발간등록번호
11-1079930-000004-01

빅데이터 환경에서 개인정보보호 강화를 위한 법·제도적 대책 방안 연구

2012. 12. 23.

개인정보 보호위원회

개인정보보호위원회 연구용역 보고서

빅데이터 환경에서 개인정보보호 강화를 위한 법·제도적 대책 방안 연구

2012. 12. 23.

연구기관 : 가천대학교 산학협력단

책임연구원 : 최경진(가천대학교 교수)

연구원 : 정준현(단국대학교 교수)

구태언(테크앤로법률사무소 대표변호사)

지성우(성균관대학교 교수)

김도승(한국법제연구원 연구위원)

성준호(홍익대학교 강사)

제 출 문

개인정보보호위원장 귀하

이 보고서를 연구용역사업「빅데이터 환경에서 개인정보 보호 강화를 위한 법·제도적 대책 방안 연구」과제의 최종결과물로 제출합니다.

2012. 12. 23.

가천대학교 산학협력단
책임연구원 최 경 진

요 약

최근 SNS, 클라우드 등 빅데이터 환경에서 개인정보가 침해될 가능성이 증가하고 있으며, 과거와는 다르게 대규모적인 피해의 발생이 우려되고 있다. 그런데 현행 개인정보 관련 법제도가 대규모 데이터 집적을 효과적으로 규율할 수 있는지에 대하여 의문이 제기되었고, 개인정보가 대규모로 집적되어 유통되는 것에 그치지 않고 빅데이터가 국외에서 운용되거나 이전되는 문제가 발생한다. 또한 개인정보에 관한 국내 법제의 수준이 외국의 법제도와 상이함으로 인하여 빅데이터에 대한 효과적인 개인정보보호의 필요성이 증대되고 있다.

이러한 인식 하에 빅데이터에 대한 합리적인 법제도 규율 방향을 도출하기 위하여 연구를 진행하였다. 연구과정에서 국내외 현황 조사 및 분석, 해외 법제도 비교 분석, 국내 전문가 자문 청취 및 문헌조사 등의 방법론을 활용하였다

그 결과 개인정보 보호법의 개선방안으로서 개인정보 개념 정의의 개선, 프로파일링 거부권 선언 및 고지의무 신설, EU 국외이전 규범과의 정합성 강화, 국외이전 관련 자율규제 유도 방안 마련, 인증제 개선, 분리보관의무 명시, 개인정보 보유기간 제도 개선, 거버넌스의 체계적 일원화 방안이 도출되었다.

정보화 사회에서의 정보가치는 자료나 단편정보가 아니라 그것들을 모아 놓은 데이터베이스 안에 숨어 있는 정보가 더 큰 가치를 가진다. 수많은 자료와 단편정보들이 많으면 많을수록 융합분석 결과정보에 대한 확률적 신뢰성

이 커진다. 세계 각국은 빅 데이터의 활용성을 인지하여 육성 계획을 경쟁적으로 발표하고 있다. 우리나라도 빅 데이터에 대한 관심과 수요가 점차 늘어나고 있고 빅 데이터와 관련된 정보통신 기반 역시 세계에서 유래를 찾아볼 수 없을 정도로 갖춰져 있으나 관련 인력의 부족, 입법적·행정적 조치의 미비로 인하여 그 발전 속도가 매우 더디다. 또한 세계에서 유래를 찾아 볼 수 없는 강력한 개인정보 보호 법령으로 말미암아 빅 데이터를 활용하려는 정부나 기업은 위법의 위험을 감수해야 한다.

빅 데이터는 하나의 공공서비스이자 산업으로 거스를 수 없는 세계적 추세가 되었을 뿐 아니라 빠른 속도로 발전하고 있다. 기술의 발전화 현실적 필요성을 고려하지 않은 입법과 행정조치는 국가와 사회의 발전에 저해가 될 뿐이다. 어떤 제도나 기술이 항상 효용만 있을 수는 없다. 우리에게 남겨진 과제는 그것이 궁극적으로 국민의 권익 향상에 합하는 것인지 판단하고 어떻게 하면 효용을 높이고 부작용을 줄이는 것이냐를 고민하여 해결책을 찾는 것이다.

법과 기술의 괴리, 법과 현실의 괴리가 점점 커질수록 그로 인한 피해는 고스란히 국민의 몫이 된다. 따라서 환경변화에 대응하면서도 국민의 권익을 보호하고 개인정보처리자의 활동을 최대한 보장할 수 있는 균형 잡힌 법제도의 구축이 절실하다.

목 차

제1장 서 론 ····· 1
제1절 연구목적 및 범위 ····· 1
Ⅰ. 연구의 필요성 ····· 1
Ⅱ. 연구의 목표 ····· 1
제2절 연구범위 및 방법 ····· 1
Ⅰ. 연구의 범위 및 내용 ····· 1
Ⅱ. 연구의 방법 ····· 3

제2장 빅데이터의 현황과 개인정보보호의 필요성 ····· 4
Ⅰ. 빅데이터의 기초 ····· 4
Ⅱ. 빅데이터의 활용 ····· 14
Ⅲ. 국내외 정책동향 ····· 23
Ⅳ. 빅데이터의 문제점과 개인정보보호의 필요성 ····· 29

제3장 빅데이터와 관련한 해외 법제 동향 ····· 38
Ⅰ. UN ····· 38
Ⅱ. OECD ····· 40
Ⅲ. 미국 ····· 44
Ⅳ. EU ····· 49
Ⅴ. 일본 ····· 60
Ⅵ. ICDPPC ····· 60

제4장 빅데이터에 적합한 개인정보 보호법의 개선방안 ····· 62
Ⅰ. 빅데이터 환경의 개인정보보호를 위한 법제적 분석 ····· 62
Ⅱ. 현행 개인정보 보호 법제의 문제점 ····· 72
Ⅲ. 개인정보 보호법의 개선방안 ····· 93

제5장 결 론 ····· 103

참고문헌 ····· 104

제1장 서 론

제1절 연구목적 및 범위

Ⅰ. 연구의 필요성

○ 최근 SNS, 클라우드 등 빅데이터 환경에서 개인정보가 침해될 가능성이 증가하고 있으며, 과거와는 다르게 대규모적인 피해의 발생이 우려됨

○ 현행 개인정보 관련 법제도가 대규모 데이터 집적을 효과적으로 규율할 수 있는지에 대하여 의문이 제기됨

○ 개인정보가 대규모로 집적되어 유통되는 것에 그치지 않고 빅데이터가 국외에서 운용되거나 이전되는 문제가 발생함

○ 개인정보에 관한 국내 법제의 수준이 외국의 법제도와 상이함으로 인하여 빅데이터에 대한 효과적인 개인정보보호의 필요성 증대

Ⅱ. 연구의 목표

○ 빅데이터 분석을 통한 맞춤형광고, CRM 등을 위한 개인정보 처리 관련 개인정보 침해요소를 분석

○ 빅데이터 현황에 대한 인식을 바탕으로 하여 개인정보 보호법 등 현행법 상의 규율의 한계와 문제점을 분석

○ 타당한 정책방향 도출을 위한 해외동향 소개

○ 현황 및 현행법 분석, 외국법과의 비교 등을 바탕으로 개인정보보호 강화를 위한 대책 및 개인정보보호 제도 개선 방안 도출

제2절 연구범위 및 방법

Ⅰ. 연구의 범위 및 내용

○ SNS, 클라우드 등 빅데이터 환경의 개인정보 침해현황 및 요소 분석

- 최근 SNS, 클라우드 등 빅데이터 환경에서의 무차별적으로 유통(공개)되는 경우 개인정보 침해 현황 및 요소 등 문제점 분석

○ 국내·외 인터넷 사업자의 불법마케팅(광고), 목적외 이용 등 개인정보 관련 위반사례 분석을 통한 문제점 제기

- 빅데이타(Big Data) 시대에 행태정보의 프로파일링을 통하여 생성되는 개인정보를 마케팅, 광고 등에 이용하는 경우 목적외 이용, 사전동의 원칙, 관련 법령상 상충 문제 등
- 종전의 CRM, 맞춤형 광고기법 등을 발전시켜 각 고객군에 맞는 맞춤형 마케팅을 제공하는 과정에서, 이용자 동의 없이 취미・기호・자산・건강・거주지・연락처・구매이력 등 개인의 민감한 자료들이 광범위하게 수집되거나 자동 생성 되는 등의 문제점 분석

○ 글로벌업체 등 국내외 서비스에서 이루어지고 있는 불법적인 개인정보 수집·이용 관행, 법 규범 조사·분석을 통한 문제 제기

※ 개인정보 처리방침, 서비스 이용 약관 등

○ 행태정보를 이용한 맞춤형 광고(Online Behavioral Advertising)에서의 개인정보보호를 위한 자율규제 등 관련 규율체계 분석

- 미국 및 EU의 온라인 광고 마케팅 협회 자율 규약, FTC의 맞춤형 광고 기준, EU의 행태정보 기반 광고 가이드라인 등

○ 최근 미국, EU의 관련 정책 및 법제 동향 조사

- EU의 2012년 Data Protection Regulation 및 2009년 ePrivacy Directive상의 Privacy by design, Right to be forgotten, Do-not-track 등을 통한 연관 과제 발굴

○ 미국, 오바마 행정부의 소비자 프라이버시 권리장전(12.2, 백악관) 및 FTC의 소비자 프라이버시 보호 권고(12.3, FTC) 분석 등

- 개인정보보호 정책 및 제도 개선 방안 제시

○ 빅데이터, 클라우드 컴퓨팅 등의 프라이버시 침해 요인을 분석

- 특히 데이터 마이닝, 프로파일링, 개인정보 통합·연계 등 개인 정보 수집·이용 허용 범위와 한계를 분석하여,
  ※ 현행 개인정보 보호법상 동의원칙, 열람권, 동의철회권 등으로는 빅데이터 시대의 효과적 개인정보보호 장치로써 한계가 있음
- SNS 상에 공개범위, 공개 경로·방법 등의 개인정보 공개기준, 잊혀질 권리 등 개인정보 자기정보결정권 강화 방안 마련

○ 첨단 정보화 사회에서 개인정보보호 제고 방안을 제시하고, 현행 개인정보보호 법·제도의 개선방안 도출·제시
- 빅데이터 환경에서 개인정보 국외이전 문제, 제3자 제공 등 종전 개인정보 규율체계와의 정합성을 검토하고 관련법령 위반시 행정제재 실효성 방안 마련

Ⅱ. 연구의 방법

○ 국내·외 SNS, 클라우드컴퓨팅 등 빅데이터 환경에서의 개인정보 침해 사례 분석
○ 개인정보 수집·분석 등에 이용되는 침해현황 분석
○ 빅데이터 시대에 행태정보의 프로파일링을 통하여 생성되는 개인정보 관련 법령상 상충문제 분석
○ 행태정보를 이용한 맞춤형 광고에서의 개인정보보호를 위한 자율규제 등 규율체계 분석
○ 빅데이터 환경에서 개인정보 국외 이전 문제 등 관련법령 위반시 행정제재 방안 연구
○ 관련 전문가 등으로 연구진, 자문위원 등을 구성·운영

제2장 빅데이터의 현황과 개인정보보호의 필요성

Ⅰ. 빅데이터의 기초

1. 서설

스마트 단말기를 비롯한 각종의 디지털 장비의 증가에 따른 디지털 데이터양의 증가는 다양한 정보의 이동을 용이하게 하였다. 이때 사용되는 데이터의 양은 과거의 상상을 초과하는 정도에 이르게 되었으며,[1] 이러한 상황을 제타바이트(ZB: ZettaByte)(약 1조8000억 기가 바이트)[2] 시대라고 표현하고 있다. 세계적으로 생산되는 데이터의 양이 2007년부터 활용 가능한 저장용량을 초과하는 데이터 홍수가 시작되었으며, 이후 기하급수적으로 증가하고 있으며 2020년에 이르면 현재의 데이터양보다 약50배이상 증가할 것으로 예측하고 있다.[3] 이처럼 막대한 양의 데이터의 이동과 이를 통한 다양한 정보의 이동은 비즈니스, 과학, 그리고 정부에서부터 예술분야까지 다양한 분야에서 현실세계에서 발생할 수 있는 문제점의 발견, 분석 그리고 대안의

---

1) IDC의 조사결과에 따르면 2011년도 전 세계의 디지털 데이터양은 약 1.8 제타바이트, 약 2조 기가바이트(GB: GigaByte) 이르고 있으며, 정형・비정형데이터의 급격한 증가추세는 더욱 가속화 되어 2020년에는 디지털 데이터의 양이 35.2 제타바이트에 달할 것으로 전망했다(윤미림, “빅데이터 비즈니스 활용과 과제” 한국정보산업연합회 Issue Report, 2012, 10-13면).

2) 대용량 정보가 늘면서 정보를 세는 단위도 기가나 테라를 넘어 이제는 페타, 엑사, 제타까지 등장하고 있다. 제타바이트는 1021 를 의미하는 SI 접두어인 제타와 컴퓨터 데이터의 표시단위인 바이트가 합쳐진 자료량을 의미하는 단위이다. 이진 접두어를 사용한 제비바이트(ZiB) 와 구분된다.

※ 참고 (바이트 크기)

SI 접두어		전통적 용법		이진 접두어	
기호(이름)	값	기호	값	기호(이름)	V값
kB (킬로바이트)	$1000^1 = 10^3$	KB	$1024^1 = 2^{10}$	KiB (키비바이트)	2^{10}
MB (메가바이트)	$1000^2 = 10^6$	MB	$1024^2 = 2^{20}$	MiB (메비바이트)	2^{20}
GB (기가바이트)	$1000^3 = 10^9$	GB	$1024^3 = 2^{30}$	GiB (기비바이트)	2^{30}
TB (테라바이트)	$1000^4 = 10^{12}$	TB	$1024^4 = 2^{40}$	TiB (테비바이트)	2^{40}
PB (페타바이트)	$1000^5 = 10^{15}$	PB	$1024^5 = 2^{50}$	PiB (페비바이트)	2^{50}
EB (엑사바이트)	$1000^6 = 10^{18}$	EB	$1024^6 = 2^{60}$	EiB (엑스비바이트)	2^{60}
ZB (제타바이트)	$1000^7 = 10^{21}$	ZB	$1024^7 = 2^{70}$	ZiB (제비바이트)	2^{70}
YB (요타바이트)	$1000^8 = 10^{24}$	YB	$1024^8 = 2^{80}$	YiB (요비바이트)	2^{80}

이용수, “스마트혁명 시대 빅데이터 활용과 프라이버시 사이의 충돌에 관한 연구”, 경원대학교 소프트웨어대학원, 2011, 25면 각주 18)참조.

3) 안창원/황승구, 빅 데이터 기술과 주요 이슈, 정보과학회지, 제30권 제6호, 2011, 10면.

제시가 가능한 정도에 이르게 되었다. 이처럼 '빅데이터'(Big data)는 정치·사회·경제·문화·과학 기술 등 다양한 분야에서 사회와 인류에게 가치있는 정보를 제공함으로써, 그 중요성은 점점 더해가고 있다. 이는 지난 2012년 세계 경제 포럼이 선정한 떠오르는 10대 기술 중 그 첫 번째를 빅 데이터 기술에 선정[4]되었고, 대한민국 지식경제부 R&D 전략기획단이 선정한 IT 10대 핵심기술 가운데 하나로 선정[5]됨으로써 그 중요성에 대하여 다시 한번 확인하게 되었다.

하지만 '빅데이터'가 가지고 있는 대량의 정보의 유통과 저장이라고 하는 환경 속에서 발생할 수 있는 문제점으로서 개인정보의 보호라고 하는 중요한 화두를 떠올리지 않을 수 없다. 개인정보의 보호는 특히 디지털시대에 들어서면서 더욱 그 중요성이 강조되고 있으며, 빅데이터 시대로 접어드는 현재의 상황에서는 더욱 중요한 이슈로 되고 있다. 이하에서는 빅데이터의 의의, 현황과 빅데이터환경에서 개인정보보호 관련 문제점 등에 대하여 기술하기로 한다.

2. 빅데이터의 의의

종래 데이터의 개념은 단순한 정보의 저장이나 수집을 의미하였다. 하지만 오늘날에 들어와 데이터의 영역은 각종 디지털 디바이스들을 통해 저장 수집된 데이터 속에서 가치 있는 정보를 찾아내어 알기 쉽게 전달하고, 정보를 원하는 사람이나 기관에 판매하는 비즈니스 과정을 전부 포괄하고 있다. 특히 '빅데이터'란 기존 데이터베이스 관리도구의 데이터 수집・저장・관리・분석의 역량을 넘어서는 대량의 정형 또는 비정형 데이터세트[6] 및 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술[7]을 말한다. 이하에서

4) Global Agenda Council on Emerging Technologies, << The top 10 emerging technologies for 2012 >>, World Economic Forum, Feb 15th 2012.

5) "융합・스마트시대 IT산업 주도를 위한 잰걸음", <<지식경제부 보도자료>>, 2012년 4월 5일, 2면, 24면.

6) James et. al., Big data: The next frontier for innovation, competition and productivity, McKinsey & Company, 2011.http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation

7) John Gantz & David Reinsel, << Extracting Value from Chaos >>, IDC IVIEW June, 2011, p.6.[2] (http://idcdocserv.com/1142)

는 ‘빅데이터’의 개념과 그 특징에 대하여 살펴봄으로써 본 보고서에서 다루고자 하는 개인정보보호의 문제에 대한 논의의 시발점을 제공하고자 한다.

가. 빅데이터의 개념

앞서 언급한 것처럼 오늘날의 각종의 스마트기기들은 소셜네트워크, 사물인터넷 등을 통한 막대한 정보를 생산하고, 그 기기들로부터 생산되는 수많은 데이터들은 분산파일형태로 수집되어 중요한 정보로 가공된다. 그리고 수집한 데이터에서 현실의 문제점을 발견하고 해결책을 찾는 것이 가능하다. 이러한 현상을 과학자들과 컴퓨터 공학자들은 ‘빅데이터’라고 하는 새로운 용어를 통해 설명하고 있다.[8] 하지만 ‘빅데이터’에 대한 명확한 정의는 아직 내려지고 있지 않고 있으며, 다만 ‘빅데이터’가 가지고 있는 여러 특징을 들어 빅데이터를 설명하고 있다.

1) McKinsey는 빅 데이터는 단순히 데이터 용량에 따른 분류가 아니라 기존의 데이터베이스 처리방식으로 해결할 수 없는 데이터의 세트로 정의하고 이러한 데이터를 처리할 수 있는 기술이나 역량을 의미하는 것이며, 따라서 이러한 기술을 보유한 기업이나 국가가 미래에 경쟁력을 갖게 될 것이라고 했다.[9] 그럼에도 불구하고 데이터양의 증가는 필연적일 수밖에 없는데, 이러한 데이터양의 증가의 주요원인을 전세계 인구의 60%에 해당하는 40억명이 사용하는 모바일 폰에서 찾고 있다. 또한 이는 더욱 많은 스마트폰의 보급에 따라 더욱 가속화 될 것이며, 따라서 빅데이터가 제공하는 다양한 정보활용의 기회는 데이터가 증가하는 특정 영역의 사람들 뿐만 아니라, 스마트기기(대표적으로 스마트폰)을 사용하는 대부분의 국가에서 발견할 수 있을 것으로 보고 있다.[10]

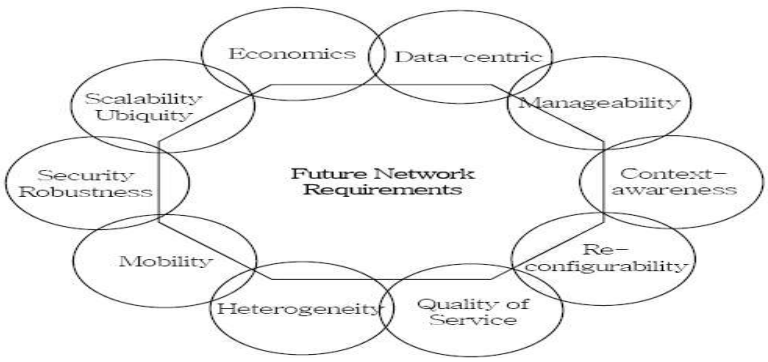
8) 강만모/박상무/김상락, 빅 데이터가 여는 미래의 세상, 한국정보과학회, 정보과학회지 제30권 제6호, 2012.6, 18면.

9) James et. al., Big data: The next frontier for innovation, competition and productivity, McKinsey & Company, 2011.http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation

10) James et. al., Ibid.

2) IDC는 빅 데이터를 기존의 데이터베이스 도구의 파일화, 저장, 관리 및 분석의 역량을 넘어서는 크기의 데이터 집합으로 정의하였다.[11]

3) 오늘날과 같은 고도 정보사회에 있어서는 아래의 <그림 1>에서 보는 바와 같이 다양한 기기의 융합을 통한 사람과 사람, 사람과 물건 또는 환경 및 물건과 물건 상호간의 소통을 통해 얻어지는 막대한 양의 개인을 비롯한 생활환경[12]등에 관한 정보가 생성되고 있다. 이와같은 환경하에서 현실공간에서 생활하는 개개인의 모습을 비롯한 모든 생활환경이 바로 트위터나 페이스북에 올라가고 사람들은 그러한 정보들을 어디서든지 볼 수 있다. 이처럼 모바일에서 생산하는 실시간 정보뿐만 아니라 인터넷에서 실시간으로 생성되는 정보의 양도 엄청나게 많다.



<그림 1> 미래인터넷의 특성(출처: 신명기, 2007, p.118)

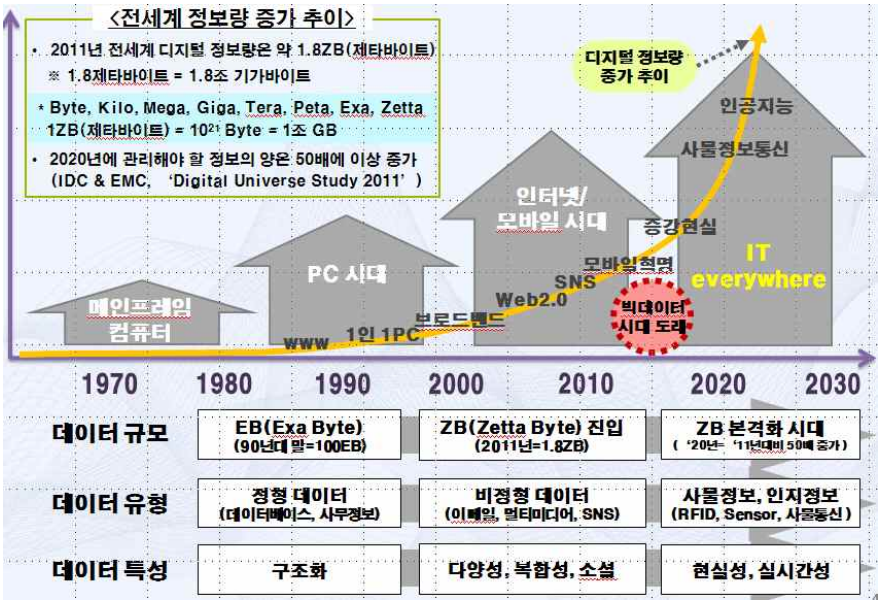
삼성경제연구소 보고서에 2010년 디지털 공간에 축적된 정보의 규모가 약 12억 TB에 육박한다고 한다고 하며, 월마트의 경우 시간당 100만 건 이상의 거래 기록이 저장되며, 트위터의 경우 2011년 매일 약 1억 1,000만 개의 트윗이 발생되는 등 아래의 <그림 2>에서 보는 바와 같이 2020년에 관리해야 할 정보의 양은 현대 보다 약 50배 이상 증가할 전망이라고 한다. 특히 다양한 기능을 가진 스마트폰의 출현과 확산으로 인해서 정보의 생성뿐만 아니라 확산 또한 상상이상 빨라지고 있음을 확인할 수 있다.[13]

---

11) Richard et. al., Big Data: What It Is and Why You Should Care, IDC, June 2011; 이명진/김우주, 빅데이터를 위한 고급분석 기법과 지원 기술, Entrue Journal of Information Technology, 제11권 제1호, 2012, 47면.

