Data

Park, Jong-Su*

This article aims at the issue of protection of personal data in area of cloud computing. Cloud computing means a new way of network computing where a program or application (or platform) runs on a connected server. Todays cloud computing grows rapidly into an industry worldwide. But the development of cloud computing industry needs enough supplies of informations. Informations, such as personal data lies under strict protection of law. In this situation data protection can be obstacle of development of cloud compution industry. Recent case of information spill in credit cards freezed the whole information industry. The resposibility of service carriers became heavier than ever before. The drafts of cloud act include not a single provision of information protections. The using of cloud services can happen cross-border. By this form of cloud using it lacks in many cases the relevent provisions, which rule the data protections. This article gives ideas of developments of current relevent legislations. It is very expected that in close future Korean cloud computing industry will much better develop than ever. This article's goal will be found hopefully there.

Key Words : Cloud Computing, Data Protection, Security, Internet, ICT

* Professor of Law, Korea University.