12) 생활환경의 의미에 대하여는 「환경정책기본법」 제3조제3호의 "대기, 물, 토양, 폐기물, 소음·진동, 악취, 일조(日照) 등 사람의 일상생활과 관계되는 환경"으로 이해하는 것이 법제간의 소통을 위해서도 바람직할 것으로 생각된다.

13) 예컨대, "강남 스타일"로 세계적인 관심을 끌고 있는 한국 가수 "싸이"의 경우 자신의 동영상을 공개한 2012년 9월29일부터 52일이 된 날에 조회수가 1억을 돌파하여 하루당 조회건수가 약 560명에 달하는 것으로 밝혀진 것이 그 예이다. http://news.mk.co.kr/ newsRead.php?year=2012&no=720014



<그림 2> 빅 데이터시대의 도래(출처 : 정지선, "신가치창출의 엔진 빅 데이터의 새로운 가능성과 대응전략, 2011.12.)

이와 같이 가상과 현실, 현실과 가상이 공존하는 가운데 이루어진 정보의 대홍수속에 기존의 분석 도구 및 관리체계로는 감당할 수 없는 엄청난 양의 데이터를 빅데이터[14]라고 하거나 "기존 데이터베이스 관리 도구의 데이터 수집·저장·관리·분석의 역량을 넘어서는 대량의 정형 또는 비정형 데이터 세트[15] 및 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술을 빅데이터라고 하는 바[16], 빅데이터의 일반적인 개념 요소는 정보의 집적, 정보의 결합, 정보의 분석이라 정의할 수 있다.[17] 이러한 빅 데이터시대에는 데이터의 활용가치를 높이기 위하여 필연적으로 다양한 프로그램 특히 클라우드 컴퓨팅에 의한 개인의 형태정보나 개인의 생활환경정보에 대한 처리를 통하여 다양한 수요를 충족시킬 새로운 지식의 창출이 따르게 될 것으로 보이며, 그 점에서 종전과 다른 양상의 개인정보보호의 이슈가 제기될 것이다.

나. 빅데이터의 분석기술

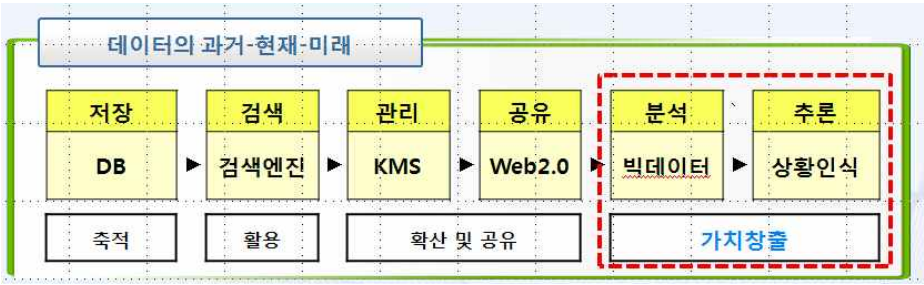
대부분의 빅 데이터 분석은 아래의 <그림 3>에서 보는 바와 같이 가치창출

14) http://yoingseon.tistory.com/57?top3

15) James Manyika & Michael Chui, "Big data: The next frontier for innovation, competition, and productivity", McKinsey Global Institute, (2011년 05월), p.1

16) John Gantz & David Reinsel, "Extracting Value from Chaos", IDC IVIEW June, (2011년), p.6

17) 김경환, "빅데이터 시대에 걸맞은 새로운 개인정보보호 프레임워크 필요", http://www.boannews.com/media /view.asp?idx=33450



<그림 3 > 데이터에 대한 패러다임의 변화

을 그 목적으로 하며 그 기술과 방법들은 기존 통계학과 전산학에서의 사용되던 데이터 마이닝, 기계 학습, 자연 언어 처리, 패턴 인식 등이 해당된다.[18] 특히 최근 소셜 미디어등 비정형 데이터의 증가로 인하여 분석기법들 중에서 비정형 또는 반정형 텍스트 데이터에서 자연 언어 처리 기술에 기반하여 유용한 정보를 추출·가공하는 것을 목적으로 하는 '텍스트 마이닝', 소셜미디어 등의 정형 또는 비정형 텍스트의 긍정, 부정, 중립의 선호도를 판별하는 '오피니언 마이닝(또는 평판분석)', 소셜 네트워크 연결구조 및 연결강도 등을 바탕으로 사용자의 명성 및 영향력을 측정하는 '소셜네트워크 분석' 및 비슷한 특성을 가진 개체를 합쳐가면서 최종적으로 유사 특성의 군을 발굴하는데 사용되는 '군집분석' 등이 주목을 받고 있다. 대규모의 정형 또는 비정형 데이터를 처리하는 데 있어 가장 기본적인 분석 인프라로 하둡[19]이 있으며, 데이터를 유연하고 더욱 빠르게 처리하기 위해 NoSQL 기술이 활용되기도 한다.[20]

다. 빅데이터의 특징

앞서 본 바와 같이 빅데이터는 여러 가지 측면에서 그 특징을 가지고 있다. 이러한 특징을 정리하여 Doug Laney와 IBM은 빅 데이터의 특징으로써 3Vs를 이용하여 빅 데이터를 정의하였다.[21] 3Vs란 데이터의 규모의 방대성(V

18) 정병권 외 2명, "미래사회와 빅 데이터(Big data) 기술", IT기획시리즈, 정보통신산업진흥원, (2012년), 20~ 21쪽.

19) 하둡(Apache Hadoop)이란 방대한 양의 데이터가 간결한 프로그래밍 모델을 이용하여 여러대의 컴퓨터로 이루어진 클러스터에서 분산・처리될 수 있도록 하는 하는 프레임웍을 의미한다. 즉, 하나의 컴퓨터에서 처리되던 작업을 수천대의 컴퓨터로 작업을 분산해서 처리할 수 있는 확장성을 제공하기 위해 설계된 것을 하둡이라고 한다. http://blog.naver.com/PostView.nhn?blogId=wnxodnr&logNo=10149708932

20) 조성우, "Big Data 시대의 기술", KT종합기술원, (2011년 10월 05일), 5~ 7쪽.

olume), 데이터 처리 및 분석의 속도(Velocity) 그리고 데이터 종류의 다양성(Variety)을 그 주요한특징으로 들고 있으며, 이를 통해 새로운 가치를 창출해 낼 수 있어야 한다.[22] 이하에는 빅데이터의 중요한 특징인 3Vs에 대하여 세부적으로 살펴보기로 한다.

(1) 데이터 규모의 방대성(Volume)

빅데이터의 특징으로 우선 양적인 측면에서의 특징을 가지고 있다. 용량(Volume)은 조직에서 수집하고 저장 및 관리와 분석해야 될 데이터가 수십 테라바이트를 넘어 수 페타바이트에 이를 만큼 그 양이 방대하다는 특징을 의미한다.[23][24] 이러한 용량은 단순 저장되는 물리적 데이터양의 증가만을 의미하는 것이 아니라, 이를 분석 및 처리하는 과정에서 발생하는 네트워크 데이터의 급속한 증가를 말하며, 이러한 것이 빅데이터의 가장 기본적인 특징이라고 할 수 있다.

(2) 데이터 처리 및 분석의 속도(Velocity)

빅데이터의 특징으로 속도(Velocity)를 들 수 있다. 빅데이터는 수집되고 처리되어야 할 데이터에 대한 입력과 출력이 빠르게 증가하고 실시간적인 처리를 요한다. 이러한 빠른 처리능력인 속도(Velocity)는 막대한 양의 데이터의 처리에 있어 필연적인 특징이라 할 것이다. 데이터 생산 및 유통, 수집 및 분석 속도의 증가와 이에 대한 실시간 처리 및, 장기간에 걸쳐 데이터를 수집·분석 하는 장기적 접근이 빅데이터의 속도적 특성이다.[25]

(3) 데이터 종류의 다양성(Variety)

---

21) Doug Laney, “3D Data Management: Controlling Data Volume”, Velocity, and Variety, Gartner, February 2001; Paul C. Zikopoulos, Chris Eaton, Dirk deRoos, Tom Deutsch, and George Lapis, “Understanding Big Data”, Paul Zikopoulos, 2012;

22) 안창원/황승구, 빅 데이터 기술과 주요 이슈, 정보과학회지, Vol.30 No.6, 2011, 10면.

23) Oracle, “Oracle: Big Data for the Enterprise”, Oracle White Paper, January 2012.

24) 이명진/김우주, 빅 데이터를 위한 고급분석 기법과 지원 기술, Entrue Journal of Information Technology, 제11권 제1호, 2012, 47면.

25) Oracle, Ibid.

빅데이터의 특징으로서 다양성(Variety)은 분석해야 될 데이터가 기존에는 정형적인 데이터만을 대상으로 했다면 빅 데이터에서는 정형적인 데이터뿐만 아니라 비정형적인 데이터까지 그 데이터의 형태가 다양화되어 가고 있음을 의미한다.[26] 가령 고정된 시스템에 저장되어 있지 않은 XML, HTML 등과 같은 반정형 데이터를 이용한 분석뿐 아니라 사진·오디오·비디오 형식의 소셜미디어 데이터나 로그파일(Database log) 같은 비정형 데이터도 처리할 수 있는 능력을 포함한다. 즉 빅 데이터의 성장이란 단순히 데이터의 양이 증가하는 것을 넘어서서, 다양한 형태의 데이터양이 증가하는 것을 의미하는 것이다.[27]

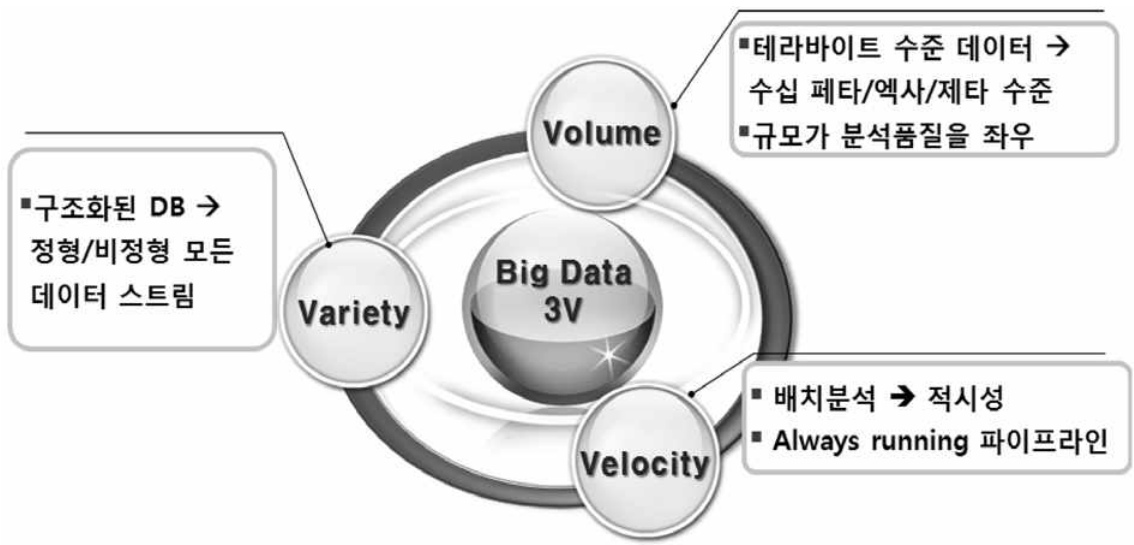


그림 4 빅데이터의 특성 : 안창원, 황승구, 빅 데이터 기술과 주요 이슈, 정보과학회지, Vol.30 No.6, 2012, 10면.

(4) 부가적 특징요소

빅데이터의 대표적 특징인 3Vs에 더하여 다른 특징적 요소를 꼽기도 한다. 가령 오라클(Oracle)은 빅 데이터에 대한 정의와 특징으로써 가치(Value)를 언급하고 있다.[28] 이는 빅 데이터에서 가치는 서로 다른 데이터에 대한 경

26) Oracle, Ibid.

27) 안창원/황승구, 빅 데이터 기술과 주요 이슈, 정보과학회지, Vol.30 No.6, 2012, 10면.

제적 가치가 다르기 때문에 빅 데이터안에 내재된 가치 있는 정보를 파악해야 한다는 것이다. 또한 가트너(Gartner)는 일반적으로 빅 데이터에서의 문제가 3Vs 중에 2개 이상이 결합되어 발생한다는 복잡성(Complexity)을 추가하여 빅 데이터를 정의하고 있으며,[29] 포레스터(Forrester)는 빅 데이터 환경에서는 그 데이터의 형태가 점차 증가하고 있음을 의미하는 변동성(Variability)을 그 특징으로 들고 있다.[30]

3. 빅데이터 시장 현황

International Data Corporation(IDC)은 국제 빅 데이터 기술과 서비스 시장이 2010년 32억 달러에서 2015년 169억 달러의 규모에 달할 것으로 전망했다.[31] IDC는 동 보고서에서 향후 5년간 연평균 성장률(CAGR, Compound Annual Growth Rate)이 40%에 육박할 것으로 예상했다. 그러나 IDC는 이와 같은 빅 데이터에 대한 늘어나는 요구에도 불구하고 대부분의 기업들은 데이터 분석에 대한 전문인력을 확보하지 못해 빅 데이터를 제대로 활용하지 못하는 상태로서, 훈련된 빅 데이터 기술 전문가와 분석가가 부족한 상태가 빅 데이터 시장의 발전에 저해가 될 수 있다고 예상하였다.[32]

출처 : Jefferies, 2012[33]

또한 빅 데이터 열풍은 관련 시장의 규모만 확장시킨 것이 아니라 IT 업계의 지각 변동을 불러일으키고 있다. 빅 데이터 선도기업들은 각 영역의 데이터를 축적하고, 솔루션을 장악함으로서 주도권을 더욱 더 공고화하고 있는

---

28) Oracle, Ibid.

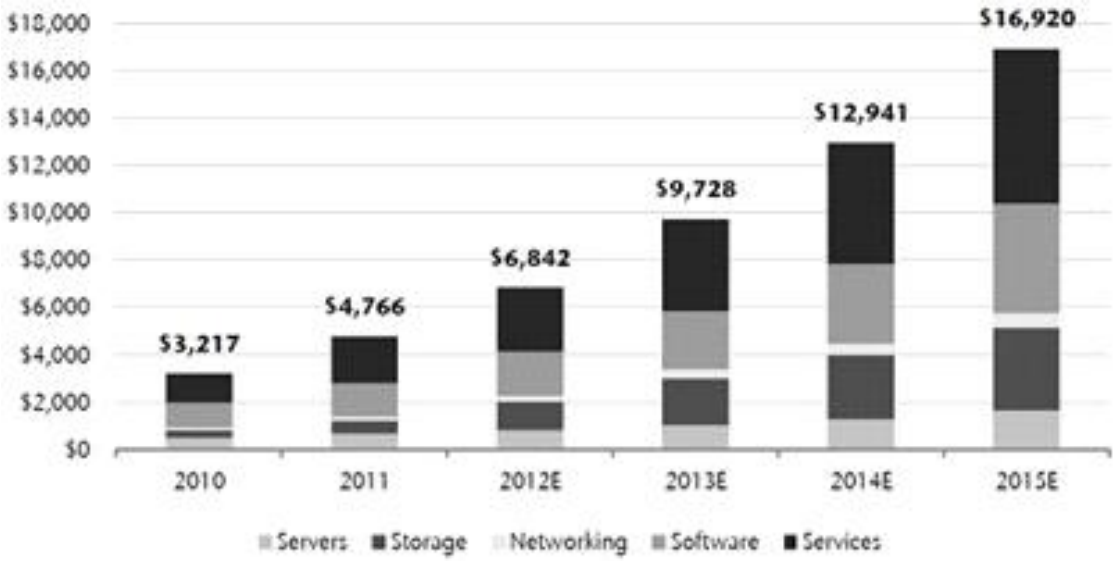
29) Mark A. Beyer, Anne Lapkin, Nicholas Gall, Donald Feinberg, and Valentin T, April 2011. “Sribar, 'Big Data' Is Only the Beginning of Extreme Information Man-agement”, Gartner

30) James G. Kobielus, Connie Moore, Brian Hopkins, and Shannon Coyne, “Enterprise Hadoop: The Emerging Core Of Big Data”, Forrester, October 2011; 이명진,김우주, 빅 데이터를 위한 고급분석 기법과 지원 기술, Entrue Journal of Information Technology, 제11권 제1호, 2012, 47면.

31) http://www.idc.com/getdoc.jsp?containerId=prUS23355112(최종방문일: 2012. 10. 30.)

32) 한국인터넷진흥원, 「민간 기업의 빅데이터 도입 증가 추세 - 관련 전문가 부족이 빅테이터 활용의 최대 장벽」, 주간 인터넷 동향, 2012. 9. 3주.

33) Jefferies, "Business Intelligence to Intelligent Businesses: Big Data in the Enterprise", 2012. 4.3 [한국정보보호진흥원, 「기업의 빅데이터 도입 트렌드 확산세」, 주간인터넷동향(4월 4주)에서 재인용].



실정이다. 구글, 아마존, 페이스북, 애플 등 글로벌 빅 데이터 기업들은 핵심 서비스를 무료 또는 염가로 제공함으로서 고객들로부터 방대한 데이터를 수집·축적하고 있다.

출처 : 채승병, 안신현, 전상인, CEO Information 851호

빅 데이터 분석을 통해 얻은 양질의 정보를 일반 기업이 쉽게 활용할 수 있도록 제공하는 정보 플랫폼도 새로운 비즈니스 모델로 부각하고 있고, 단기간에 빅 데이터 역량을 확보하고 강화하기 위한 기업간 인수합병과 관련 기업들간의 합종연횡이 활발하다.

주요 글로벌 기업들도 빅데이터 시장의 중요성을 인식하고 있다. “우리는 절대로 데이터를 내다버리지 않는다”는 제프 베조스 아마존 CEO의 말처럼 글로벌 기업들 역시 데이터의 중요성을 인식하고 빅 데이터를 이용하여 고객들의 패턴을 읽고 그들의 욕구에 선제적으로 대응함으로써 자사의 이익을 극대화 하기 위하여 재빠르게 움직이고 있다. 빅 데이터 선도기업들의 행적을 간략히 살펴보면, 구글은 빅 데이터를 활용하여 검색창에 발열, 기침 등의 검색 빈도를 취합·분석하여 독감 유행수준을 파악하는 ‘구글 독감 트렌드 서비스’를 제공하고 있고, 이베이는 이용자의 구매 이력과 소셜미디어 활동 내역 등을 분석하여 지인에게 선물할 만한 대상을 추천하고 있으며, 아마존의 경우 고객의 검색어와 도서 구입 패턴 분석을 통해 이전에 특정 도서를 구입한 사람이 어떤 관련 도서를 구입했는지 추천해주는 서비스를 제공하고 있는데 아마존 고객의 30% 정도가 추천 알고리즘을 통해 물품을 구입하는 것으로 알려지고 있다. 미국의 의료보험사인 웰포인트는 IBM의 왓슨 솔루션을 도입하여 환자의 증상과 면담 결과 등을 분석해 3초 안에 진단 또는 치료 가이드라인을 제시하고 있다.
국내 기업들도 빅 데이터를 활용하고 있다. 대표적으로 SK텔레콤은 네비게이션 서비스 티맵(T-map)과 관련하여 콜택시와 유류운반차량 및 고속버스 등에 설치된 GPS 장치를 통해 전국 도로의 교통 정보를 5분 단위로 수집한 후 이용자들에게 제공하고 있고, SK 플래닛은 모바일 사용자들의 성별, 나이, 위치, 단말기, 사용액, 이통사 등의 기본정보를 조합하여 사용자 프로파일과 행동유형을 분류하여 광고를 제공하는 빅 데이터 기반 광고플랫폼을 개발하였다.

Ⅱ. 빅데이터의 활용

1. 현황

빅데이터는 데이터를 수집하거나 축적할 뿐 아니라, 수많은 데이터 속에서

목적에 부합하는 데이터를 찾아내고, 효과적인 분석과 분석 결과를 제공해야 한다. 이를 통해 빅데이터 속에서 다양한 패턴을 추출할 수도 있으며, 이는 빅데이터 활용주체에게 핵심자원으로 활용되어 혁신과 경쟁력 강화, 생산성 향상을 촉진시킬 것이다.[34] 그렇다면 이렇게 폭발적으로 증가하는 데이터를 과연 어떻게 활용할 수 있는지에 대해서 다양한 활용 사례를 통해 알아보기로 한다.[35]

가. 빅데이터 활용분야

빅데이터는 여러 측면에서 활용이 가능하며, 특히 이상 현상 감지, 가까운 미래 예측, 현 상황 분석 등에 사용될 수 있다.[36]

(1) 이상현상의 감지

업무에서 발생하는 다양한 이벤트기록을 통하여 '정상 상태' 또는 '비정상상태'의 패턴을 알 수 있으며 패턴에 기초하여 새로운 이벤트가 발생했을 경우, 이상 현상 여부를 판단할 수 있다. 그 예로서 신용카드 회사인 VISA사는 카드 부정이용방지를 위해 빅데이터 기술을 이용하고 있다. 시스템로그를 이용한 패턴 분석으로 내부 범죄 등의 부정행위를 알아낼 수 있다. 이상 현상은 부정, 범죄 분석뿐만 아니라 마케팅 분야에서도 제품과 서비스에 대한 고객 변심을 감지하여 고객 이탈 방지 대책을 수립하는데 활용할 수 있다. 또한 의료/간호 분야에서도 의료인들이 감지하기 어려운 이상 현상을 신속하게 감지하는데 활용되고 있다. 캐나다 온타리오 공과대학은 집중치료실(ICU)에 있는 약 100명의 환우 아동을 대상으로 심전도, 심박수, 혈압 등 16개의 종류의 검사 결과 수치를 수집·분석한 패턴을 도출하여 신생아 이상 징후의

34) 채승병/안신현/전상현, "빅데이터: 산업 지각변동의 진원", 삼성경제연구소 CEO Information, 제851호, 2012, 1-25면; What is a big data?, http://www-01.ibm.com/software/data/bigdata; Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

35) 이하에서 소개하는 빅데이터 활용분야에 내용은 강만모/박상무/김상락, 빅 데이터가 여는 미래의 세상, 한국정보과학회, 정보과학회지 제30권 제6호, 2012.6. 20-21면에 소개된 '빅데이터 활용 시나리오'내용을 정리하여 기술한 것이다.

36) 윤미림, "빅데이터 비즈니스 활용과 과제", 한국정보산업연합회 Issue Report, 2012, 10-13면.

감지에 활용하고 있다.

(2) 가까운 미래 예측

빅데이터를 고속으로 수집·분석하는 것으로 가까운 미래의 수 분 또는 수 시간 후를 예측하는 'Nowcast'가 가능해진다. 기업에서는 '이용자의 마음이 변했다'라는 사실을 인지하는 것보다 '이용자의 마음이 변할 것 같다'라는 정보와 이에 대한 사전대응을 통해 고객의 이탈을 방지하는 적극적인 마케팅을 가능하게 한다. 이러한 예측기능은 캘리포니아 산타크루즈 카운티에서는 8년간의 범죄기록을 분석하여 범죄자의 행동패턴 및 점포 영업시간과 같은 환경요인과 범죄발생과의 관계성 도출, 범죄가 일어날 것으로 예상되는 장소를 매일 예측하고 있다. 또한 미국 포드사는 개발 중인 커넥티드 자동차에 적용한 기술로, 네비게이션이 운전자의 주행이력과 패턴을 분석하여 운전자에게 앞으로 도착해야 할 목적지에 이르는 최단 또는 최적 경로와 연료 배분을 제안한다.

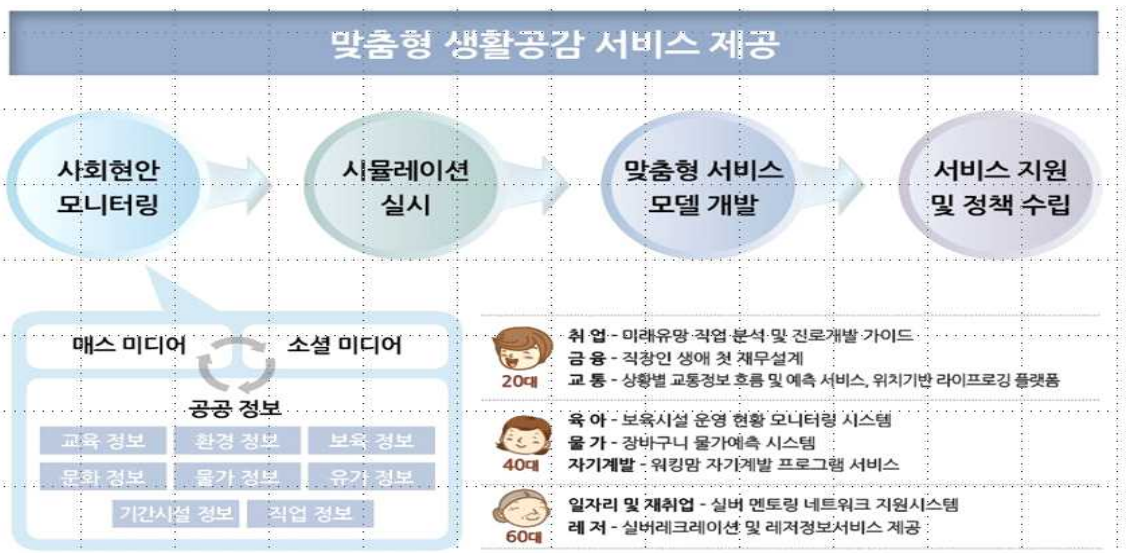
(3) 현 상황 분석

빅데이터를 이용하여 현재까지 면밀히 검토하지 못했던 것까지 분석함으로서 자사의 현 상황을 보다 명확하게 이해할 수 있게 한다. 가령 일본의 西鐵스토어(Nishitetsu Store)는 2012년 상반기 가동을 목표로 빅데이터를 이용한 회계 시스템을 구축하고 있다. 이를 통해 매월 그룹 단위의 상품 원가율을 입고액과 매출액에서 산출하는 회계시스템에서 매일 단일 상품의 원가율을 산출하는 체계로 변경하여 단일 상품별 원가율과 원가 변동 추이를 분석하여 이익률이 높은 상품에 대한 일자별 주력 마케팅 정책을 수립한다.

나. 빅데이터 활용 사례

빅데이터 기술의 발전은 앞에서 언급한 바와 같이 사람과 사람 및 사람을 둘러싼 생활환경에 관련된 정보가 상호소통하면서 실시간으로 다양한 데이

터가 생성·수집되고 있는 현대 정보융합사회에 있어서는 이들 데이터에 대한 앞서의 분석기술을 통해 동전의 양면처럼 사회의 순기능적인 지식의 창출뿐만 아니라 역기능적인 지식의 창출 또한 가능하게 된 오늘날 빅 데이터 기술은 아래의 <그림 5> 및 <표 3>에서 보는 바와 같이 정치·사회·경제·문화·과학기술 및 국민생활 일반 등 전 영역에 걸쳐 그 중요성이 부각되고 있다.



<그림 5 > 빅데이터로 진화하는 행복한 세상

빅데이터 활용사례는 특히 기업의 서비스영역에서 눈에 띄고 있다. 빅데이터를 이용하여 서비스를 향상하고, 고객의 이탈움직임을 감지하여 특별한 관리를 하거나, 환자의 사례를 분석하여 새로운 의료기술을 개발하기도 하였으며, 다양한 형태의 데이터를 분석하여 새로운 전술정보를 개발해 내기도 하였다. 이하에서는 실제 빅데이터의 활용사례를 소개하기로 한다.

<표 3 > 글로벌 빅 데이터 활용사례

출처:http://news.mk.co.kr/newsRead.php?year=2012&no=614916

산 업	기 업	특 징
유통	월마트	각 매장의 모바일과 소셜 쇼핑의 특징 이용한 웹마트랩 운영
	아마존닷컴	과거 고객이 구입한 서적 목록을 분석해 개인화된 구폰 발행
	자라	전세계 매장 판매·재고 데이터 분석으로 무재고 시스템 실현

서비스	T모바일	과거 탈퇴고객의 이용패턴 분석하여 이탈 가능성 높은 가입자 관리
	넷플릭스	고객에 대여한 영화목록 등을 분석하여 개인별 맞춤형 영화 콘텐츠 제공
	디사이드닷컴	전자제품 가격 흐름을 예측하여 고객에게 적절한 구매시기를 알려줌
	웰포인트	환자차트, 병원시술자료, 논문 등 모든 정보를 검색하여 적절한 치료법 제시
제조	볼보	모든 차량 내부에 센서부착하여 이동 중 발생하는 결함 발견
	히타치플렌트테크놀로지	크레인 곳곳에 센서부착하여 무게중심 이탈여부, 오작동 징후 파악
	마이크론테크놀로지	제품생산시간에 영향을 미치는 요소분석하여 비용절감 방안 마련

(1) 실시간 교통정보 서비스

SK텔레콤의 네비게이션 서비스인 티맵은 전국 도로의 교통 상황을 5분 단위로 수집, 분석해 정확한 도착 시간을 제공한다. 이러한 실시간 교통정보 서비스는 콜택시, 유류 운반차량, 그리고 고속버스 등에 위성위치확인시스템(GPS) 장치를 장착해서 전국 도로의 교통정보를 실시간으로 수집함으로써 가능하다. 기존의 네비게이션이 지도와 길 안내 프로그램을 기계에 내장하는 것과 달리 SK텔레콤 서버에 접속해 고성능 컴퓨터가 계산한 길 안내 결과를 수신하고 있다.[37]

(2) 경제 및 경영

아마존닷컴의 추천 상품 표시, 구글 및 페이스북 의 맞춤형 광고아마존닷컴은 모든 고객들의 구매 내역을 데이터베이스에 기록하고, 그 기록을 분석해 소비자의 소비 취향과 관심사를 파악한다.[38] 이런 빅 데이터의 활용을 통해 아마존은 고객별로 '추천 상품(레코멘데이션)'을 표시한다. 고객 한사람 한사람의 취미나 독서 경향을 찾아 그와 일치한다고 생각되는 상품을 메일, 홈페이지상에서 중점적으로 고객 한 사람 한 사람에게 자동적으로 제시하는

37) 채승병/안신현/전상현, 전게논문, 2012, 1-25면.

38) 장영재, 「아마존닷컴, 현대의 서점 아저씨」(2012년), 비즈니스북스, 119쪽.

것이다.[39] 아마존닷컴의 추천 상품 표시와 같은 방식으로 구글 및 페이스북도 이용자의 검색 조건, 나아가 사진과 동영상 같은 비정형 데이터 사용을 즉각 처리하여, 이용자에게 맞춤형 광고를 제공하는 등 빅 데이터의 활용을 증대시키고 있다.

그밖에, 서비스업체들은 과거 고객이 남긴 데이터를 토대로 이용자 성향을 파악하여 가입자 이탈을 방지하거나 판매고를 늘리는 기업전략의 자료로 활용되고 있다. 예컨대, 미국 통신사 T모바일(T-Mobile)은 2011년 1분기 T모바일에서 다른 통신사로 갈아탄 고객 수가 9만9000명에 달하여 가입자 유치만큼이나 유지가 중요한 만큼 이탈 방지 해결책이 필요하였으며, T모바일은 3000만명이 넘는 가입자와 관련하여 매일 170억건 이상 쏟아지는 통화의 송수신 내역을 분석해 고객의 통신사 전환위험을 감지하는 시스템을 개발하였다. 이를 통해 다른 통신사로 회선을 옮겼던 고객이 사전에 보인 특유의 이용 패턴을 발견하고, 탈퇴 징후를 보이는 고객에게 맞춤형 추가 혜택을 제공한 결과 2011년 2분기 T모바일에서 타 통신사로 빠져나간 고객 수를 절반가량 줄이는 성과를 거두었다.

(3) 위치기반 서비스

영국의 이동통신회사인 O2는 Placecast와 협력하여 위치 기반 서비스(LBS, Location-Based Services)를 이용하여 실시간으로 스타벅스 프로모션을 모바일로 서비스 가입자에게 제공한다. 가령 가입자가 스타벅스 매장 근처에 도달하면 문자메시지와 함께 프로모션 쿠폰이 가입자에게 전송된다. 이러한 위치기반 서비스는 스마트폰 확산에 SNS와 결합된 모바일 서비스가 증가하고 있으며, 이미 스마트폰 사용자 50% 이상이 위치 기반 서비스를 이용한 프로모션을 통해 물건을 구매한 경험을 가지고 있다고 한다.[40]

---

39) 미국에서 실제 있었던 일이다. 한 남자가 고등학생 딸이 출산용품 관련 광고 메일을 받자 매장에 찾아가 강력하게 항의했다. 매장 점장은 자신들의 실수로 판단하고, 고개 숙여 남자에게 사과했다. 그러나 얼마 후 딸이 임신 사실을 가족들에게 숨겨왔다는 사실이 밝혀졌다. 이 업체는 어떻게 부모도 몰랐던 딸의 임신 사실을 알고 광고 메일을 보냈을까. 월마트에 이어 미국 할인유통업계 강자로 떠오른 타깃(target)은 고객 구매 이력을 분석한 뒤 향후 구매품목을 예측하는 모형을 만들었다. 이를 통해 임산부가 보이는 특정 패턴도 찾아냈고, 임신부가 구매할 만한 품목을 대거 사들인 고등학생 딸에게 광고 메일을 보냈던 것이다. 위 사례는 빅데이터 분석의 위력을 여실히 보여준다. http://news.mk.co.kr/newsRead.php?year=2012&no=614916

(4) 데이터 분석 통한 효과적인 전술 정보제공

드루 콘웨어(뉴욕대학의 박사과정)는 위키리크스에 저장돼 있는 테라바이트급의 핵심 데이터를 분석해 미국과 아프가니스탄 연합군의 병력 활동 동향을 알아내었다. 데이터 분석을 위해 R통계언어를 사용하였고, 아프가니스탄 주요 5곳을 적, 중립, 동맹지역으로 나눠 정보를 분류하고, 각 지역에서 어떤 활동들이 주로 일어나고 있는지에 대한 패턴을 분석했다. 결과 정보를 통해 탈레반의 활동이 어느 지역에서 많이 일어나는지, 미국과 동맹 맺은 지역이 어딘지를 쉽게 파악할 수 있었으며, 시간 흐름에 따라서 아프가니스탄에서 전쟁 양상이 어떻게 진행되는지 확인할 수 있었다.[41)]

(5) 환자 사례 분석을 통한 새로운 수술 기법개발

게놈 연구를 수행하는 캘리포니아에 소재한 의료진단회사 카디오DX(Cardio DX)에서는 관상 동맥 질환을 식별할 수 있는 기술을 개발했다. 실제로 이 기술은 약 1억 이상의 유전자 샘플을 추출해서 사용하고, 23번의 테스트를 거쳐 예측 유전자를 확인해야 해야만 가능한 기술이다. 하지만 이러한 복잡한 과정을 빅데이터 기술을 사용하여 쉽게 해결하였다.[42)]

(6) 볼보의 빅데이터 활용

최근의 자동차는 전자기술이 집약되어 정교한 운전제어를 위한 많은 센서와 CPU가 내장되어 있다. 볼보는 소비자의 자동차 운행 과정에서 수집된 데이터를 본사의 분석 시스템에 자동 전송하도록 하여 빅데이터를 축적하고, 이를 활용해 제품개발 단계에서 알기 어려운 다양한 결함과 소비자의 잠재 요구를 파악하여 빠르게 대응하고 있다. 종래에는 50만 대의 차가 팔린 뒤에나 제기되었을 결함을 이제는 1,000대의 판매 시점에 포착하여 사후관리 비

40) 이성춘/임양수/안민지, “Big Data, 미래를 여는 비밀열쇠”, KT경제경영연구소 보고서, 2012.
41) 빅데이터 분석이 세상을 바꾼다, http://www.bloter.net/archives/68798
42) 강만모/박상무/김상락, 전게논문, 2012.6, 21면.

용이 크게 줄어들었다.[43]

(7) 정치 및 사회(2008년 미국 대통령 선거)

2008년 미국 대통령 선거에서 버락 오바마 미국 대통령 후보는 다양한 형태의 유권자 데이터베이스를 확보하여 이를 분석·활용한 '유권자 맞춤형 선거 전략'을 전개했다.[44] 당시 오바마 캠프는 인종·종교·나이·가구형태·소비수준과 같은 기본 인적 사항으로 유권자를 분류하는 것을 넘어서서, 과거 투표 여부·구독하는 잡지·마시는 음료 등 유권자 성향까지 전화나 개별 방문을 또는 소셜 미디어를 통해 유권자 정보를 수집하였다. 수집된 데이터는 오바마 캠프 본부로 전송되어, 유권자 데이터베이스를 온라인으로 통합관리하는 '보트빌더(VoteBuilder.com)'시스템의 도움으로 유권자 성향 분석, 미결정 유권자 선별, 유권자에 대한 예측을 해나갔다. 이를 바탕으로'유권자 지도'를 작성한 뒤, '유권자 맞춤형 선거 전략'을 전개하는 등 오바마 캠프는 비용 대비 효과적인 선거를 치를 수 있었다.

요컨대, "롱테일 정치"(longtail politics) 내지 "위키정치"(Wiki politics)라고 불리는 오바마의 IT선거전략은 다음의 3가지로 요약할 수 있다. 첫째, 웹사이트를 단순한 홍보용사이트가 아닌 유권자가 서로 의견을 나누고 교감할 수 있는 소셜네트워크 사이트로 운영한 것이었고, 두 번째는 다양한 방법으로 유권자의 데이터베이스를 확보하는 것이었으며, 끝으로 상세한 데이터 베이스를 바탕으로 마이크로 선거운동을 전개한 것이다.[45]

이러한 경향에 영향을 받아 우리의 중앙선거관리위원회는 대한민국 제19대 총선부터 트위터와 페이스북과 같은 소셜 네트워크 등 인터넷 상의 선거 운동을 상시 허용하였다.[46] 이에 소셜 미디어 상에서 선거 관련 데이터는 증

43) 채승병, "정보홍수 속에서 금맥 찾기: '빅데이터(Big Data)' 분석과 활용", 삼성경제연구소 SERI 경영 노트, 제91호, 2011, 1-12면; Converting Data into Business Value at Volvo, http://www.i-cio.com/case-studies/volvo-big-data.

44) "오바마가 인터넷 덕분에 당선되었다고 아무도 말하지는 않을 것이다. 그러나 인터넷이 없었다면 승리할 수 없었을 것이다. 오바마 측은 처음부터 인터넷을 온라인과 오프라인 선거운동을 한데 묶는 도구를 활용했고 인터넷은 선거운동의 중추신경과 같은 것이었다"고 한다. Washington AFP, 연합뉴스 2008.11.5.

45) http://blog.naver.com/PostView.nhn?blogId=mssophia&logNo=40119593734

46) 선관위, "인터넷 선거운동 상시 허용 결정(종합2보)", 연합뉴스, 2012년 01월 13일. ; http://bbs1.ag

폭되었으며, 2010년 대한민국 제5회 지방 선거 및 2011년 대한민국 재보궐 선거에서 소셜 네트워크 서비스의 중요성을 확인한 정당들 또한 SNS 역량 지수를 공천 심사에 반영하는 등[47] 소셜 네트워크 활용에 주목했다. 이 가운데 여론 조사 기관들은, 기존 여론조사 방식으로 예측한 2010년 제 5회 지방 선거 및 2011년 재보궐선거의 여론조사 결과와 실제 투표 결과와의 큰 차이를 보완하고자, 빅 데이터 기술을 활용한 SNS 여론 분석을 시행했다. 그러나 SNS 이용자의 대다수가 수도권·20~30대에 치우쳐있는 관계로[48] 빅 데이터를 이용한 대한민국 제19대 총선에 대한 SNS 분석은 수도권으로 한정되어 일치하는 한계를 드러내기도 했다.

(8) 문화

MLB (메이저 리그 베이스볼)의 “머니 볼”(Money Ball) 이론 및 데이터 야구머니볼 이론이란 경기 데이터를 철저하게 분석해 오직 데이터를 기반으로 적재적소에 선수들을 배치해 승률을 높인다는 게임 이론이다.[49] 이는 미국 메이저 리그 베이스볼 오클랜드 어슬레틱스의 구단장 빌리 빈이 리그 전체 25위에 해당하는 낮은 구단 지원금 속에서도 최소비용으로 최대효과를 거둔 상황에서 유래되었다. 빌리 빈은 타율·타점·홈런 등 흥행 요소만을 중시하던 야구계에서 출루율·장타율·사사구 비율이 승부와 관련되어 있음을 간파하고 데이터를 수집・분석하여 경쟁이 심한 MLB 인재 시장에서 가치만큼 평가를 받지 못하고 있는 선수들을 찾고, 드래프트를 할 고등학교와 대학 선수를 발굴하고 이들을 적재적소에 배치해, 최하위에 그치던 팀을 4년 연속 포스트시즌에 진출시키고 메이저리그 최초로 20연승이라는 신기록을 세우도록 탈바꿈 시켰다.

미국 월스트리트 저널은 미국 경제에 큰 영향을 끼치는 파워 엘리트 30인에 워렌 버핏, 앨런 그린스펀과 함께 빌리 빈을 선정[50]하는 등, 머니볼 이론은

---

ora. media.daum.net/gaia/do/debate/read?bbsId=D003&articleId=4627164

47) 새누리당, “SNS 역량지수, 주중 공천위 전달”, 연합뉴스, 2012.02.21.

48)“소셜 여론의 총선 예측 실패는 이용자 수도권 집중 때문”, 경향신문, 2012년 04월 24일.

49) '머니볼(Moneyball) 이론', "에듀윌 정보통신/오늘의 일반상식", 평생교육 No.1 에듀윌, (2012년 01월 11일). http://blog.eduwill.net/1079#comment_area ; http://www.danbinews.com/news/articleView.html?idxno=1462

50) Those Who Influence The Markets Most>>, The Wall Street Journal, (November 10, 2003).

경영, 금융 분야에서도 주목받았다. 최근 들어서 과학기술 및 카메라 기술의 발달로 더욱 정교한 데이터의 수집이 가능해졌으며, 투구의 궤적 및 투수의 그립, 타구 방향, 야수의 움직임까지 잡아낼 수 있게 되었다.[51] 이처럼 기존의 정형 데이터 뿐만 아닌 비정형 데이터의 수집과 분석, 활용을 통해 최근 야구경기에서 빅 데이터의 중요성은 더욱 커지고 있다.

(9) 의료

빅 데이터를 활용하면 미국 의료부문은 연간 3,300 억 달러(미 정부 의료 예산의 약 8%에 해당하는 규모)의 직·간접적인 비용 절감 효과를 보일 것으로 전망된다.[52] 특히 임상분야에서는 의료기관 별 진료방법·효능·비용 데이터를 분석하여 보다 효과적인 진료방법을 파악하고, 환자 데이터의 온라인 플랫폼화하여 의료협회 간 데이터 공유로 치료 효과를 제고하며, 공중보건 영역에선 전국의 의료데이터를 연계하여 전염병 발생과 같은 긴박한 순간에 빠른 의사결정을 가능케 할 전망이다.[53]

미국 건강보험 2위 업체인 웰포인트는 IBM이 개발한 왓슨을 통해 3,420만 명에 달하는 환자의 질병치료법을 제시한다. 이 과정에서 왓슨이 활용하는 정보는 엄청나다. 환자 차트와 의사, 병원이 갖고 있는 각종 질병 치료에 대한 기록, 보험회사가 보유한 치료법과 시술 자료, 왓슨 자체에 저장된 의료 논문에 이르기까지 활용할 수 있는 정보는 모두 왓슨의 손을 거친다. 왓슨이 정보를 처리하는 데 걸리는 시간은 단 3초에 불과하다.[54]

Ⅲ. 국내외 정책동향

1. 미국

미국은 대통령 직속기관인 과학기술정책실(the White House Office of Sci

51)"데이터 야구", http://ko.wikipedia.org/wiki/%EB%8D%B0%EC%9D%B4%ED%84%B0_%EC%95%BC%EA %B5%AC

52) James Manyika & Michael Chui, op.cit., p.36

53) 이성춘・임양수, "Big Data, 미래를 여는 열쇠", KT경제경영연구소, 2011년, 12쪽.

54) http://news.mk.co.kr/newsRead.php?year=2012&no=614916

ence and Technology Policy, OSTP)의 주도아래 “빅 데이터 이니셔티브” (Big Data Research and Development Initiative)를 발표하였다. 실행방법으로 ‘Big Data Senior Steering Group(BDSSG)’을 운영하고 있는데 빅 데이터를 통한 과학발견 및 혁신 프로세스 가속화, 새로운 경제적 성장의 촉진, 새로운 연구 영역 및 분야 선도를 비전으로 하고 있다.

미국은 연방 정부의 정보기술 R&D에 대한 투자가 슈퍼컴퓨팅과 인터넷의 개발의 획기적 발전을 이끌었던 것처럼, 이번 빅 데이터 이니셔티브 역시 과학, 환경, 바이오 연구, 교육 그리고 국방 영역과 관련된 빅 데이터 처리 역량을 획기적으로 증가시킬 것으로 예상하고 있다. 그러나 각 부처와 기관의 불충분한 사전 조사 및 통합 스케쥴 미비로 차질을 겪고 있으며, 부처간 유사한 내용의 수많은 프로젝트가 추진되어 중복 투자 문제점이 제기되고 있는데, 이러한 점들은 우리나라가 빅 데이터 정책과 전략을 짜는데 타산지석으로 삼아야 할 것이다.

미국에서 빅 데이터를 이용한 구체적인 예를 살펴보면, 2010년 기준으로 탈세 금액이 저소득층 의료보장 총액을 초과하는 등 탈세와 사기로 국가 재정에 누수가 발생하자 국세청이 대용량의 데이터와 다양한 기술을 결합한 탈세 및 사기 범죄 예방 시스템을 구축한 바 있고, 오하이오, 오클라오마 주 정부가 국세청 데이터와 고용데이터를 바탕으로 빅 데이터 분석을 통해 새로운 세원과 미납세금을 확인하기도 하였다. 미국 국립보건원은 75개 기업 및 기관과 파트너십을 통해 진행한 1000 유전체 프로젝트(1000 genomes project)의 일환으로 200TB의 유전자 정보를 확보하기도 하였다.

2. 일본

다음으로 일본의 경우를 보면, IDC 재팬에 따르면 2012년 일본 빅 데이터 기술·서비스 시장 규모는 2011년도의 142억 5000만엔 대비 38.2% 성정한 197억 엔에 달할 것으로 추산되고, 2011년부터 향후 5년간 39.9%의 연평균 성장률(CAGR)을 기록해 2016년에는 765억 엔의 시장을 형성할 것으로 전망했다. 다만 일본의 경우 빅 데이터 기술·서비스 시장이 일본 IT 시장 전체에서 차지하는 비중이 0.1%에 불과하여 아직은 여명기에 해당한다고 할

수 있다. 즉 데이터 분석을 통한 마케팅·상품개발의 활용에 관심이 증가하고는 있으나 실질적인 수요는 제한적인 것으로 분석된다.

공공분야와 관련하여서는 정부차원(건설성, 통산성, 운수성, 우정성, 경찰청)에서 지능형 교통 정보 시스템을 마련하였고, 일본 노무라연구소는 스마트폰형 네비게이션 서비스를 활용하여 2011년 일본 대지진 당시 도로교통 체증 피해를 최소화하기도 하였다.

이에 총무성이 2020년까지 중점 추진할 IT 분야의 전략 테마로 '대량 데이터 활용'을 선정하였고, 2013년도 예산안에 빅 데이터에 관한 연구개발을 지원하는 비용을 포함할 계획이다. 일본은 빅 데이터의 활용을 통해 정보 수요에 정확한 정보를 제공하고 효율적인 에너지 이용, 민간 부문 신규사업 창출 등의 효과를 기대하고 있다.

한·미·일 빅 데이터 R&D 추진 체계

구분	미국	일본	한국
의사결정기구	OSTP	국가전략회의	국가정보화전략위원회
R&D 추진기구	NSTC(NITRD)	총무성(정보통신심의회, ICT기본전략위원회)	빅 데이터 활용추진단(신설 제안)
참여 부처	상무부, 국방부, 에너지부, 보건부, 기타 독립기구	문부과학성 경제산업성	지식경제부, 방통위, 행정안전부 등

3. 영국 등

영국은 정부사이트(data.gov.uk)를 통해 공공 부문의 정보 공유 및 활용을 위한 데이터 원스톱 서비스를 제공하고 있다. 호주는 정보관리청을 중심으로 Government 2.0을 통한 정보를 개방(data.gov.au)하고 있으며, 싱가포르도 RAHS(Risk Assessment & Horizon Scanning)을 통해 질병, 금융위기 등 국가적 위험을 수집·분석하여 선제적으로 관리하고 있다.

4. 국내 추진 현황

가. 개요

우리나라는 대통령 직속 국가정보화전략위원회, 방송통신위원회, 지식경제부, 행정안전부를 중심으로 빅 데이터에 관한 정책수립을 추진하고 있다. 국가정보화전략위원회가 범정부적 데이터 연계와 분석체계 구축, 정부·민간 데이터 융합 추진, 공공데이터 진단체계 구축을 담당한다면, 각 부처는 소관 업무분야에서의 빅 데이터 기술을 개발하고, 산업을 육성하며 인력을 양성하는 등 세부 정책을 수립·시행하는 역할을 담당하고 있다.

나. 주요 위원회 및 부처별 추진 현황

국가정보화전략위원회는 국가정보화기본법을 근거로 지난 2008년 분산된 정보화 기능을 조정하고 부작용에 대응하기 위해 설립됐다. ICT 관련 업무가 여러 부처로 분산되면서 나타나는 난맥상을 조정해보자는 취지로 부처 위에 상위 거버넌스 체계를 두는 개념이다. 국가정보화전략위원회는 대통령 소속으로 국무총리와 대통령이 위촉한 민간위원장이 공동으로 이끌고 있으며, 그 산하에는 국가정보화전략실무위원회를 두고 있다. 국가정보화전략위원회는 지난 2011. 11. '빅데이터를 활용한 스마트 정부 구현(안)'을 발표하여 스마트정보를 구현하기 위해 공공정보 개방과 공유를 확대하고, 인터넷·SNS 등의 대용량 데이터분석 및 활용을 실현하기 위한 비전과 미래정책 방향을 제시하였다.
방송통신위원회 역시 빅 데이터와 관련하여 적극적인 행보를 보이고 있다. 방송통신위원회는 지난 6. 21. '빅 데이터 서비스 활성화 방안'을 발표했고, 방송통신, 교육, 교통, 의료 등 여러 분야에서 혁신적인 시범서비스를 발굴하여 빅 데이터에 대한 인식을 제고하고 이용자의 편익을 높일 계획으로서, 빅 데이터 기술과 서비스 플랫폼의 경쟁력을 강화시키고 전문인력 양성 및 개인정보보호 관련 법제도 개선을 주요 추진 과제로 선정하였다. 한편 방송통신위원회는 한국정보화진흥원(NIA), 한국정보통신진흥협회(KAIT)와 함께 통신사, 방송사, 전자업계, 빅 데이터 전문업체, 학계, 연구기관 등이 참여하는 '빅 데이터 포럼'을 출범시키기도 하였다.

행정안전부는 범정부적 차원에서 빅 데이터 마스터플랜을 수립할 계획으로, 자료를 체계적으로 분석하여 재난·환경문제 등에 사전 대응하기 위하여 데이터 분석 기반 정책수립·업무혁신, 맞춤형 대국민 서비스 제공 등을 위한 '빅 데이터 마스터 플랜'을 수립하고 후속조치를 마련 중에 있다. 행정안전부는 정부 기관들이 보유하고 있는 데이터들을 연계하여 분석할 수 있는 기능을 수행할 '빅 데이터 공통기반 시스템'을 구축할 계획으로, 2012년 11월부터 2013년 3월까지 사전 준비 작업을 진행한 뒤 구체적인 설계 및 운영방안을 마련하여 단계적 추진 로드맵을 수립할 계획이다.

다. 전자정부 3.0

우리나라의 전자정부는 기본적으로 「전자정부법」에 근거를 두고 있다. 전자정부법은 전자정부를 '정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부'라고 정의하고 있다(법 제2조 제1호). 전자정부법은 제4조에서 전자정부의 원칙 중 하나로 대민서비스의 전자화 및 국민편익의 증진(제1호), 행정업무의 혁신 및 생산성·효율성의 향상(제2호), 행정정보의 공개 및 공동이용의 확대(제4호)를 들고 있고, 제16조에서 행정기관 등의 장은 국민의 복지향상 및 편익증진, 국민생활의 안전보장, 창업 및 공장설립 등 기업활동의 촉진 등을 위한 전자정부서비스를 개발하여 제공하고 이를 지속적으로 보완·발전시키기 위한 대책을 마련하여야 한다고 규정하고 있으며, 제18조에서는 행정기관 등의 장으로 하여금 첨단 정보통신기술을 활용하여 국민·기업 등이 언제 어디서나 활용할 수 있는 행정·교통·복지·환경·재난안전 등의 서비스(이하 "유비쿼터스 기반의 전자정부서비스"라 한다)를 제공하여야 하며, 이에 필요한 시책을 마련하여야 할 의무를 부과하고 있다. 실현 방편으로서 제20조는 국가는 국민에게 전자정부서비스를 효율적으로 제공하기 위하여 인터넷 기반의 통합정보시스템(이하 "전자정부 포털"이라 한다)을 구축·관리하고 활용을 촉진하여야 한다고 규정하고 있으며 제21조에서 전자정부서비스의 민간 참여 및 활용을 규정하고 있다.
우리나라의 전자정부는 1990년대 집중적인 투자와 2000년대 과감한 행정혁

신 노력에 힘입어 세계 최고 수준을 유지하고 있다. 그러나 아쉽게도 빅 데이터에 관하여는 선구자적인 지위에 있다고 보기 어렵다. 영국과 미국은 데이터 포털 사이트(영국 : http://www.data.gov.uk, 미국 : http://data.gov)를 만들어 빅 데이터 공급과 활용을 장려하고 있다. 우리나라도 이와 유사하게 '공유자원포털'(http://www.data.go.kr)을 운영하고 있으나 빅 데이터라 부를 수준에 미치지 못하고 사용자의 편의성도 낮은 편이다. 민간에서 필요로 하고 국민생활과 밀접한 공공데이터의 대부분이 실시간 데이터라는 점에서 현재 실시간성 또는 갱신주기가 짧은 데이터는 Open API 방식으로 제공이 가능함에도 불구하고 공유자원포털에서 Open API로 개방하는 공공데이터는 13종에 불과한 실정이다.

라. 관련 법령의 제정 움직임

현재로서는 빅 데이터를 직접적으로 규율하는 법령이나 담당부처를 규정한 직제에 관한 법령은 제정되지 않은 실정이다. 관련 규정들은 앞서 본 「전자정부법」이나 「국가정보화 기본법」과 「통계법」, 「기상산업진흥법」, 「공간정보산업 진흥법」 등에 산재하여 있고, 관련 부처는 자신의 업무에 관련된 사업을 독자적으로 진행하고 있으며, 심지어 뒤에서 보는 바와 같이 빅 데이터의 수집과 분석을 어렵게 하는 개인정보 보호에 관한 강력한 법령들이 존재한다.

빅 데이터와 관련한 입법 움직임을 살펴보면, 우선 김을동 의원이 2012. 7. 31. 「공공데이터의 제공 및 이용 활성화에 관한 법률안」을 제출한 것이 눈에 띈다. 동 법률안은 공공과 민간의 빅 데이터 육성·관리를 직접적으로 규율하기 위한 법률은 아니다. 다만, 공공기관이 보유하고 있는 대량 정보의 효율적 이용 및 안정적인 민간 제공이라는 측면에서 참고적으로 살펴볼 필요가 있다. 동 법률안은 '제안이유'에서 스마트 기기 기반의 모바일 서비스 확산이 개인의 일상생활은 물론 기업의 업무 혁신, 신규 시장 창출 등 사회 전반에 일대 변혁을 일으키고 있고 이미 유럽연합, 미국, 영국 등 세계 각국은 법·제도적 기반을 마련하고 강력한 실행 리더십을 발휘하여 스마트 시대 사회·경제 성장의 원동력으로서 공공데이터를 적극 활용하고 있으나, 우리나

라의 경우 민간의 급증하는 활용수요에도 불구하고 공공영역에 축적되어 있는 데이터 제공이 수요에 부응하지 못하는 수준에 머물러 있어 공공데이터의 무한한 잠재적 가치가 사장되고 있는 실정이므로 이러한 데이터를 지속적이고 체계적으로 민간에 제공하고 이용을 보장하기 위하여 법률 제정을 통한 안정적 지원기반을 마련함으로서 우리나라를 스마트 선진국으로 도약시키는 추진 동력을 마련하는데 입법 취지가 있다고 설명하고 있다.
동 법률안은 공공기관이 보유·관리하는 데이터의 제공 및 그 이용에 관한 사항을 규정하고 있으며 총칙, 공공데이터 정책의 수립, 공공데이터 등록 등 제공기반 조성, 공공데이터의 제공절차 및 보칙 등, 부칙을 제외하고 총6장 38개 조문으로 되어 있다. 동 법률은 대통령 소속 공공데이터전략위원회를 두고, 공공데이터활용지원센터를 설치·운용하도록 하고 있으나, 대통령 소속 국가정보화전략위원회 등과의 역할 분담에 관한 논의가 부족하고, 공공제공 데이터를 이용한 이용자에 대한 면책규정 미비 등이 문제로 제기되고 있다.

Ⅳ. 빅데이터의 문제점과 개인정보보호의 필요성

급변하는 새로운 환경 속에서 대다수의 사람들은 신규 기술에 대한 장점에 치중한 나머지 잠재적 위험에 대한 연구 및 고찰이 심층적으로 이루어 지지 않고 있다. 특히 이와 같은 빅데이터 환경 속에서 발생할 수 있는 또 하나의 커다란 문제로서 개인정보보호가 중요한 문제로 등장하게 되었고,[55] 다수의 개인 사용자들 개인정보가 남용될 수 있다는 부분에 대해 가장 많이 염려하고 있다[56]. 또한 2011년 Gartner CIO 조사 결과에 따르면, 기업 CIO들은 빅데이터/클라우드 컴퓨팅 환경에서 보안 및 개인정보보호에 대해 가장 관심을 가지고 있었다.[57] 이하에서는 빅데이터 환경 속에서 발생할 수 있는 개

55) 다수의 이용자들 역시 이에 관한 문제에 많은 관심을 보이고 있다. 미국의 보안 컨설팅 업체 포네몬(Ponemon)이 2010년 미국 및 유럽 6개국의 127개 사 업자를 대상으로 클라우드 서비스 보안 인식에 대한 설문 조사를 실시한 결과에 따르면, 미국은 73%, 유럽은 74%의 사업자가 클라우드 자원 보호를 위한 별도의 보안을 적용하지 않고 있는 것으로 드러났다. 박대하/백태석, 전게논문. 37면 참조.

56) 민옥기, “훤히 보이는 클라우드 컴퓨팅,” pp. 42, 2009년 10월; Security of Cloud Computing Providers, Ponemon, 2011년 4월, 1-2면.

57) Gartner, "Cloud computing ranks as the top concern of CIO’s agendas for 2011,” pp. 4-9.

인정보보호에 관한 문제점을 살펴보고자 한다.

1. 빅데이터 이슈

위에서 살펴 본 바와 같이 기기간의 융합에 의한 사람과 사람 및 사람과 생활환경간의 상호소통에 의해 생성되는 빅 데이터는 그 데이터의 소유자의 정책방향에 따라 다양한 지식을 창출할 수 있으며, 그 지식의 창출은 개개인의 정치적·문화적·경제적 성향이나 형태 등에 대한 식별할 수 있거나 식별할 수 없는 모든 데이터를 대상으로 정보처리자가 원하는 목적의 예측프로그램(패턴 분석프로그램)에 의하여 하여 생성되는 결과 해당 데이터의 수익자는 기업 등 정보소유자 내지 정보처리자인 반면 희생자는 해당 데이터의 귀속주체인 정보주체로 될 수 있다.[58]

이와 같이 생성된 정보는 클라우드 컴퓨팅기술에 의하여 확장된 정보저장능력과 다양한 유형의 미래예측 프로그램간의 결합에 의하여 프로그램설계자가 원하는 것 이상의 새로운 지식창출을 가능하게 하고 있다. 이와 같이 지식화된 정보는 순기능적으로 보면, 개개인의 현재 수요를 통한 미래수요의 예측은 물론이거니와 우리의 생활환경에서 발생할 수 있는 각종 재난이나 범죄의 예방을 가능하게 할 것으로 예측되는 반면, 역기능의 측면에서 보자면, 개인이 원하지 아니하는 인격의 형성이나 개인에 대한 실시간의 감시를 비롯하여 향후의 행동방향에 대한 예측도 가능하게 하고, 프로그램에 대한 공격 내지 조작을 통해 각종 재난을 야기하게 하는 테러의 수단으로 사용될 가능성 또한 배제할 수 없는 동전의 양면성을 내포하고 있다.

이러한 빅 데이터 내지 클라우드 컴퓨팅 시대에 있어서 이슈로 될 문제에 대하여는 다음과 같은 견해가 제시되고 있다. 첫째, 「빅 데이터 환경에서의 개인정보보호와 관련해 기술적 측면에서는 크게 3가지를 제안할 수 있을 것 같다. 사용자, 컨텐츠, 매체를 한 번에 검증할 수 있는 통합인증에 대한 요구, 그리고 능동적 패턴인식이 가능한 지능형 모니터링 체계를 중심으로 한 대용량 개인정보 유출방지 솔루션 도입, 그리고 Privacy Compliance, 즉 개인정보보호 기술기반 관련 법·제도를 체계적으로 시스템에 적용·인지시키는 과정이 필요할 것으로 본다」[59]고 하여 개인정보의 통합인증과 보안을 위한

58) "빅데이터 논란의 희생자는 수요자이다". http://www.itdaily.kr/news/articleView.html?idxno=34723

59) 홍승필 성신여대 교수, http://www.boannews.com/media/view.asp?idx=33306

법제정비를 지적하는 견해가 있다.

둘째로, 「빅 데이터는 정보 집적의 고도화와 정보 결합의 고도화, 그리고 정보 분석의 고도화로 대변된다. 이렇듯 집적되고, 결합되며, 분석된 정보를 바탕으로 상업적으로 개인별 맞춤 활용이 가능해 프라이버시 침해 위험이 커지고 있는 것이다. 이와 함께 개인정보의 국외 이전 문제도 주요 이슈가 된다고 볼 수 있다"는 점을 지적하면서 "이로 인해 향후 법제화 과정에서 기존 개인식별정보 및 민감정보 등으로 한정된 개인정보의 개념을 개인에 관한 모든 정보로 확대할 필요가 있다. 여기에 정보의 프로파일링을 반대할 권리 등 개인정보의 동태적 측면의 규율방안과 개인정보의 국외이전에 대한 강력한 통제장치를 마련할 필요가 있다」[60]고 하여 프라이버시 침해 및 개인정보의 국외이전이 빅 데이터 시대의 법적 문제가 될 것임을 지적하고 있다.

셋째로,「현재의 디지털 시대를 이끌어가는 글로벌 기업들은 모두 빅데이터의 중요성을 알고, 효과적으로 활용하는 기업이다. 사용자들과 소비자들의 감정을 읽기 위해서는 결국 데이터를 활용할 수밖에 없고, 이는 사람들이 디지털에 남기는 흔적, 즉 디지털 풋프린트(Digital Footprint)의 분석을 통해 유추할 수 있기 때문이다. 디지털 시대에는 빅데이터가 과거 아날로그 시대의 부품과 소재라고 할 수 있다. 이렇기에 빅데이터는 기업에게는 디지털 시대를 선도할 수 있는 매우 핵심적인 자산이 될 수 있다. '구슬이 서말이라도 꿰어야 보배'라는 말처럼 데이터는 연결되고, 분석되어야 새로운 가치를 만들어낼 수 있다. 그러나 우리나라는 데이터 활용에 대한 장벽이 아직까지 높고, 법 기준도 모호한 편이다. 빅데이터에 대한 새로운 가이드라인과 지침은 반드시 필요하지만, 이 과정에서 활용과 보호의 균형을 찾는 노력이 병행되어야 한다고 본다」[61]고 하여 실시간으로 생성되는 디지털 데이터의 활용과 보호의 조화성을 강조하고 있다.

넷째로 「빅데이터 환경에서의 개인정보 활용에 있어 가장 중요한 것은 사용목적을 명확히 하는 것이다. 통계·역사·연구목적 외에 상업적인 마케팅 용도로써의 활용은 원칙적으로 맞지 않다고 본다. 결국 개인정보는 수집시 뿐만 아니라 이용, 제공 등을 위한 결합, 가공, 조합, 통합, 연동 등에 있어서

60) 최경진 가천대 교수, ibid.

61) 채승병 삼성경제연구소 수석, ibid.

도 최소처리 원칙과 목적 외 처리금지 원칙이 준수되어야 한다」[62]고 하여 목적외 사용에 대한 통제를 강화하여야 한다는 견해를 제시하고 있다.
다섯째로「개인정보의 범주와 관련해서는 현재 국제표준화 기구에서의 프라이버시 프레임워크를 통해 국제표준 논의가 마무리될 시점에 와 있다. 특히, 빅데이터에서 가장 이슈가 되는 결합되고 연결되는 정보의 중요성에 대한 논의도 진행되고 있다」[63]거나 「빅데이터와 개인정보보호를 관통하는 것은 바로 연결성이라고 본다. 각종 정보가 연결돼 새로운 정보로 가공되는 측면에 대한 논의가 더욱 필요하리라 생각한다」[64]는 견해 등 개인에 관한 정보의 연결성과 이러한 연결로 인한 프라이버시보호를 위한 국제표준노력의 제고를 촉구하는 견해 등이 있다.

2. 종래 개인정보보호 정책의 무력화

앞서의 빅 데이터의 활용기술 및 활용에 의하거나 위에서 제시한 이슈 등에 의하게 되면, 빅 데이터 기술은 분산된 데이터와 데이터간의 연결 및 프로파일링 등에 의하여 개인의 식별정보를 중심으로 한 데이터뿐만 아니라 식별정보와 연결되지 아니한 데이터에 대하여도 맞춤서비스가 가능할 정도로 상품화되어 있다고 한다. 예컨대, 미국은 10년마다 행하여지는 인구 센서스데이터가 수집되고 비식별화되어 있지만 많은 미국인의 데이터는 이미 상품화되어 있을 뿐만 아니라 미국 전체 인구의 87%는 출생연월일, 성별 및 우편번호 등과 데이터 마이닝에 의한 추론가능한 개인별 데이터 등을 조합하는 기능을 가진 매칭프로그램 등에 의하여 이미 식별가능한 데이터베이스로 구축되어 있는 결과 개인에 관한 각종 데이터의 비식별화에 기반을 둔 각종 정책은 정보사회의 문제점을 더 이상 해결할 수 있는 수단이 되지 못한다고 한다.[65]

62) 이창범 김·장 법률사무소 위원, ibid.
63) 신용녀 한양사이버대 교수, ibid.
64) 진승헌 한국전자통신연구원 팀장, ibid.
65) Jane Winn, "Intensification of Personal Information Protection by the Development of Big Data and SNS in the USA", "2101 International Conference on Recent Trend of Personal Information Protection", 2012.11.1. "22쪽

3. 빅데이터환경에서의 개인정보

「개인정보 보호법」에 따르면 “개인정보”란 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.[66] 또한 개인정보의 넓은 의미로 가장 많이 사용되는 Privacy에 대하여 OECD Privacy Guidelines에서는 “사용자의 개인 정보의 사용 및 접근에 대한 이해를 보장하는 것”이라 명시하고 있다. 이때 빅데이터 환경에서의 개인정보란 빅데이터 서비스를 위해 수집, 저장, 처리 및 이용 되는 개인에 관한 모든 정보를 의미하며, 개인정보 처리과정에서 새롭게 생성되는 모든 정보를 포함한다. 이러한 개인정보는 서비스 제공자와 이용자 간 정보 주체 및 소유에 따라 개인정보보호의 범위를 합리적으로 규정하고 통제 절차를 수립하는 것이 매우 중요하다.[67]

빅데이터 환경에서 개인정보의 분류				
데이터의 유형		하위유형과 실례		
정태정보	아이덴티티	오프라인	생체정보	・지문, 홍채, 인증키 등
			경제정보	・계좌 및 신용카드 번호 등
			사회적 정보	・종교, 동호회 등
			관계적 정보	・자녀, 부모, 배우자 ・자녀에 대한정보
			부동산 관련 정보	・집, 직장 주소 등
		온라인	디지털 아이덴티티	각종 계정, 이메일 주소 사용자명, IP주소 등
	자산	유형자산	재산	・부동산, 차량, 기타 보유물 ・주식, 계좌내 잔액 등
		낮은수준	・거래내역, 여행기록, 통화내역 등	

66) 「개인정보 보호법」[법률 제10465호, 2011.3.29]

67) 유우영/임종인, 전게논문, 339면.

동태 정보	통시적 데이터	높은 수준	・빅데이터 환경에서 수집된 로그 데이터(시간, 장소
	실시간 데이터	・유비쿼터스 환경에서 수집된 데이터	
파생 정보	분석데이터	・시간흐름에 따라 수집되고 분석된 데이터 -경제적 데이터 : 매달 잔고의 흐름 -새로운 제안에 대한 응대 패턴 : 경험 근무 -사회적 행동 : 약물 사용, 위법사항, 가족 특성 등 -취향 : 소비패턴 - 계층에 따른 아이템으로 분류 가능(구매설득)	
	통합데이터	・다른 데이터와 결합된 개인정보 -DNA분석 : 정신질환을 포함한 유전질병 발병 가능성 -다자간 연계 데이터 : MAC어드바이스를 제공하는 기기들의 위치로 현재 위치 및 활동시간을 추정	

표 5 신덕호, 유비쿼터스 컴퓨팅 환경에서의 개인정보보호정책 발전에 관한 연구, 단국대학교 석사학위논문, 2009, 87면.

4. 빅데이터 환경에서 개인정보보호 중요성

정보통신 기술의 발전에 따라 정보의 수집, 저장, 유통이 손쉬워지고, 상업적인 서비스는 물론이고 공공행정이나 교육 등 다방면에 걸쳐 정보주체의 개인정보 수집 및 활용이 용이해짐에 따라 그에 대한 보호조치 및 정보주체의 권리보장이 요구되고 있다. 현재 국내외 기업과 공공기관에서는 다양한 개인정보를 획득하고 관리하며 이용함으로써 조직 본연의 역할을 수행하고 있다. 조직이 가지고 있는 정보를 보호하는 것은 현대와 같이 인터넷에 기반을 둔 정보시스템을 운영하는 대부분의 기업에서 더욱 중요한 문제가 되고 있으며, 특히 빅데이터 환경에서는 조직의 개인정보 보유량 및 위탁 관리의 증가 등으로 인해 개인정보보호의 중요성이 증대되고 있다.[68] 이에 따라 개인정보의 수집・이용은 정보 주체의 인식 또는 자발적 동의를 그 전제로 하고 있으나, 빅데이터 환경에서는 정보의 수집과 이용이 무의식적이며, 동의를 받을 수 없는 상황에서 이루어질 가능성이 높기 때문에 이용단계에서의 통제를 보다 강화함으로써 그 실질적인 보호를 확보할 수 있을 것이다.

68) 박대하/백태석, 클라우드 컴퓨팅 개인정보보호 연구동향과 과제, 한국정보보호학회, 정보보호학회지 21(5), 2011.8. 39면..

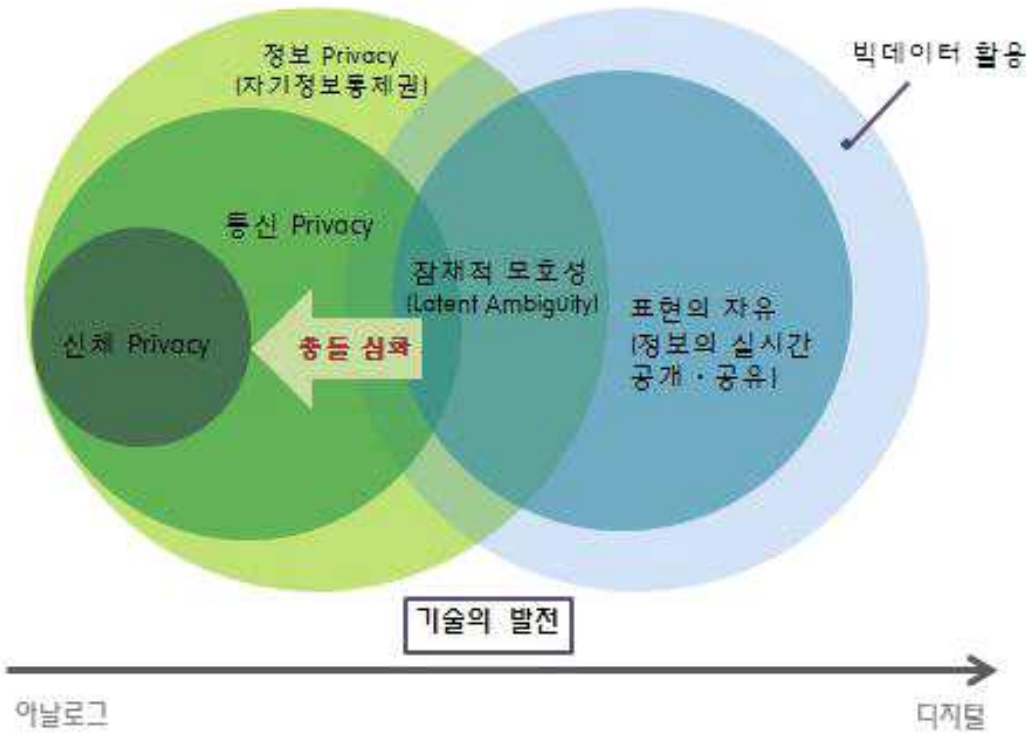


그림 8 프라이버시 외연 확장과 정보 공개·공유와의 충돌 : 류종현 “사이버스페이스에서 ‘표현의 자유’와 ‘프라이버시권’의 갈등에 관한 연구”, 고려대학교 박사학위논문, 2005, 157면.

5. 빅데이터 환경에서의 개인정보 침해유형

개인정보의 침해란 정보주체와 관련된 제반의 정보가 도용, 유출, 변경, 훼손 등과 같은 방법으로 오용되거나 남용되어 정보주체의 자기통제권이 침해되는 것을 말한다. 특히 빅데이터 환경에서 발생할 수 있는 개인정보침해의 유형은 ① 부적절한 모니터링, ② 부적절한 접근 및 수집, ③ 부적절한 이전, ④ 부적절한 분석, ⑤ 동의받지 아니한 영업행위, ⑥ 부적절한 저장 등으로 그 형태를 나눌 수 있다. 개인정보 보호법에 따른 침해의 유형으로는 이용자의 동의 없는 개인정보의 수집, 수집시 사전 고지 의무 또는 명시의무 불이행, 과도한 개인정보의 수집, 고지·명시한 범위를 넘어선 이용 또는 제3자 제공 개인정보 취급자에 의한 훼손·침해 또는 누설, 개인정보처리 위탁시

고지의무 불이행, 영업의 양수 등의 통지의무 불이행, 개인정보관리책임자의 미지정, 기술적·관리조치 미비로 인한 개인정보 누출 등, 수집 또는 제공받는 목적 달성 후 개인정보 미파기, 동의철회·열람 또는 정정요구 불응 등과 같은 동의철회, 열람·정정을 수집보다 쉽게 해야 할 조치 미 이행, 법정대리인의 동의 없는 아동의 개인정보 수집, 타인정보의 훼손·도용·침해·누설, 명예 훼손 등으로 나누어 볼 수 있다. 단지 그 비중이나 형태의 변화가 다소 차이가 있을 수 있겠으나, 이러한 침해의 방법이나 유형은 빅데이터 환경에서도 유사하게 나타날 수 있다. 특히 종래의 개인정보보호가 개인의 신상정보나 신용정보 등에 집중되었다면, 빅데이터 환경에서는 개인의 생활패턴이나 성향 등에 대해 분석할 수 있게 되므로, 빅데이터 환경 하에서의 개인정보 침해는 개인정보 수집과 관련하여 모든 사람이 자신의 의지와 관계없이 상시적으로 정보를 수집당할 수 있는 환경에 놓이게 될 수 있으며, 현재의 제시되고 있는 일반적인 개인정보 침해 그 이상의 위험이 발생할 수 있다고 할 것이다. 특히 한번 수집된 개인정보는 기술적으로 전전(轉傳) 유통이 용이하고, 정보의 공유자를 파악할 수 없다는 점에 문제가 있다. 이와 같은 빅데이터 환경에서의 개인정보 침해는 개인의 사적 공간과 개인의 안정성 위협, 사회적 배제 초래, 기업과 소비자 혹은 정보를 가지고 활용하는 자와 정보를 단순히 제공하는 자 간의 힘의 불균형이 발생한다는 점에서 중대한 위협이 될 수 있다는 문제점을 가지고 있다.[69]

6. 정리(검토)

이상에서 빅데이터/클라우드의 개념과 특징, 빅데이터의 활용현황과 구체적인 사례 그리고 빅데이터 환경에서 발생할 수 있는 개인정보보호와 관련된 문제를 살펴보았다. 빅데이터란 단어가 의미하는 바와 같이 단순한 데이터의 양적인 측면에서의 접근이 아니라 수집된 다양한 정보의 신속한 처리를 통해 새로운 정보를 형성하는 일련의 과정에서 발생하는 막대한 데이터를 말하는 것으로, 정체되어 있는 저장수단으로서의 데이터가 아니며 능동적인 가

69) 신덕호, 유비쿼터스 컴퓨팅 환경에서의 개인정보보호정책 발전에 관한 연구, 단국대학교 석사학위논문, 2009. 90면.

치를 가진 정보라고 할 수 있다. 이러한 정보의 수집과 분석을 통한 새로운 가치의 창출을 통해 다양한 분야에서 활용할 수 있었다. 가령 기존의 데이터를 분석하여 정상과 비정상상태를 파악하고 비정상상태에 적극적으로 대처할 수 있으며, 먼 미래가 아닌 가까운 미래에 대한 예측을 하고 즉각적인 대처를 할 수 있었으며, 현재의 주변상황을 분석할 수 있었다. 이러한 것을 실제로 사용하고 있는 사례들로서 일상에서 흔히 사용하고 있는 실시간 교통정보서비스나 고객의 행태를 분석하여 이를 기초로 하여 이탈을 방지하기 위한 일련의 대처를 하는 것을 보았고, 위치기반 서비스를 통해 고객의 현재 위치에서 적합한 서비스를 제공하는 등 각종의 다양한 서비스가 제공되는 것을 보았다. 하지만 빅데이터가 가지고 있는 이러한 편리한 서비스에도 불구하고 염두에 두어야 할 것으로 개인정보보호의 문제가 있었다. 특히 서비스 영역에서 활용되고 있는 빅데이터 서비스는 고객의 정보를 수집하고 분석을 통해 다음 서비스를 제공하는 것으로 기초적인 정보의 수집이 전제로 하고 있다. 하지만 이렇게 수집된 정보는 쉽게 이동할 수 있으며, 국내를 넘어서 국외까지 손쉽게 이전될 가능성을 가지고 있다. 또한 수집된 개인정보의 보존과 파기가 문제가 된다. 이러한 문제에 대하여 어떻게 대처하여야 할 것인가가 본 보고서의 쟁점이라 할 수 있다.

제3장 빅데이터와 관련한 해외 법제 동향

Ⅰ. UN

UN에서 프로파일링을 직접적으로 규율하기 위한 규범은 아직 제정되지 않았다. 다만, 개인정보의 보호와 관련하여 1990년 12월 14일 총회에서 결의·채택된 “컴퓨터화된 개인정보 파일의 규율 지침(Guidelines for the regulation of computerized personal data files, A/RES/45/95)”에 개인정보의 수집 및 활용에 관한 기본적인 합의가 규정되어 있으며, 구체적인 내용은 다음과 같다.

1. 합법성 및 공정성의 원칙 (Principle of Lawfulness and Fairness)

개인에 관한 정보는 합법적인 방법으로 수집, 처리하여야만 하고 UN헌장에 명시된 목적과 원칙에 반하여서는 안된다는 원칙으로서, OECD의 8원칙 중 수집제한의 원칙과 그 맥을 같이 한다. 이에 의하면, 쿠키나 트랙킹 소프트웨어의 설치 및 활용이 단순한 개인적 편의를 넘어 타인의 비밀정보 유출이나 프라이버시 침해에까지 이르는 경우에는 해당 개인정보의 수집·처리행위는 불법하게 된다.

2. 정확성의 원칙 (Principle of Accuracy)

개인정보를 수집하거나 저장하는 사람 및 이에 관하여 책임 있는 담당자는 개인정보를 정기적으로 검사하여 수록된 정보가 정확한 정보인지를 검토하여야 한다는 원칙으로서, OECD 8원칙 중 정보의 정확성 원칙과 유사한 내용이다. 이 원칙은 소극적인 측면에서 부정확한 정보로 인하여 정보주체가 피해를 입지 말아야 한다는 취지이다. 프로파일링된 정보는 단편적이거나 연속된 정보 또는 개인식별이 불가능한 정보들의 조합이나 나아가 개인식별정보와의 결합을 통하여 생성된다. 그런데, 대부분 프로파일된 정보는 일반 정보보다 광범위하고 보다 정확하겠지만, 각종 정보들이 프로파일링되는 과정에서 일정한 추론·분석·조합 등이 이루어지는 경우가 많은데, 이 때문에 정확성이 떨어지는 경우도 생각할 수 있다. 정확성의 원칙은, 이러한 부정확한

프로파일정보로 인하여 정보주체가 피해를 입는 경우가 없도록 법정책이 추진되어야 한다는 점을 천명한 것이다.

3. 목적 명확화의 원칙 (Principle of Purpose-Specification)
개인정보의 수집 및 처리의 목적은 구체적이고 정당하여야 한다. 즉, 모든 개인정보는 특정된 목적과 관련해서 수집 및 처리되어야 하고, 이러한 개인정보는 정보주체의 동의가 없는 한 다른 목적에 이용되거나 공개되어서는 안되며, 특정의 목적에 필요한 기간을 넘어서서 저장되어서는 안된다는 원칙이다. 이 원칙은 특히 쿠키나 트랙킹 소프트웨어에 의하여 수집된 정보가 다른 제3의 기관이나 업체가 보유하고 있는 정보와 결합될 때에 중요한 의미를 가진다. 즉, 쿠키나 스파이웨어를 이용하여 개인정보를 수집한 네트워크 광고자나 정보통신서비스제공자는 정보주체의 동의가 없는 한, 제3자에게 무단으로 제공되거나 소비자를 위한 마케팅 목적 등 쿠키나 트랙킹 소프트웨어를 필요로 한 목적을 넘어서 활용하지 말아야 한다.

4. 정보주체 접근의 원칙 (Principle of Interested-Person Access)
정보주체는 자신의 정보가 어떻게 처리되며 이용되는지에 관하여 알권리를 가지며, 잘못되거나 정확하지 않은 정보의 삭제권 등 여러 보호권리가 정보주체에게 부여되어야 한다는 원칙으로서, OECD의 8원칙 중 개인참가의 원칙과 유사하다.

5. 차별 배제의 원칙 (Principle of non-discrimination)
개인정보의 주체는 종교적, 인종적, 성별 차이나 정치적 견해 등을 이유로 부당하거나 자의적인 차별을 받아서는 안된다는 원칙이다.

6. 보안의 원칙 (Principle of Security)
자연재해, 컴퓨터 바이러스, 권한 없는 접근 등으로부터 개인정보 파일을 보호하기 위한 적절한 조치들을 취하여야 한다는 원칙이다. 이 원칙에 의하면, 프로파일링의 경우에, 프라이버시 향상 기술(Privacy Enhancement Technologies)의 개발 및 보급 등을 통하여, 특히 쿠키나 스파이웨어를 설치한 경

우에, 제3자가 무단으로 이를 활용하여 정보를 수집하지 못하도록 적절한 조치를 강구하여야 한다.

7. 예외 인정권 (Power to make exception)
국가안전보장, 질서유지, 타인의 자유와 권리 보호, 반인륜적 범죄를 범한 범인 추적과 같이 그 목적과 근거가 국내법 절차에 따라서 정당하게 제정된 법에 명시된 경우에 한하여 예외를 인정할 수 있다는 것이다.

8. 감독과 제재 (Supervision and Sanctions)
개인정보의 보호를 위하여 위 원칙을 준수하는지의 여부를 감독한 독립된 기관을 설치하여야 하며, 이들 원칙이 위배된 경우에 한하여 제재를 가하여야 한다는 내용을 담고 있다.

9. 국제적 정보 유통 (Transborder data flows)
개인정보가 국가간에 이동될 때 당해 국가들이 개인정보보호에 관한 충분한 보호대책을 마련하고 있다면 개인정보는 당해 국가들 사이에서 가능한 한 자유롭게 전달 및 처리될 수 있어야 한다는 것이다.

10. 적용 범위 (field of application)
위 원칙들은 모든 공적 및 사적 기관들에 적용되어야 하고 컴퓨터 파일뿐만 아니라 수작업 파일도 그 적용대상에 포함된다고 한다.

Ⅱ. OECD

OECD에서는 정보컴퓨터통신정책위원회(Committee for Information, Computer and Communications Policy) 과학기술산업분과(Directorate for Science, Technology and Industry)에 설치된 정보보안프라이버시작업반(Working Party on Information Security and Privacy)에서 쿠키나 웹버그(Web Bug) 등의 트랙킹 소프트웨어의 이용과 이를 통한 프로파일링에 대한 대응방안과 프라이버시 향상 기술(Privacy Enhancing Technologies)에 대하여

논의하였으나, 아직 합의된 규범을 만들어내지는 못하였다. 다만, OECD는 1980년 9월 국가간 합법적이고 자유로운 정보유통 및 정보처리산업의 보호를 도모할 목적으로 “프라이버시 보호와 개인정보의 국제적 유통에 관한 지침(Guidelines Governing the Protection of Privacy & Transborder Flow of Personal Data)”을 이사회 권고 형식으로 채택하여 개인정보보호를 위한 8개 원칙을 제시하였고, 1998년 10월에는 “범세계 네트워크상의 개인정보보호를 위한 각료선언(Ministerial Declaration on the Protection of Privacy on Global Networks)”을 채택하여, 1980년에 채택한 8개 원칙이 인터넷 환경에서도 적합하다는 점에 합의하였으며 세계 각국이 네트워크 환경에서 효율적인 프라이버시 보호를 위한 조치를 취할 것을 촉구하였다. 이 지침에 의하여, UN과 마찬가지로, 기본적인 규율방향은 채택되어 있는 상태이며, 프라이버시 보호를 위한 8개 원칙은 다음과 같다.

1. 수집제한의 원칙 (Collection Limitation Principle)

가. 개인정보의 수집 제한

개인데이터의 수집은 원칙적으로 제한되어야 하고, 합법적이고 정당한 절차에 의해 적절한(appropriate) 경우에 데이터 주체의 인지나 동의(the knowledge or consent of the data subject)를 얻은 후에 수집되어야 한다. 이것은 개인데이터의 수집제한, 개인데이터의 수집방법에 관한 요건이다. 예컨대, 개인데이터의 수집제한은 인종, 신조, 범죄기록 등 미묘한 데이터의 수집을 제한하고 있는 나라(유럽 제국)가 있는 반면, 본질적으로는 미묘한 데이터가 아니더라도 그 이용·처리 형태 여하에 따라서는 미묘한 것이 될 수 있는바 원칙적으로 개인데이터의 수집에는 한계를 두어야 한다는 것이다. 따라서 프로파일링을 위하여 일정한 장치나 프로그램에 의하여 개인정보를 수집하는 경우에도 개인과 관련된 민감한 정보(sensitive data)는 수집하지 말아야 하며, 수집된 정보가 개인을 식별할 수 없는 정보라고 할지라도 민감한 정보와의 결합을 통한 프로파일링은 제한되어야 한다.

나. 개인정보의 수집방법 제한

개인데이터의 수집방법에 있어서도 마이크를 숨겨서 데이터를 수집한다든가 데이터 주체를 속여 정보를 제공하는 일 등을 금하는 것이다. 인터넷 이용자

가 전혀 알지 못하는 사이에 스파이웨어가 그 이용자의 인터넷 이용 전반을 감시한다면, 이러한 스파이웨어의 설치 및 활용은 제한되어야 한다. 이처럼 데이터 주체에게 통지나 그 동의를 얻은 것은 일반적으로 중요하지만 실제 내지 정책적 이유로 그럴 필요가 없다고 생각되는 경우가 있다. 예컨대 범죄 수사활동이나 우편 송달 리스트의 통상적 개정 등이다.

2. 정보의 정확성 원칙 (Data Quality Principle)

개인데이터는 그 이용목적에 부합하는 것이어야 하고, 이용목적에 필요한 범위 내(to the extent necessary for those purposes)에서 정확하고 완전하며 최신의 것(accurate, complete and kept up-to-date)이어야 한다. 이용목적에 부합하여야 한다는 것은 개인데이터가 이용되는 목적과 관계가 있어야 한다는 것이며, 정확하고 완전하며 최신의 것이어야 한다는 것이 데이터 내용 개념의 중요한 요소를 이룬다.

3. 목적명확화의 원칙 (Purpose Specification Principle)

개인데이터를 수집하는 목적은 데이터를 수집할 당시에 구체화되어야 하며, 그 후의 이용은 구체화된 목적의 달성 또는 수집목적과 일치되어야 하고, 수집목적이 변경될 때마다 그 목적을 구체화하여야 한다. 이것은 정보의 정확성 원칙 및 이용제한의 원칙과 밀접하게 관련되어 있다. 이 목적구체화 원칙은 대체적 또는 보완적인 수단 예컨대 일반적인 공표, 데이터 주체에 대한 통지, 입법, 행정의 결정, 감독기관으로부터 나오는 라이센스 등에 의해 행할 수가 있다. 또한 이 원칙은 데이터가 목적에 적합하지 않게 되었을 때는 그것을 없애거나 이름을 없앨 것을 요구하고 있다.

4. 이용제한의 원칙 (Use Limitation Principle)

개인데이터는 정보주체의 동의(the consent of the data subject)가 있거나 법률의 규정에 의한 경우를 제외하고는 목적구체화의 원칙에 따라 확인된 목적 이외의 다른 목적을 위하여 공개, 이용, 그 밖의 사용에 제공되어서는 안된다는 원칙이다.

5. 안전보호의 원칙 (Security Safeguards Principle)

개인데이터는 분실 또는 불법적인 접근·사용·훼손·변조·공개 등의 위험으로부터 적절한 안전장치에 의하여 보호되어야 한다. 예컨대 출입문 잠금 ID카드에 의한 물리적 조치, 데이터의 액세스에 관한 권한의 레벨이라는 조직상의 조치 및 암호화, 이상행동에 대한 경고 등 정보상의 조치를 포함한다. 이는 UN 지침 상의 “보안의 원칙”과 맥락을 같이 한다.

6. 공개의 원칙 (Openness Principle)

개인데이터의 처리와 관련된 정보처리장치의 설치·활용과 관련정책은 일반에 공개하여야 한다. 또한 개인데이터의 존재·성질·주요 이용목적 및 데이터관리자를 식별하고, 그 주소를 명확하게 하기 위한 수단을 쉽게 이용할 수 있어야 한다. 이것은 개인참가 원칙의 필요요건이다. 쉽게 이용할 수 있는 수단이란 개인이 시간, 사전지식, 교통편, 비용 등에 관해서 부당한 부담을 지지 않고 정보를 얻을 수 있는 것을 의미한다.

7. 개인 참가의 원칙 (Individual Participation Principle)

개인은 자기에 관한 데이터의 소재를 확인할 권리를 가지며, 필요한 경우에는 자신에 관한 정보를 합리적인 시간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지받을 권리를 가진다. 이러한 권리가 거부되는 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기·정정·보완을 청구할 권리를 가진다. 이것은 프라이버시 보호를 위해 대단히 중요한 수단이며, 데이터에 대한 액세스권 행사의 절차는 간단해야 한다는 것이며, 이의 신청을 데이터의 관리자, 재판소, 행정기관 등에 대한 것으로 좁게 해석되어서는 안된다.

8. 책임의 원칙(Accountability Principle)

데이터관리자에게는 위에서 언급한 여러 원칙을 실시하기 위한 조치에 따를 책임이 부여되어야 한다. 여기에서의 책임은 법적 제재에 의한 책임 외에 자기규범에 규정되고 있는 책임도 포함된다.

Ⅲ. 미국

미국에서는 아직 프로파일링을 직접적으로 규율하는 법률은 제정되지 않았으며, 다만 프로파일링에 대한 규제를 하기 위한 2개의 법률안이 미국 의회 제107기 회기에 제출되어 있다. 또한 프로파일링을 직접 규율하고 있지는 않지만, 개인정보의 보호를 위한 여러 법률들이 제정되어 있다. 즉, 개인정보의 보호와 관련하여 포괄적인 입법을 지양하고 개별 분야별로 규율하는 단행법을 제정하여 시행하고 있다.
현재 개인정보와 관련된 법률로는, 1966년 제정된 정보자유법(Freedom of InromationAct), 1978년 금융프라이버시법(Right to Financial Privacy Act), 1980년 프라이버시 보호법(Privacy Protection Act of 1980), 1996년의 통신법(Communication Act), 1998년 11월에 상무부가 제시한 개인정보보호를 위한 세이프하버 원칙(Safe Harbor Principles), 2000년 4월의 아동 온라인 프라이버시 보호법(Child Online Privacy Protection Act) 등이 있다.
의회에 제출된 법률안은 “소비자 온라인 프라이버시 공개법(Consumer Online Privacy and Disclosure Act)”과 “소비자 인터넷 프라이버시 증진법(Consumer Internet Privacy Enhancement Act)” 등이 있었다.

법적 규율 외의 자율규제로서, 1999년 11월 온라인 프로파일링에 관한 워크샵에서 기업들은 Network Advertising Initiative의 창설을 공표하였고, 그 후 “NAI 원칙(The NAI Principles)”이 제안되었다.
이하에서는 세이프하버 원칙, 입법적 노력으로서의 2개 법률안 및 자율규제로서의 NAI 원칙에 대하여 살펴보겠다.

1. 세이프하버 원칙 (Safe Harbor Principles)

미국은 EU와의 무역을 위한 장벽을 제거하기 위하여 EU가 제시하는 개인정보보호기준을 준수하는지의 여부를 판가름하는 기준으로써 7가지 항목의 세이프하버 원칙을 제시하였다. 이 원칙을 충족하는 미국 기업은 EU 기준에 적합한 개인정보보호에 충실한 기업으로 추정되어 향후 아무런 제재 없이 E

U와의 개인데이터를 이전할 수 있다. 이 원칙은 1998년 11월 4일에 초안이 발표된 이후 5차례의 수정을 거쳐서 2000년 5월 31일 EU회원국의 만장일치로 그 내용에 대한 승인을 받았으며 2000년 6월 9일에 최종안 발표되었다. 세이프하버 원칙의 내용은 아래와 같다.

가. 고지 (Notice)

고지는 최초 정보수집 시 또는 그 후 가능한 빨리 통지하여야 한다. 그러나 최초 수집 목적 이외의 용도로 사용하는 경우 또는 최초로 제3자에게 정보를 공개하는 경우에는 반드시 사전에 통지하여야 한다.

나. 선택 (Choice)

개인정보의 제3자에 대한 공개, 최초수집 목적 외 이용의 경우에는 정보주체에게 그에 대한 선택의 기회를 제공하여야 한다. 일반적으로는 opt-out 방식을 취할 수 있지만 민감한 정보의 경우 opt-in 방식을 채택하여야 한다.

다. 제공 (Onward Transfer; Transfers to Third Parties)

제3자에게 정보를 공개하는 경우 통지 및 선택에 관한 원칙을 실행하여야 한다. 기업은 대리인으로서 활동하는 제3자에게 정보를 전송하고자 하는 경우, 그 제3자가 세이프하버 원칙에 가입하였거나 EU 지침 혹은 기타 적절한 방법을 준수하거나, 최소한 세이프하버 원칙의 관계조항이 요구하는 정도와 동일한 프라이버시 보호를 제공한다는 서면협정을 그 제3자와 체결하여야 한다. 또한 제3자가 이러한 요건을 충족한다면, 기업은 제3자가 제한사항 등에 반하여 그 정보를 처리하고 있음을 알았거나 알 수 있었거나 제3자의 처리를 방지하기 위한 적절한 조치를 취하지 않은 경우를 제외하고는, 제3자가 어떠한 제한사항 등에 반하여 그 정보를 처리하고 있는 것에 대하여 책임을 지지 않는다.

라. 안전 (Security)

개인정보 관련 기록을 생성, 유지, 이용 또는 보급하는 기업은 손실과 오용, 비인가 접근, 공개, 변경이나 파기로부터 보호하기 위한 합리적 예방조치를 취하여야 한다.

마. 데이터 무결성 (Data integration)

세이프하버 원칙에 적합하도록 개인정보는 사용목적과 연관성이 있어야 한다. 기업은 당초 수집 목적 또는 개개인이 이후 허가한 목적과 양립할 수 없

는 방법으로 정보를 처리할 수 없다. 그러한 목적에 맞게 필요한 경우, 기업은 정보의 원래 목적에 맞는 사용, 정확성, 완전성, 그리고 최신성을 보장하는 합리적인 조치를 취하여야 한다.

바. 접근 (Access)

개인은 자신에 관한 정보에 접근하여 그 비용이 개인의 프라이버시에 비해 그리 크지 않고 다른 사람의 프라이버시가 손상되지 않는 범위 내에서 이를 수정하거나 삭제할 수 있어야 한다.

사. 강제 (Enforcement)

효과적인 프라이버시보호는 원칙의 준수 및 원칙을 준수하지 않음으로 인하여 영향받는 개인을 위한 청구권, 원칙을 준수하지 아니한 기업에 대한 제재 등을 확실히 할 수 있는 체계를 포함하여야 한다. 최소한 이러한 체계는 (a) 항의와 분쟁이 “원칙 및 관계법령 혹은 민간분야가 설정하여 산정한 손해액”에 의거하여 조사되고 처리될 뿐만 아니라 쉽게 이용가능하고 독립적이며 경제적으로 감당할 수 있는 구제 수단과, (b) 프라이버시 처리 관행에 관한 산업계의 주장 등이 진실하고 그러한 관행이 현재에 이행되고 있음을 확인할 수 있는 지속적 절차, (c) 원칙의 준수를 확약한 기업의 비준수로 제기된 문제를 구제하기 위한 의무 및 그러한 기관의 제재 등을 포함하고 있어야 한다.

제재조치는 기업의 원칙준수를 보장하기 위하여 엄격하여야 한다. 또한 매년 자체 검증 보고서를 제출하지 않으면, 세이프하버 원칙에 따르는 보호대상에서 제외된다.

2. 과거 프로파일링 관련 법안

가. 소비자 인터넷 프라이버시 증진법

“소비자 인터넷 프라이버시 증진법(Consumer Internet Privacy Enhancement Act, 이하 ‘CIPEA’)”은 2001년 1월 20일에 미국 하원 자원통상위원회(Committee on Energy and Commerce)에 제출되었다. 이 법안에 의하면, 종래의 인터넷상의 프라이버시 보호에 대하여 보다 구체적으로 접근하여, 프라이버시 침해 가능성이 있는 기술적인 조치, 특히 프로파일링을 가능하게 하는 쿠키나 트랙킹 소프트웨어에 의한 개인정보의 수집에 대한 규제도 포

함하고 있다.

CIPEA는 개인식별정보(Personally Identifiable Information)의 수집과 관련하여, ① 고지(Notice) 및 ② 마케팅 목적으로 이용하는 것 또는 웹사이트에 의하여 제공된 제품·서비스의 제공과 관련이 없는 경우이거나 법에 비공개로 규정된 경우임에도 불구하고 수집된 개인식별정보를 제3자에게 공개하는 것을 이용자가 제한할 수 있는 기회를 부여하지 않는다면, 상업적 웹사이트 관리자는 해당 웹사이트의 이용자로부터 온라인 상의 개인식별정보를 수집하는 것은 불법이라고 규정하고 있다(Section 2. (a)). 또한 CIPEA는 "수집(Collect)"이라는 개념에 대하여 '수집하는 방법이 직접적이든 간접적이든, 능동적이든 수동적이든 관계없이 일정한 수단에 의하여 서비스나 웹사이트의 제공자 또는 운영자가 직접 또는 이들을 위해서 인터넷 서비스, 온라인 서비스 또는 상업적 웹사이트의 이용자에 대한 개인식별정보를 모으는 것'이라고 정의하고 있다(Section 6. (3)). 특히 동 규정에서 '쿠키의 이용을 포함하여 서비스나 웹사이트의 이용자와 연결된 일정한 식별 코드의 추적 또는 이용이 있는 경우'에도 수집에 포함한다고 규정함으로써, 프로파일링을 위한 쿠키 등의 프로그램에 의한 개인정보의 수집도 규율의 대상으로 하고 있다.

나. 소비자 온라인 프라이버시 공개법

"소비자 온라인 프라이버시 공개법(Consumer Online Privacy and Disclosure Act, 이하 'COPDA')"은 2001년 1월 31일에 미국 하원 자원통상위원회(Committee on Energy and Commerce)에 제출되었다. COPDA는 온라인 상의 개인정보의 프라이버시 보호를 목적으로 제안되었으며, 특히 프로파일링을 정면으로 규율하고 있다.

COPDA는 개인정보의 수집, 이용 및 공개와 관련된 불공정사기행위 및 업무의 규제를 규정하면서, 인터넷 프로파일링을 금지하고 있다. 즉, 웹사이트나 온라인 서비스의 관리자는, ① 고지(고지) 시에 프로파일링 업무에 대하여 개인에게 명백하게(clearly) 공개하지 않고 또한 ② 제3자(the third party)가 영구쿠키를 설치하도록 허용하기 위하여 개인에게 사전 동의의 기회(the opportunity to opt-in)를 부여하지 않는다면, 개개인의 인적 프로파일링을 개발하는 수단으로서 제3자가 영구쿠키를 설치하는 것을 허용하지 못하도록 규정하고 있다(Section 2.(2)).

3. NAI 원칙

가. 고지 (Notice)

온라인 프로파일링과 관련된 공정한 정보 업무에 있어서의 핵심적인 문제는 소비자들이 프로파일링되고 있는 중에 얼마나 투명성을 가지느냐 하는 점이다. 이와 관련해서, NAI 원칙은 소비자에게 네트워크 광고사들의 프로파일링 활동과 프로파일링에 참가하지 않을 것을 선택할 권한에 대하여 고지할 것을 정하고 있다.

나. 선택 (Choice)

NAI 원칙은, 네트워크 광고사들의 정보수집업무에 대하여 일단 고지가 이루어지면, 소비자들은 프로파일링에 참가할지의 여부를 결정할 수 있어야 한다고 정하고 있다. 이는 프로파일링으로 인한 유익한 측면과 불이익한 측면에 대하여 판단할 수 있는 권한을 개인 소비자들에게 부여하고자 하는 것이다.

다. 접근 (Access)

공정한 정보업무와 관련된 세 번째 원칙으로서 NAI 원칙은 접근을 천명하고 있다. 즉, 소비자들은 개인식별정보 및 프로파일링을 위하여 네트워크 광고사들이 수집한 개인식별정보와 결합되는 기타 정보에 합리적으로 접근할 수 있어야 한다는 것이다.

라. 보안 (Security)

NAI 원칙은 프로파일링과 관련된 개인정보보호를 위한 원칙으로서 보안을 천명하고 있다. 즉, 네트워크 광고자들은, 소비자들의 개인정보를 보다 효과적으로 보호하기 위하여, 프로파일링을 위하여 수집하는 정보를 보호하기 위한 합리적인 노력을 기울여야 한다는 점이다.

마. 강제 (Enforcement)

NAI 원칙은, 효과적인 자율규제 또는 입법적 구조의 기반은 강제에 있다는 점을 인식하면서, 모든 기업들이 스스로 프로파일링을 통한 개인정보의 침해를 감시하고 NAI 원칙을 담보할 수 있도록 제3자와 공조하도록 천명하고 있다.

바. 부가적인 소비자보호 (Additional Consumer Protections)

NAI 원칙은 전통적인 공정한 정보업무에서 요구되는 원칙들 이외에 추가적

인 소비자보호원칙을 규정하고 있다. 예를 들면, NAI 참가 기업들이 프로파일링을 위하여 민감한 의료 또는 재무 정보, 성적 취향이나 성별, 또는 사회보장번호 등에 대하여 개인식별정보를 이용하지 않을 것을 정하고 있다.

4. 최근의 노력

최근 2012.2. 오바마 대통령은 “네트워크세계에서의 소비자정보프라이버시: 글로벌 디지털경제에서의 프라이버시 보호 및 혁신 촉진을 위한 기본구상”을 발표하면서, 소비자 프라이버시 권리장전(A Consumer Privacy Bill of Rights)을 제시하였다. 이는 개인정보와 관련한 개인의 권리 및 그에 대응하는 기업의 의무를 설정하고자 의도하고 있으며, 개인의 권리는 미국 국내외에서 인정되는 공정한 정보실행원칙을 기초로 한다. 이 권리장전의 적용대상은 개인정보의 상업적 이용이며, 개인정보란 특정 개인과 관련 있는 모든 정보를 의미한다.

이에 의하면 소비자에게 보장되는 권리 중에서 특히, 목적 제한적 수집(focused collection)에 따라 기업은 개인정보를 폐기하지 말아야 할 의무가 없는 이상 개인정보가 더 이상 필요하지 않은 경우 확실히 폐기하거나 비식별 처리하여야 한다고 천명하였다.

아울러 백악관은 소비자프라이버시 강화를 위하여 의회에 입법을 촉구하였는데, 관련 법안으로서 캘리포니아주 하원의원인 Jackie Speier가 2011.2.11. 발의한 온라인추적방지법안(Do Not Track Me Online Act of 2011, H.R. 654)과 2011.4.12. 캘리포니아주 상원의원들이 발의한 온라인 프라이버시권 보호 법안(Commercial Privacy Bill of Rights Act of 2011, S.799)이 있다. 온라인추적방지법안에 의하면, 타겟광고를 위하여 이용되는 온라인 추적으로부터 소비자가 옵트아웃할 수 있도록 규정하고 있다.

Ⅳ. EU

1. 발전과정 및 주요내용

EU는 회원국 국민의 기본권과 자유를 보호하고 개인정보 처리와 관련한 프라이버시권을 보호하며 EU 국가간의 개인정보의 자유로운 유통을 촉진하기 위하여 1995년 10월 24일 “개인 정보의 처리와 자유로운 유통에 관한 개인정보보호지침(Directive of the European Parliament of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC)”을 채택하였다. 이 지침은 회원국에 대한 법률의 제·개정을 강제하고 있으며, 독립된 감독기구의 의무적 설치 및 자국민의 개인정보 보호와 관련하여 EU 수준으로 적절하게 개인정보를 보호하지 않는 국가에 대하여 개인정보의 이전을 금지하고 있다.

1997년 12월 15일의 “정보통신부문의 개인정보 처리와 프라이버시 보호에 관한 지침(Directive of the European Parliament and the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 97/66/EC)”를 채택하여 ISDN(Integrated Services Digital Network)이나 공공디지털이동네트워크(public digital mobile networks)를 통한 정보통신서비스도 적용범위에 포함시키고 있으며 개인정보의 처리와 관련한 기본적 인권과 자유, 특히 프라이버시권의 균등한 보호수준을 보장하고 EU에서의 데이터와 통신설비 및 서비스의 자유로운 이동이 보장되도록 각 회원국 규정들간의 조화를 목적으로 하고 있다.

1999년 2월에는 “정보고속도로에서 신상정보의 수집 처리와 관련한 개인정보 보호 지침(Recommendation No R (99) 5「Guidelines for the protection of individuals in connection with the collection and processing of personal data on information highways」)”을 채택하면서, 인터넷 이용자와 서비스 제공자의 권리와 의무를 규정하고, 특히 서비스 제공자의 의무로써 개인정보를 합법적이며 공정하게 이용하고 데이터의 통합성·기밀성·네트워크의 보안을 보장하며 개인정보의 은밀한 수집, 기록 또는 국가간 전송을 금지하는 것에 대한 책임을 인식하도록 권고하고 있다.

2001년 11월에는 쿠키나 스파이웨어 등과 같은 개인정보의 침해위험을 야기하는 기술적 조치에 대한 규제도 인정하는 “전자통신분야에서의 개인정보 처리와 프라이버시보호에 관한 유럽의회 및 이사회 지침안(the proposal for

a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector)"을 제안·채택하였으며, 이후 논의를 거듭한 끝에 2002년 7월 12일에 최종적으로 "전자통신분야에서의 개인정보처리와 프라이버시 보호에 관한 유럽의회 및 이사회 지침(Directive 2002/58/EC of The European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the eletronic communications sector, 이하 'E-Privacy 지침')"을 채택하였다.

E-Privacy 지침은 전문에서, 전자통신망 이용자의 단말장치 및 그 단말기에 저장된 정보는 유럽인권협약의 보호를 받아야 하는 이용자의 사적인 영역이라고 천명하고 있다. 특히 E-Privacy 지침은 스파이웨어, 웹버그, 숨은 식별자 기타 이와 유사한 장치는 이용자의 단말기에 몰래 설치되어 정보에 접근하거나 정보를 저장할 수 있으며 이용자의 활동을 추적하여 프라이버시를 심각하게 침해할 가능성이 있다는 점을 인식하고 있다. 때문에 이와 같은 장치의 사용은 '당해 이용자가 인지하고 합법적인 목적으로만(only for legitimate purposes, with the knowledge of the users concerned)' 허용되어야 한다고 천명하였다(전문 (24)).

반면, E-Privacy 지침은, 쿠키와 같은 장치는 웹사이트의 디자인 및 광고효과의 분석, 온라인 거래에 참여하는 이용자의 신원 확인 등의 용도에 합법적이며 유용한 수단이 될 수 있다고 전제하면서, 다만, 이용자에게 쿠키 기타 유사 장치가 이용자의 단말장치에 저장되는 것을 '거부할 기회(the opportunity to refuse)'를 부여하여야 한다고 천명하고 있다(전문 (25)). 이 경우에, 이용자의 단말장치에 설치되어 사용될 여러 장치에 대한 정보와 거부권(the right to refuse)은 동일 접속 중 1회만 제공될 수 있으며, 이후의 접속기간 중 그러한 장치를 추가로 사용하는 경우에까지 적용된다고 한다. 다만, 정보제공, 거부권의 제공 또는 동의 요청의 방법은 최대한 사용자에게 편리하여야 한다(전문 (25)).

이러한 기본적인 방침에 기하여, E-Privacy 지침은 다음과 같이 개인정보보호를 위한 규정, 특히 전송정보에 관한 규정을 두고 있다. 이 규정은 프로파일링을 위한 쿠키나 트래킹 소프트웨어에 의한 개인정보의 수집 및 활용에

도 동일하게 적용된다.

공중통신망이나 공개전자통신서비스제공자가 처리·저장하는 가입자 및 이용자에 관한 전송정보는 통신전송을 위하여 더 이상 필요하지 않게 된 시점에는 원칙적으로 삭제되거나 익명으로 처리되어야 한다(제6조 제1항).

공개전자통신서비스제공자는, 전자통신서비스의 마케팅이나 부가서비스의 제공을 목적으로 하는 경우에, 서비스 또는 마케팅에 필요한 한도와 기간 내에 한하여 해당 데이터와 관련된 가입자나 이용자가 동의 하에 해당 정보를 처리할 수 있다(제6조 제3항). 이 경우에 가입자 또는 이용자는 언제든지 전송정보의 처리에 대한 동의를 철회할 수 있어야 한다(제6조 제3항). 또한 동의가 있기 전에는 마케팅이나 부가서비스 제공을 위한 전송정보(traffic data)의 처리 유형 및 기간을 가입자 또는 이용자에게 고지하여야 한다(제6조 제4항).

전송정보의 처리는, 공중통신망 및 공개전자통신서비스제공자의 감독을 받는 자로서 전자통신서비스의 과금 또는 트래픽 관리, 고객 문의, 부정행위 탐지, 전자통신서비스의 마케팅이나 부가가치서비스를 제공하는 자에게 제한되어야 하며 또한 당해 활동의 목적 상 필요한 범위로 제한되어야 한다(제6조 제5항).

최근 2011년 7월 6일에 유럽의회가 “유럽연합에서의 개인정보보호에 관한 종합적 접근”을 의결하면서 개인정보보호에 관한 새로운 입법 필요성을 강조하였다.[70] 그 구체적인 내용은 2012.1.25. EU 일반정보보호규정(안)[71] 및 개인정보보호지침(안)[72]을 발표하면서 드러나게 되었다. EU 차원의 개인정보보호를 위한 입법 노력은 1995년 EU가 개인정보보호지침을 제정한 이후 16년여 만이다. 더욱이 이번 발표에서 주목할 만 한 점은 지침의 전면개정에 머무르지 않고 EU 회원국의 국내에 직접 법적 효과가 발생하는 규정(reg

70) European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union(2011/2025(INI)) 16.

71) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

72) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

ulation)도 함께 추진된다는 점이다. EU 법 체계 하에서 규정은 EU 전체에 직접 적용되는 매우 강력한 규범이고, 규정이 발효되면 회원국의 국내법에 우선하여 적용된다. 따라서 회원국은 국내법을 EU 규정에 일치시키는 입법을 하거나 기존 법을 개정하여야 한다. 다만, 개정안이 발효되려면 27개 회원국 정부 대표로 구성된 이사회와 유럽의회의 승인을 받아야 한다. 이번 입법안은 2014년 발효를 목표로 하고 있다.

EU의 일반정보보호규정(안) 및 개인정보보호지침(안)의 주요 개선 방향 및 내용은 다음과 같다.[73] (1) EU 전체에 유효한 단일 규범을 정립하였다는 점이다. 또한 기업의 신고의무와 같이 불필요한 행정적 규제를 제거하기 위하여 노력했다. 이를 통하여 매년 23억 유로의 비용을 절약할 수 있게 된다. (2) 모든 정보보호활동을 감독기관에 신고하도록 한 현재의 기업 의무 대신에 새로운 규정(안)은 개인정보를 처리하는 기업들에게 증진된 책임성을 규정하고 있다. 기존의 의무로 인하여 기업들에게 불필요한 서류작업과 매년 1억3천만 유로의 비용을 발생시켰다. 이를 개선하여, 예를 들면, 기업이나 기관은 심각한 개인정보 침해가 발생한 경우에 지체 없이(24시간 내에 가능하다면) 국내 감독기관에게 신고하여야 한다. (3) 기관은 그 기관의 주된 기반을 가지고 있는 EU 국가 내의 단일한 국내 정보보호 감독기관과만 업무를 수행하면 된다. (4) 마찬가지로 개인들도 그 국가 내에서 정보보호기관에게 도움을 요청하면 된다. 심지어는 그들의 정보가 EU 외부에 기반을 둔 기업에 의하여 처리되는 때에도 마찬가지이다. 동의가 정보처리를 위하여 요구되는 경우에는 추정보다는 명시적으로 이루어져야 한다. (5) 개인들은 그들 자신의 정보에 더 쉽게 접근할 수 있어야 하고, 서비스제공자들 사이에서 개인정보를 이전할 수 있도록 해야 한다. 이를 통하여 서비스 사이의 경쟁을 증진시킬 수 있을 것이다. (6) '잊혀질 권리'를 통하여 온라인 상의 정보보호위험을 더 잘 관리할 수 있도록 하고자 하였다. 개인정보를 보유할 합법적인 근거가 없는 한 개인은 그들의 정보를 삭제할 수 있다. (7) EU 규칙들은 EU 시장에서 활동 중이고 EU 시민들에게 그들의 서비스를 제공하는 기업에 의하여 해외에서 처리되는 개인정보에도 적용되어야 한다. (8) 독립적인 국

73) EU의 최근 입법동향에 대하여는 최경진, 잊혀질 권리 - 개인정보 관점에서, 정보법학 제16권제2호(2012), 103면 이하 참조.

내 개인정보 보호 기관을 강화하여 역내에서 EU 규정을 강화할 수 있을 것이다. 특히, EU 정보보호규정을 위반한 회사에게 벌금을 과하도록 강화하였다. 예를 들면, 기업의 연간 총매출액의 2% 또는 1백만유로까지 과징금을 부과할 수 있도록 하였다. (9) 새로운 지침(안)은 형사사건에서 경찰 및 사법 공조를 위하여 일반정보보호원칙 및 규칙을 적용할 것이다. 그 규칙은 정보의 국내 및 국가간 이동에도 적용된다.

2. 프로파일링 관련 법제

새로운 EU 규정(안)에는 빅데이터와 관련하여 특별히 프로파일링과 관련된 규정을 두고 있다. 즉 제20조제1항에 의하면, 개인적 특성의 평가, 개인에 관한 분석 또는 예측을 위한 기준의 적용을 받지 않을 권리를 보장함으로써 자연인에 대한 프로파일링 거부권을 선언적으로 규정하고 있다. 다만, 정보주체의 적법한 이익을 보호해주는 적합한 기준이 제공되거나 정보주체에 의한 계약 체결 또는 이행의 요청이 충족되는 경우에 계약 체결 또는 이행 과정에서 처리되는 경우, 정보주체의 합법적 이익을 보장하기에 적합한 기준을 규정한 EU 또는 회원국의 법률에 의하여 명시적으로 승인되어 처리되는 경우, 제7조의 동의요건과 적합한 보호조치 하에서 정보주체의 동의 하에 처리되는 경우에는 프로파일링이 예외적으로 허용된다. 이러한 프로파일링 거부권 선언과 함께 규정(안)은 자연인과 관련된 일정한 인적 특성을 평가하기 위한 자동화된 처리는 개인정보의 특정 범주에만 의존하지 말아야 한다고 하여 자동화된 처리의 제한을 규정하였다. 동시에 프로파일링 처리방식 및 정보주체에 대한 처리로 인하여 예상되는 효과에 대한 정보를 제공받을 권리를 보장하기 위하여 이러한 사항을 고지할 의무로서 규정하였다. 이러한 프로파일링과 관련된 구체적인 사항에 관하여는 EU 집행위원회가 구체적인 입법권한 부여받았다.

3. 국외이전 관련 법제[74)]

74) 국외이전 관련 EU를 비롯한 영국 등의 법제현황에 대하여는 한국인터넷진흥원, 개인정보 국외이전 관련 법률정비 방안 연구(2012.11.) 및 최경진, “개인정보 국외이전에 관한 합리적인 법제 개선방안”, 개인정보보호 법제정비 연구포럼 토론회(201212.7.) 자료집, 55-75 참조.

가. EU 개인정보보호지침

EU 개인정보보호지침 전문 제57항[75]과 제25조 제1항[76]에 따르면, EU 회원국 국민의 개인정보를 '적절한 수준'의 보호를 보장하지 않는 경우에는 제3국[77]으로 이전할 수 없도록 하고 있다. 따라서 개인정보에 대해서 적절한 수준의 보호를 하는 경우에 한해서 이전할 수 있게 된다. EU지침 제25조 제2항에 따르면 보호의 '적절성'(Angemessenheit)은 제3국으로 정보 이전 활동과 관련된 주변 사정에 비추어 판단되어야 하며 개인정보의 성격, 개인정보의 처리 목적과 기간, 개인정보의 최초 이전국과 최종 도착국, 제3국에서 시행되고 있는 법률규범·직무규정 및 보안조치 등 개인정보 이전을 둘러싼 모든 환경이 고려되어야 한다.[78] 하지만 개인정보 보호 수준이 낮은 제3국으로의 개인정보 이전이 무조건 금지되는 것은 아니며, 일정한 경우에는 예외적으로 개인정보보호수준이 EU의 수준에 미치지 못하더라도 제3국으로의 개인정보이전이 허용된다.[79] 즉, ① 정보주체가 개인정보 이전에 명백히 동의한 경우, ② 정보주체와 개인정보처리자 사이에 체결된 계약의 이행에 필요한 개인정보의 이전 또는 정보주체의 요청에 따른 계약 체결전 조치를 이행하기 위하여 필요한 개인정보의 이전, ③ 개인정보처리자와 제3자

---

75) RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr(이하 : Richtlinie 95/46/EG)

(57) Bietet hingegen ein Drittland kein angemessenes Schutzniveau, so ist die Übermittlung personenbezogener Daten in dieses Land zu untersagen.

76) Richtlinie 95/46/EG Art. 25

(1) Die Mitgliedstaaten sehen vor, daß die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

77) 이하에서 말하는 제3국이란 유럽경제영역(European Economic Area : EEA) 회원국을 제외한 그 밖의 국가를 의미한다. EEA는 EFTA와 EU회원국들이 EEA협정(Agreement on the European Economic Area)에 합의함으로써 성립(Jan.1, 1994)하였다. EEA는 회원국간 4가지 자유(상품, 서비스, 사람, 자본의 자유이동)를 근간으로 하며, 이러한 법적 배경을 근거로 EEA 회원국간 정보이동은 제3자로의 이동으로 간주하지 않으므로 금지대상이 되지 않는다.

78) 이광현, 국경간 개인정보 이전과 보호 : EU와 영국, 미국의 사례를 중심으로, 선진상사법률연구, 제50호, 2010. 120면; 한국인터넷법학회, 개인정보 보호와 적정 활용의 조화를 위한 제도 도입 연구, 법제처, 2009, 143면.

79) Richtlinie 95/46/EG Art. 26(1)

사이에 정보주체의 이익을 위한 계약의 체결 또는 이행을 위하여 필요한 개인정보의 이전, ④ 중요한 공익적 근거에 기초하거나 소송의 제기, 수행 및 방어를 위하여 필요하거나 법적으로 요구되는 개인정보의 이전, ⑤ 정보주체의 중대한 이익 보호를 위하여 필요한 개인정보의 이전, ⑥ 개별 사안에 있어서 법률적인 조건이 충족되는 범위 내에서 공중에게 정보를 제공할 목적으로 구축되었고 동시에 공중이나 이해관계자의 상담(consultation)에 제공될 목적으로 구축된 등록부(Register)로부터 개인정보가 이전되는 경우 등이 이에 해당된다. 또한 열거된 요건에 해당하지 않는다고 하더라도 개인정보처리자가 개인의 프라이버시와 자유권 그밖에 이에 준하는 권리의 보호와 행사를 위해 적절한 보호조건을 제시한 경우, 회원국은 제3국의 개인정보 보호수준이 EU 수준에 미치지 못한 경우에도 제3국으로 개인정보 이전을 승인할 수 있다. 이 경우 개인정보처리자가 이행해야 할 개인정보의 보호조건은 계약에 의해서 보증하는 것도 가능하다.[80]

회원국과 유럽위원회는 제3국의 개인정보 보호수준이 적정수준에 이르지 못한다고 판단되는 경우에는 그 사실을 다른 회원국에게 알려야 한다. 위원회는 보호수준을 높이기 위해 제3국과 협상을 추진할 수 있으며, 또한 제3[81]국의 국내법, 제3국이 체결한 국제조약, 위원회와의 협상결과 등을 고려하여 제3국이 적절한 보호수준을 보장하고 있다고 인정할 수 있다.[82]

EU 개인정보보호지침 상의 적절성 평가기준은 최소한의 기준으로 실체적 측면과 절차적 측면으로 구분된다. 실체적 측면에서는 1. 목적제한의 원칙, 2. 정보의 질 확보 및 비례성 원칙, 3. 투명성 원칙, 4. 안전성 원칙, 5. 열람·정정 및 반대할 권리, 6. 개인정보의 제공 제한 등 기본원칙을 충족시켜야 하며, 추가적으로 민감정보 처리제한, 다이렉트마케팅 제한, 개인에 대한 자동화된 결정의 제한이 충족되어야 한다.

절차적 측면에서는 보호원칙을 효과적으로 적용하고 집행할 수 있도록 하는 절차적 수단(매커니즘)이 확보되어야 한다. 즉, EU에서는 독립기구 형태의 '외부적 감독' 시스템이 개인정보보호 컴플라이언스 체계를 위한 필수적 특

80) Richtlinie 95/46/EG Art. 26(2)

81) 인터넷법학회, 전게문헌, 144면.

82) Richtlinie 95/46/EG Art. 25(3)~(6)

징이라는 광범위한 합의가 이루어져 있으나, 전 세계의 다른 국가들은 그렇지 않은 경우도 많다. 따라서 제3국의 보호수준을 평가할 때에는 개인정보보호체계의 근본 목적과 각국의 다양한 사법체계를 함께 고려해야 한다. 이 때 개인정보보호체계의 핵심은 다음 세 가지가 기본이 되어야 한다. 즉, 보호원칙이 잘 준수되는 체계의 확보(good level of compliance) 여부, 정보주체의 권리행사를 지원하고 도와주는 보호체계(support and help to individual data subjects)의 여부, 보호원칙 미준수로 피해를 입은 자에 대한 적절한 구제조치 (appropriate redress) 여부이다.

나. 2012년 일반정보보호규정(안)

2012년 일반정보보호규정(안)[83]에서는 보다 구체적으로 개인정보의 역외이전에 대하여 규정하고 있다. 즉, 제5장(제40조에서 제45조)에서 제3국 및 외국 기관으로의 개인정보 이전을 규정하고 있다.
2012년 일반정보보호규정안 제40조는 이전을 위한 일반 원칙을 규정하고 있다. 즉, 제3국이나 국제 기관에서 다른 제3국이나 다른 국제 기관으로의 향후 이전을 포함하여, 제3국이나 국제 기관으로 이전된 후 처리되고 있거나 처리될 예정인 개인정보의 이전은 본 규정(안)에서의 다른 조항과 함께 본 장에서 규정된 요건을 개인정보처리자가 충족하는 경우에 가능하다.

먼저 2012년 일반정보보호규정안 제41조는 적법성 결정에 따른 이전을 규정한다. 즉, EU 집행위원회가 제3국, 제3국의 영토 또는 처리 부문, 국제 기관 등이 적절한 수준의 보호를 보증하고 있다고 판단하는 경우 이전이 가능하다. 이러한 이전에 추가 승인이 필요하지는 않다. 이처럼 EU집행위원회가 보호 수준의 적절성을 평가할 때에는 다음 요소에 대해 고려해야 한다. 즉, (a) 법률 규정, 일반적으로 또는 부문별로 시행 중인 공공의 안녕, 국방, 국가 안보, 형법 등과 관련된 것을 포함한 관련 법률, 해당 국가 또는 해당 국

83) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

제 기관에서 준수해야 하는 관련 법률 및 보안 조치, 정보주체, 특히 개인정보가 이전되는 유럽연합에 거주하는 정보주체에 대한 효과적인 행정 및 사법적 시정을 포함한 효과적이고도 실행 가능한 권리, (b) 정보 보호 규정의 준수, 권리 행사하는 정보주체에 대한 지원 및 통지, 유럽연합 및 회원국 감독기관과의 협력 등에 책임이 있는 하나 이상의 제3국의 독립적인 감독기관이나 해당되는 국제 기관의 존재 및 효율적 역할, (c) 해당되는 제3국이나 국제 기관이 체결한 국제 협약을 고려하여야 한다.
EU집행위원회는 제3국 또는 제3국의 영토나 처리 지역 또는 국제 기관이 적절한 수준의 보호를 보증하지 않는지 여부를 결정할 수 있으며, 정보주체, 특히 개인정보가 이전되는 유럽연합에 거주하는 정보주체를 위한 효과적인 행정 및 사법적 시정 조치를 포함하여, 제3국이나 국제 기관에서 일반적 또는 부문별로 시행 중인 적절한 법률이 효과적이고 집행 가능한 권리를 보호하지 않는지 여부를 결정할 수 있다. 그 나라의 이행 법안은 제87조 (2)항에서 규정한 평가절차에 따라 채택되거나, 개인정보 보호에 대한 권리와 관련하여 긴급한 경우에는 제87조 (3)항에서 규정한 절차에 따라 채택되어야 한다.

2012년 일반정보보호규정(안) 제42조는 적절한 안전장치가 보장되는 경우의 역외이전을 규정하고 있다. 즉, 집행위원회가 제41조에서 언급한 결정을 하지 않는 경우, 개인정보처리자가 법률적으로 구속력을 가진 방법을 통해 개인정보의 보호에 대한 적절한 안전 조치를 제시하는 경우에만 개인정보처리자가 개인정보를 제3국이나 국제 기관으로 이전할 수 있다. 이 때 적절한 안전조치란 (a) 제43조에 따른 구속력 있는 기업규칙, (b) 집행위원회가 채택한 표준 정보 보호 조항, (c) 제62조 (1)항의 (b)에 따라 집행위원회가 유효하다고 인정하는 경우, 제57조에서 규정한 준수체계(consistency mechanism)에 따라 감독기관이 채택한 표준 정보 보호 조항, (d) 제4항에 따라 감독기관이 승인한 개인정보처리자와 정보 수령인 사이의 계약 조항을 말한다. 이 중 (a), (b), (c)의 표준 정보 보호 조항이나 구속력 있는 기업규칙에 기초한 이전의 경우 추가 승인이 필요하지 않다. 반면, 이전이 (d)의 계약 조항에 기초하는 경우, 개인정보처리자는 제34조 (1)항의 (a)에 따라 감

독기관으로부터 계약 조항에 대해 사전 승인을 받아야 한다. 역외이전이 상대방 회원국이나 다른 회원국에 거주하는 정보주체와 연관된 처리 활동과 관련되거나 유럽연합 내에서 개인정보의 자유로운 이전에 큰 영향을 미치는 경우, 감독기관은 제57조에서 규정된 준수체계를 적용해야 한다.

개인정보의 보호와 관련된 적절한 안전 조치가 법률적으로 구속력이 있는 방법으로 제공되지 않는 경우, 개인정보처리자는 이전에 대한 이유를 제시하면서 이전 또는 일련의 이전에 대한 또는 행정 협정에 이러한 규정을 포함시키는 것에 대한 사전 승인을 받아야 한다. 감독기관의 이러한 사전 승인은 제34조 (1)항의 (a)에 따라 이루어져야 한다. 개인정보의 역외 이전이 상대방 회원국이나 다른 회원국에 거주하는 정보주체와 연관된 처리 활동과 관련되거나 유럽연합 내에서 개인정보의 자유로운 이전에 큰 영향을 미치는 경우, 감독기관은 제57조에서 언급한 일관성 보장 장치를 적용해야 한다. 1995년 개인정보보호지침의 제26조 (2)항에 기초하여 집행위원회가 결정한 승인은 집행위원회가 수정, 교체, 폐기할 때까지 계속 유효하다.

2012년 일반정보보호규정(안) 제43조는 구속력 있는 기업규칙(BCRs)에 의한 이전을 규정한다. 즉, 구속력 있는 기업규칙이 (a) 법적으로 구속력 있고, 관리자 또는 처리자의 사업체 집단 내의 피고용인을 포함한 모든 구성원에게 적용되고 이들에 의해 시행되며, (b) 정보주체에 대해 실행 가능한 권리를 명시적으로 부여하고, (c) 제2항에서 언급한 요건을 충족하는 경우에 감독기관은 제58조에서 언급한 준수체계에 따라 이를 승인해야 한다.

이상의 경우에 해당하지 않는 경우에 제3국이나 국제 기관으로의 개인정보 이전 또는 일련의 이전은 다음의 조건을 충족하는 경우에만 가능하다. 즉, (a) 정보주체가 정당한 결정이나 적절한 안전 조치의 부재로 인해 발생할 수 있는 이전의 위험에 대해 통지를 받은 후 제안된 이전에 동의하는 경우, (b) 정보주체와 개인정보처리자 사이에서의 계약 이행을 위해 또는 정보주체의 요청에 의해 취해진 계약 전 사전 조치의 이행을 위해 이전을 해야 하는 경우, (c) 정보주체의 이익을 위해 개인정보처리자와 다른 자연인 또는 법인

사이에서 체결된 계약의 이행을 위해 이전을 해야 하는 경우, (d) 공공의 이익을 위해 이전이 필요한 경우, (e) 법률 소송의 구성, 행사, 방어를 위해 이전이 필요한 경우, (f) 정보주체가 물리적으로 또는 법률적으로 동의를 할 수 없는 경우, 정보주체 또는 다른 사람의 주요한 이익을 보호하기 위해 이전이 필요한 경우, (g) 유럽연합이나 회원국 법률에 따라 일반 대중에 정보를 제공하기 위해 그리고 일반 대중 또는 정당한 이익을 입증할 수 있는 사람에 의한 협의를 위해 유럽연합이나 회원국 법률에서 규정한 조건이 충족되는 한도 내에서 공개되는 등록부(register)로부터 이전되는 경우, (h) 개인정보처리자가 정보 또는 일련의 정보 이전 공정과 관련된 모든 상황을 평가하고 이러한 평가에 기초하여 개인정보의 보호를 위해 적절한 안전 조치를 제시하는 경우로서 개인정보처리자가 추구하는 정당한 이익의 목적을 위해 이전되는 경우에는 역외이전이 허용된다.

Ⅴ. 일본

일본은 공공부문에서는 “행정기관이 보유한 개인정보에 관한 법률”(行政機關の保有する個人情報の保護に關する法律)이, 민간 부문에서는 2003. 5. 30. 제정된 “개인정보의 보호에 관한 법률”(個人情報の保護うに關する法律)이 각각 시행되고 있다. 민간부문에서 시행되는 개인정보의 보호에 관한 법률에서는 개인정보의 국외이전에 특별한 별도의 규정을 두고 있지 않으며, 일본 국외로 이전하는 것이 성격이 제3자 제공에 해당한다면, 본래 그 성격에 따라 사전 동의가 요구될 뿐이다[84]. 또한 빅데이터의 핵심 요소인 프로파일링에 대하여도 별도의 고려를 하고 있지 않다.

Ⅵ. ICDPPC

최근 우리나라의 개인정보보호위원회가 방송통신위원회 산하의 한국인터넷진흥원에 이어 국제개인정보보호회의(ICDPPC)에 정회원으로 가입하였다. ICDPPC는 영국·프랑스·독일·캐나다 등 54개국 87개 기관이 참여하는 개인정

84) http://uk.practicallaw.com/5-520-1289?source=relatedcontent#a629036 참조

보보호 국제회의체이다. 매년 국제적으로 부각되는 개인정보보호 관련 이슈에 대해 공동으로 해결책을 모색하고 있다. 최근 2012. 10. 25. ~ 10. 26. 우루과이에서 개최된 ICDPPC 회의에서는 최신 서비스와 기술로부터 문제되고 있는 소위 '빅데이터'와 관련된 개인정보보호의 문제에 대한 합의를 도출하고자 하였다. 이를 통하여 빅데이터에서 가장 문제가 되는 프로파일링에 대한 법적 측면에서의 고려사항을 도출하고자 시도하였다. 즉, (1) 프로파일링에 대한 고지, (2) 프로파일링 단계별 구분, (3) 프로파일링 결과에 대한 통제, (4) 자동화된 프로파일링의 제한, (5) 프로파일링 생성과 적용 사이의 균형, (6) 프로파일링에 대한 거부권, (7) 프로파일링에 대한 독립적인 감독기관, (8) 독립적인 프라이버시 감독기관에게 정부의 입법권한에 대한 견제권한 부여 등이 2012 우루과이 선언에 포함되었다.

제4장 빅데이터에 적합한 개인정보 보호법의 개선방안

Ⅰ. 빅데이터 환경의 개인정보보호를 위한 법제적 분석

1. 빅 데이터와 개인정보

빅 데이터 시대는 정보화기술과 매체간의 융합기술 등이, 고인이 된 스티브 잡스의 표현을 빌리자면, “혁신적인 진화(Innovation Darwinism)”를 거듭하여 인간의 상상력이 공상과학의 차원을 벗어나 기술적으로 구현되는 시대로 특징지워질 수 있다. 이러한 사회에서는 전자식별장치(RFID)를 통해 인간과 동·식물을 비롯한 모든 물건과도 전자적인 소통을 가능하게 하는 IT기술 - 특히, 사람이 읽고 해석하기에 편리하게 설계되어 있는 현재의 웹 대신에 컴퓨터가 이해할 수 있는 형태의 새로운 언어로 표현해 기계들끼리 서로 의사소통을 할 수 있는 지능형 웹을 의미하는 시멘틱 웹의 개발 등[85] - 과 위치정보기술(GPS) 및 네트워킹 CCTV 등의 결합에 힘입어 언제·어디에서나 개인이나 국가 또는 사회의 다양한 수요를 실시간으로 충족할 수 있는 “매듭없이 깔끔하게 전자적으로 소통되는 사회”(seamless networking society) 내지 “유비쿼터스사회”(Ubiqutous society)[86]로서 개별법령이나 정보주체와의 계약 등 합법적으로 정해진 범위에서든, 법령의 미비에 의하든, 접근권한이 있는 자 또는 접근권한이 없는 자에 의하든 불법적이거나 정보주체의 인식범위를 초과하는 개인정보의 오·남용으로부터 자유로울 수 없는 소위 “사

85) 현재의 컴퓨터처럼 사람이 마우스나 키보드를 이용해 원하는 정보를 찾아 눈으로 보고 이해하는 웹이 아니라, 컴퓨터가 이해할 수 있는 웹으로서, 컴퓨터 스스로가 정보자원의 의미를 해석하고, 컴퓨터나 저장매체간 서로 정보를 주고받으면서 자체적으로 필요한 일을 처리하는 것을 가능하게 한다. 2004년 현재 시멘틱 웹과 관련된 연구는 RDF(Resource Description Framework)를 기반으로 한 온톨로지 기술과 국제표준화기구(ISO) 중심의 토픽 맵(Topic Map) 기술이 주류를 이루고 있다. http://100.naver.com/100.nhn?docid= 780515 <2008.8.1. 접속>. 특히 토픽맵은 정보를 상호연관성에 따라 연결하고 조직하여 지식구조를 일종의 지도와 같이 표현하여 대용량의 정보를 분류하고 의미론적 연관관계를 검색하는데 사용할 수 있는 탁월한 기술로서 정보세계의 GPS로 평가되고 있다. http://ko.wikipedia.org/wiki/%ED%86%A0%ED%94%BD%EB% A7%B5 <2010. 7.21. 접속>

86) USN사회로 진입하게 됨에 따라 “인간의 요구사항을 고도로 적용하는 환경”, “모든 이에게 가장 기본적인 서비스제공", "어떤 컨텐츠, 기기, 포맷이라도 언제나 접속가능한 환경” 및 “스팸, 정크메일, 해킹, 바이러스 등이 존재할 수 없는 환경(Digital Dystopia)” 등 4대 미래 인터넷 시나리오가 제시되기도 한다. Smart Internet Technology CRC, "Smart Internet 2010", 2005. 9.(한국전산원, “통계로 본 2010년 유비쿼터스사회 조망”, 2005.9.30. 5쪽에서 재인용).

생활이 없는 사회"(Zero Privacy Society)[87]의 두려움[88] 속에 생활할 수밖에 없는 상태에 놓이게 되었다.

그렇기 때문에, 헌법 제119조제1항에 근거하여 시장의 자율과 창의를 바탕으로 이윤극대화를 추구하는 정보통신서비스제공자에 대하여는 개인정보가 갖는 인격적 가치의 보호를 기대하기 보다는 경제적 가치에 보다 중점을 두고, 그 경제적 가치를 극대화하기 위해 개인의 전자적 흔적에 대한 망라적인 수집·통합에 기초한 개인화작업에 그치지 않고 예측프로그램을 통해 현재와 장래의 개인별 맞춤식 검색·광고와 서비스를 수행할 것으로 기대하는 것이 보다 현실적이라고 할 것이다.[89]

특히, 다수 이용자의 검색 내지 방문을 배경으로 기업을 상대로 다양한 수익모델을 추구하고 있는 소위 빅 데이터 기업인 "구글", "페이스 북"이나 "트위터" 등은 보다 많은 수익창출을 목적으로 새로운 서비스와의 융합을 도모하면 할수록 위와 같은 경향을 지속적으로 시도할 수밖에 없고, 그 결과 개인에 의한 자율적인 인격형성이나 사적 영역은 더 이상 존재하지 아니하게 되고, 빅 데이터 기술에 의하여 정보주체가 인식하지도 못하는 상태에서 빅 데이터 기술적용의 목적방향에 따라 개인의 모습이 임의적으로 형성(상업적 표현)될 수 있는 위험이 점증하고 있다.

2. 개인정보의 보호법익

현행 「개인정보 보호법」 "개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호…"함을 목적으로 한다고 규정할 뿐, 일본의 「個人情報保

87) "현대 고도정보사회에 있어서는 사생활에 대해 조의를 표하여야 하며, 카메라나 데이터베이스의 침해를 방지하기엔 너무 늦었다. 이미 쏟아진 물이다. 아무리 많은 입법이 행하여진다고 하더라도 입법으로 새로운 감시도구와 데이터 베이스를 제거할 수는 없다"고 한다. D.J. Solove, Marc Rotenberg, "Information Privacy Law", Aspen. 2002. p.507.

88) 바람난 남편이나 가출한 자녀를 찾기 위해 이들이 조난을 당했다고 허위로 신고할 경우 GPS를 작동해 이들의 위치를 파악하는 것이 개인 프라이버시 문제와 어떻게 상충될지 등에 대한 연구가 필요할 뿐 아니라 정치인이나 저명인사의 동선이 파악돼 엉뚱한 용도로 악용될 가능성에 대한 우려의 시각도 있다. 졸고, "位置認識 및 通信事實確認資料 등의 個人情報與否에 관한 小考", 토지공법연구 제24집, 2004.12. 494쪽.

89) 페이스북 창업자 마크 주커버그는 2010년. 12. 8. "지금 다시 페이스북을 만든다면 소수의 친구에게만 허용하는 개인정보를 '모두에 공개'를 기본으로 설계할 것"이라며 "지난 몇 년간 (사생활 공개에 대한) 사회적 기준이 바뀐 만큼 이를 반영해야 할 것"이라고 말했다. "나를 잊어줘 …온라인에 노출된 사생활 흔적 지워라", http://www.hani.co.kr/arti/economy/it/398376.html <2011. 3. 5. 접속>

護法」제3조와 같이 "개인정보는 개인의 인격존중의 이념 하에 신중하게 취급되어야 한다"는 취지의 규정을 두고 있지 않아 개인정보를 보호하는 법익이 무엇인가에 대하여 논란이 있을 수 있다. 즉, 인격의 존중 이념이 지향하는바 포괄적인 권리로서 인격권 보호인지, 아니면 통신의 비밀을 포함하는 개인 사생활 비밀권의 보장을 그 내용으로 하는 것인지에 관하여 다툼이 있을 수 있으나 개인 사생활의 비밀을 보장한다는 것은 정보처리자의 일방적인 프로파일링이나 데이터 마이닝에 의한 개인형성으로서 개인의 인격에 대한 왜곡가능성 내지 제3자에 의해 이루어질 수 있는 정보주체가 원하지 않거나 정보주체가 허용한 범위를 넘어선 개인화로부터 개인인격의 보호를 포함한 것으로 보아야 할 것이다.

1) 헌법적 관점

우리 헌법이 개인정보의 보호와 관련하여 명문으로 규정하고 있지는 않지만 헌법상 보호되고 있는 것임은 일반적으로 시인되고 있다.[90] 다만, 그 근거에 대하여는 인간의 존엄과 가치를 규정한 헌법 제10조에서 찾는 입장, 사생활의 비밀과 자유를 규정한 헌법 제17조에서 찾는 입장 및 헌법 제17조와 주거의 자유를 규정한 헌법 제16조 및 통신의 자유를 규정한 헌법 제18조도 보충적으로 기능하다는 입장 등으로 갈라지나 어떠한 입장에 의하더라도 인간의 존엄을 구성하는 요인으로서의 개인정보의 보호는 상태권으로서의 침해방지라는 소극적 방어권으로서의 성질뿐만 아니라 자신에 관한 개인정보에 대한 인격적 지배권[91]이라는 점에서 열람·정정·차단·삭제를 요구할 수 있는 행위권 내지 적극적 요구권의 성질을 보유하고 있는 점에는 이론이 없

90) 권녕성, 헌법학원론, 법문사, 2007, 429쪽; 김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 공법연구, 제29집제3호, 88쪽; 이인호, "정보사회와 개인정보자기결정권", 중앙법학 창간호, 1999, 79쪽.

91) 이와 관련하여 "매연, 소음, 진동 등에 의한 생활방해나 일조, 통풍, 정온, 조망 등 주거환경의 침해는 토지소유권의 침해의 범주에 넣어 볼 수 있지만, 그 주된 피해법익은 인간의 건강하고 쾌적한 생활이익으로서 이러한 주거환경의 이익은 그 법익의 법적 성격으로 보아 종래의 생명·신체·자유·명예·정조·초상권·신용권 등과 같이 인격권의 일 중에 속한다고 보아야 하고 이러한 인격권은 그 지배권 내지 절대권적 성격으로부터 물권적 청구권에 준하는 방해배제청구권이 인정되고 있으므로, 생활방해나 주거환경의 침해는 실질적으로는 신체적 자유 내지 정신적 자유의 침해에 속하는 것이고, 이 경우 일정한 한도를 초과하는 침해에 대하여는 방해배제청구권이 인정되는 토지소유권 기타 물권을 가지고 있지 않는 자라고 하더라도 막바로 인격권의 침해를 이유로 인격권에 터잡아 방해배제 또는 방해예방청구권을 행사할 수 있다고 봄이 상당하다"(부산고법 1995. 5. 18. 선고 95카합5 판결)는 판결에 주목할 필요가 있다.

다.[92] 요컨대, 우리 헌법 제10조는 "모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다"라고 규정하고 있고, 헌법 제17조는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니 한다"라고 규정하고 있는 정에 비추어 개인은 자신에 관한 정보를 스스로 관리 통제할 수 있는 적극적인 권리 등을 내용으로 하는 헌법상 기본권에 해당하는 포괄적 인격권으로서 자기정보통제권을 가진다고 할 수 있다.

2) 법률적 관점

「개인정보 보호법」제2조제1항은 "정보주체를 식별할 수 있거나 다른 정보와 쉽게 결합하여 알아 볼 수 있는 개인에 관한 정보"를 개인정보로 정의한 다음 국가행정기관 지방자치단체 그 밖의 공공단체 중 대통령령이 정하는 기관과 사인 등 모든 개인정보처리자를 수범자로 하여 이들에 대해 개인정보처리 목적에 필요한 최소한의 개인정보수집과 처리 및 활용의 원칙과 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장 등 개인정보 보호원칙을 규정함(제3조)과 아울러 최소한 개인정보 수집원칙과 서비스제공 거부금지원칙(제16조), 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지의무(제20조), 목적달성시의 개인정보파일의 파기원칙(제21조) 및 민감정보의 처리제한원칙(제23조)을 비롯하여 정보주체의 처리정보에 대한 열람·정정·삭제·처리정지권 등(제35조 내지 제37조)을 보장하고 있다.

개인정보보호에 관한 일반법인 위 법률은 식별할 수 있는 개인에 관한 정보의 보호를 목적으로 하연서 이용자 내지 정보주체의 권리로서 개인정보 내지 개인데이터의 열람정정 삭제청구권 등을 인정하여 제3자에 의해 개인의 모습이 자의적으로 형성될 위험으로부터 정보주체를 보호할 수 있도록 하는 소위 포괄적 인격권으로서 정보자기결정권(정보통제권)을 보장하고 있음을 알 수 있다.

3) 판례

판례는 사생활의 비밀과 자유 및 초상권 등을 헌법 제10조에 의한 인격권으

92) 한위수, "사생활비밀의 보호 - 그 공법적 측면"(한국법학원 2003. 12. 8. 개최 심포지엄, "사생활비밀의 보호" 발표논문), 16쪽.

로 파악하고 있다. 즉, 헌법 제10조에서 국가가 보장하여야 할 인간으로서의 존엄과 가치는 생명권, 명예권, 성명권 동을 포괄하는 일반적 인격권을 의미하고, 이 일반적 인격권에는 개별적인 인격권으로서의 초상권이 포함된다[93]는 것으로 이러한 입장은 "헌법 제10조와 헌법 제17조는 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하는 데에 그 취지가 있는 것으로 해석된다"[94]고 한 것이나 "사람은 누구나 자신의 얼굴 기타 사회통념상 특정인임을 식별할 수 있는 신체적 특정에 관하여 함부로 촬영 또는 그림으로 묘사되거나 공표되지 아니하며 영리적으로 이용당하지 않을 권리를 가지는데, 이러한 초상권은 우리 헌법 제10조 제1문에 의하여 헌법적으로 보장되는 권리이다"는 대법원의 판결[95]에 의해 재확인되고 있다.

아울러 판례는 개인의 인격을 형성하는 개인의 성명이나 초상 등에 대한 퍼블리시티권(Right of Publicity)을 부인하던 입장[96]에서 벗어나 하급심의 입장이기는 하지만, "헌법상의 행복추구권과 인격권의 한 내용을 이루는 성명권은 … 인격으로부터 파생된 것이기는 하나 독립한 경제적 이익 또는 가치에 관한 것인 이상 인격권과는 독립된 별개의 재산권으로 보아야 할 것이다"[97]고 하여 식별정보로서 개인정보에 대해 재산권의 성질을 인정하고 있다.[98]

4) 학설

학자에 따라서는 고도지식정보사회에 있어서 '모든 권리 가운데에서 가장 포괄적이고 문명인에게 가장 가치가 있다고 하는 권리가 있다면, 그것이 바로 프라이버시권[99]이다"[100]고 하거나, 전자 네트워크 시대의 프라이버시를 ①

93) 서울지법 남부지원 1997. 8. 7. 선고 97가합8022 판결 : 항소기각 확정.

94) 대법원 1998. 7. 24. 선고 96다42789 판결.

95) 대법원 2006. 10. 13. 선고 2004다16280 판결.

96) 서울고법 2002. 4. 16. 선고 2000나42061 판결취하.

97) 서울중앙지방법원 2006. 4. 19. 선고 2005가합80450 판결(항소) ; 같은 취지, 서울중앙지방법원 2005. 9. 27. 선고 2004가단235324 판결.

98) 일본 판례도 프라이버시권을 "성명・초상이 갖는 독립된 재산적 가치를 적극적으로 활용하기 위해 제3자에 대하여 대가를 받고서 정보전달에 사용하는 것을 승락하는 권리"로 판시하고 있다. 光GENJI事件, 東京地判 1989. 9. 27 判例時報 1326・137.

개인의 인격에 관한 프라이버시, ②개인데이터의 프라이버시, ③개인의 통신 프라이버시, ④익명성의 4가지로 유형화하기도 한다.[101]

또는 "우리 헌법 제17조의 사생활의 비밀과 자유는 주로 사람의 인격과 관련된 안전에 관한 기본권으로서 주거의 자유권(헌법 제16조), 통신의 자유(헌법 제18조) 등을 포함하는 것으로서 종래 산업사회에 있어서 "혼자 있을 권리"(Right to be alone)라고 하는 소극적 권리(자유권)에서 오늘날에는 자신에 관한 사적 사항(정보)이 자신의 의사에 반하여 대외적으로 공개되지 아니하도록 스스로 통제할 수 있는 적극적인 권리(청구권)로 관념되기에 이르러 자유권적 성격과 아울러 청구권적 성격을 갖는 것으로 볼 수 있다"[102]거나 고도지식정보사회에 있어서 개인식별정보를 포함하여 개인정보를 보호한다는 것은 해당 개인의 사생활권, 명예권, 초상권, 성명권 등 인격권을 보호하는 의미를 가진다는 점에서 다수 학자들은 프라이버시권을 그 권리가 제창되던 당시의 "혼자 있을 권리"로 이해하지 않고 "자신에 관한 정보를 어떻게 어느 범위까지 다른 사람에게 전달할 것인가를 스스로 결정하는 권리", 즉 "자기정보통제권"을 포함하는 것으로 이해하는 등[103] 프라이버시권(사생활의 비밀권)의 하나로서 정보자기통제권을 인정하는 것이 일반적이다.[104]

그 외 헌법 제10조에 근거하는 포괄적인 행복추구권의 하나로서 정보자기통제권을 인정하는 입장도 있으며, "저작권이 인격의 표현이라고 하더라도 경제적 이익으로서 사람과 독립하여 법적인 객체로 되는 바와 같이 초상권도 이와 같이 인격권으로부터 분리되는 경우도 있다"고 하여 개인정보자기통제

---

99) 프라이버시(Privacy)라는 용어는 '사람의 눈을 피하다'라는 뜻의 라틴어 ' Privatun'에서 유래된 말로 프라이버시권에 대한 본격적인 논의는 19세기 말 시작되었다. 1888년 미국의 토마스 쿨리 판사는 종래 명예훼손의 법리와 생활방해 (nuisance), 불법침해(trespass), 사적 도청의 제한 등에 따른 반사적 이익으로 관념되어 오던 프라이버시를 불법행위법상의 "혼자있을 권리(Right to be let alone)"로 정의하였는데 2년 뒤인 1890년 Warren과 Brendeis라는 두 변호사는 자신들의 논문 "The Right to Privacy"에서 프라이버시권을 본격적으로 다루면서 민주주의에서 가장 중요한 자유로서 헌법에 반영되어야 한다는 주장을 거쳐 1902년 원고가 동의없이 자신의 초상을 회사 상품의 선전에 사용하였다는 이유로 손해배상을 청구한 사건(Roberson v, Rochester Folding Box Co.)에서 뉴욕 주 대법원이 입법에 의한 해결권고를 함으로써 비로소 입법상의 권리로서 프라이버시권의 성립을 보게 되었다.

100) 藤原靜雄, 「逐條個人情報保護法」, 弘文堂, 平成 15年, 1쪽 참조.

101) Smedinghoff. T. J., 「Online law the SPAs legal guide to doing business on the internet」, The Soft ware Publishers Association, 1996, p. 355.

102) 성낙인, 「헌법학」, 법문사 제7판, 487쪽 내지 489쪽 참조.

103) 藤原靜雄, 「逐條個人情報保護法」, 22쪽 참조.

104) 정종섭, 「헌법학원론(제2판)」, 박영사, 2007, 526쪽; 박진우, "우리나라의 개인정보보호제도와 언론보도", 32쪽.

권을 인격권으로부터 재산권으로의 전환을 지적하는 입장[105]도 있다.

3. 개인정보의 법적 속성

가. 기본적인 속성

앞에서 살펴본 바와 같이 개인정보는 명예·초상·프라이버시 등 정신적 속성의 보호이익으로서, 인격의 자유로운 발전을 위하여 제3자에 의한 침해에 대해 보호되어야할 이익의 총체라고 할 수 있는 동시에 정보주체의 개인정보자기결정권에 반하지 아니하다면 동의한 정보의 원형을 저해하지 아니하는 범위 내에서 해당 정보를 그 목적에 따라 경제적으로 사용할 수 있는 재산권적 성격 또한 보유한다고 할 것이다

따라서 제3자에 의한 개인정보의 이용 등이 갖는 정보주체의 사생활권 등 포괄적인 인격권에 대한 침해의 위험을 정보주체가 동의를 통해 인수하였다면, 그 동의한 정보의 원형성이 유지되는 범위 내에서 해당 개인정보의 보유주체는 그 동의한 목적 범위 내에서 해당 정보에 대한 수집·이용 등 처리권을 자기의 책임 하에 행사할 수 있다고 할 것이다. 그렇다고 하더라도 저작인격권과 저작재산권의 예에서 보는 바와 같이 개인정보의 기본적인 속성이 일신전속성을 갖는 인격권적 요소를 갖는 점에서 그러하지 아니한 순수한 재산권과 달리 그 귀속이나 행사에는 제한이 따를 수밖에 없는 것으로 보아야 하는 것이다.

나. 귀속상 일신전속권인지 행사상의 일신전속권인지 여부

“정보통신망 이용촉진 및 정보보호 등에 관한 법률”(이하 “정보통신망법”이라 한다)은 정보주체가 그 이용 등을 허용한 목적 범위 내에서 해당 개인정보를 보유하고 있는 정보통신사업자로 하여금 당해 정보를 이용할 수 있도록 규정하는 한편(제22조) 제3자 등에게 보유하고 있는 개인정보를 제공하고자 할 경우에는 정보주체에게 그 사실을 알리고 정보주체의 동의를 얻도록 한 점에 비추어 볼 때(제24조부터 제26조), 정보주체 이외의 제3자는 원칙적으로 개인정보를 수집·이용 등 처리를 할 수 없지만 정보주체의 정보자

105) 정영화, "인터넷상 개인정보유통의 오남용에 관한 법제연구", 「인터넷・언론・법」, 한국법제연구원, 2002, 58쪽 ; 船越一行, 「情報とプライシーの權利」, 北樹出版, 2001, 122쪽.

기통제권의 행사를 통해 일정한 목적범위에서 그 수집·이용 등 처리를 동의받은 제3자는 동의한 목적범위 내에서 개인정보를 이용할 수 있는 권리를 가질 뿐 또 다른 제3자(업무상 자신의 감독과 책임 하에 있게 되는 제3자나 그러하지 아니한 제3자 및 영업의 양수나 합병에 의해 자신의 지위를 법적으로 승계하게 된 새로운 제3자 등)에게 그 권리를 양도하거나 이용하게 하는 것은 허용되지 아니하는 것으로 보아야 한다.

이러한 점에서 개인정보에 대한 정보주체의 정보자기통제권은 귀속에 있어서 일신전속성을 갖는 것이라기보다는 행사에 있어서 일신전속성을 갖는 것으로 보아야 할 것이다. 그렇기 때문에, 정보주체가 제공한 개인정보에 대한 이용 등은 제3자에게 이전 또는 양도될 수 있으나 그 정보의 자기통제권은 항상 정보주체에게 남아있게 되는 것이다.[106] 이를 표시하면 아래의 <그림 9>와 같다.

<그림 9> 개인정보 주체의 정보자기결정권의 속성과 융통성의 제한

즉, <그림 9>에 의하면, 정보주체 이외의 자인 정보통신서비스제공자는 정보주체의 정보자기통제권의 행사로서 동의를 통해 그 동의의 목적범위 내에서 이용자의 개인정보를 수집·보관·처리·이용·제공·관리 등을 할 권리를 갖지만, 이러한 권리를 제3자에게 제공하는 것은 정보자기통제권과 관련하는 것으로서 정보주체의 동의를 요한다.

물론, 인격적 요소를 배제한 비식별화된 개인정보는 정보통신망법 상의 개인

106) 참고판례 : 원고는 피고에게 위 재산적 손해와는 별도로 원고의 명예와 신용이 현저하게 손상되었다고 주장하연서 위자료로서 금 30,000,000원을 구하나, 위에서 인정한 바와 같이 원고는 이 사건 직물디자인의 저작자인 위 이태리의 회사로부터 저작재산권을 양도받은 저작재산권자에 불과하여(저작인격권은 저작자의 일신전속권으로서 양도할 수 없다), 다른 특별한 사정이 없는 한 정신적 손해로서 위자료를 구할 수는 없다 할 것이므로, 이 부분 원고의 위 청구는 이유 없다 할 것이다(서울민사지법 1995. 1. 27. 선고 93가합48477 판결 : 항소).

정보가 아닌 것으로 된다는 점에서 그 융통성에는 어떠한 제한도 따르지 않고, 경우에 따라서는 「저작권법」상 데이터베이스권으로 보호받을 수도 있게 된다. 요컨대, 개인정보는 정보주체를 식별할 수 있는 한 정보주체의 정보자기통제권의 대상이 되지만 식별성이 없는 한 제3자의 재산권에 귀속된다고 할 것이다(일신전속성의 소멸).

4. 빅 데이터 환경과 개인정보보호의 방향

대량의 데이터를 데이터 마이닝이나 프로파일링 또는 매칭프로그램 등 다양한 분석기술을 거치게 되면, 개별 데이터가 가진 정보의 값이 아무리 미미하다고 하더라도 해당 데이터를 생산한 개인이나 법인 또는 물건의 대상별 데이터로 분류할 수 있을 뿐 아니라 이렇게 분류된 데이터의 분석을 통해 해당 대상의 속성이나 장래의 변화발전의 성향 등에 대한 새로운 지식의 창출이 가능할 것으로 보인다.
위와 같은 기술발전의 경향은 정보주체의 동의권의 지배를 받지 아니하는 개인에 관한 비식별정보로 구성되는 빅 데이터를 통해서 특정지역을 출입하는 통행인과 범죄유형 및 범죄발생유인환경 등을 종합적으로 분석하여 범죄를 예방하는 프로그램을 개발하거나 사회적 약자에 대한 보호서비스의 제공 및 한정된 지구자원의 낭비 없는 생산을 가능하게 개인별 맞춤서비스 제공 등을 가능하게 하는 순기능을 갖는 반면, 개인이 원하지 아니함에도 불구하고 빅 데이터가 자신의 필요를 충족하기 위해 일방적 내지 이용목적의 범위를 벗어난 개인별 데이터베이스의 구축 내지 개인감시 또한 가능하다는 동전의 양면성을 보여준다.
이러한 양면성과 개인에 관한 정보를 본인의 동의하에 이용할 권한을 가졌다고 하더라도 해당 정보에 대한 통제권은 정보주체의 일신에 전속한다는 점을 고려할 때 빅 데이터 시대에 있어서는 정보주체의 수집동의 대상이 되지 아니하는 비식별정보의 대량집적화와 이러한 직접화된 데이터의 분석을 통해 생성된 개인별 데이터베이스의 존재여부에 대해 정보주체에게 통지할 의무를 부여하는 한편 정보주체로 하여금 통지된 개인데이터에 대한 열람·정정·차단권 및 삭제권을 부여하는 사후통제권 내지 목적 외 사용에 대한 엄격

한 통제권 보장이 보다 중요할 것으로 생각된다.

5. 최근 동향

국회 문화체육관광방송통신위원회 소속 신경민 의원은 2012. 10. 24. 보도자료를 통해 가칭 「온라인 행태정보 보호 및 이용에 관한 법률안」을 발의할 예정이라고 밝혔는데, 사이트 접속기록, 이용 기록, 관심 분야, 구매 내역, 결제 기록, IP 정보 등 최근 몇 년 간 정보통신서비스 제공 사업자에 의해 수집된 비식별 개인정보를 활용한 맞춤형 온라인 서비스(광고) 시장이 성장하고 있으나, 현행 개인정보 법령상 이러한 비식별 개인정보 보호의 공백상태가 지속되어 프라이버시가 침해될 가능성이 높아 비식별 개인정보 역시 정보주체의 동의와 사후거부권을 제도화 할 필요가 있다고 한다.
그러나 현행 개인정보 보호법이나 정보통신망법은 개인정보를 정의함에 있어 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보 외에 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보까지도 개인정보로 본다는 포괄적 규정을 두고 있다 .[107]이와 관련하여 IP정보를 개인정보로 보려는 입장이 있고, 하급심 판례 중에는 휴대폰 IMEI(국제이동단말기식별번호)를 개인정보로 본 판결도 있다. 그런데 위 법률안에서 규제를 하려는 행태 정보들의 대부분이 개인정보 보호법이나 정보통신망법의 '개인정보'의 개념에 포섭될 수 있는 것으로 보이는바 위 입법안이 중복입법을 통한 규제인지 여부에 관한 심도 있는 논의가 필요하다.[108]

---

107) 이에 관하여 개인정보와 개인에 관한 정보를 구분하지 않고 개인정보 보호법 제2조 제1호와 정보통신망법 제2조 제6호가 괄호 부분까지 개인정보로 규율하고 있는 것에 관한 비판적 견해가 제기되고 있는바, 이와 관련하여서는 구태언, [LAW&스마트] '개인정보' 유감, 법률신문. http://www.lawtimes.co.kr/LawEdit/Edit/EditContents.aspx?serial=62580&kind=ba11) 참조.

108) 경찰은 모 포털사업자가 모바일 광고 플랫폼을 구축한 후 이용자의 동의 없이 스마트폰 애플리케이션을 통해 스마트폰 이용자의 위치정보를 수집한 것으로 보고 수사하여 검찰에 기소의견으로 송치하였는데, 이에 대하여 검찰은 현재와 같이 하나의 기지국에 여러 휴대전화가 접속하는 IP주소 체계의 특성상 IP 주소만으로는 특정 이용자가 특정 위치에 존재하고 있다는 점을 알 수 없고 다른 정보와 쉽게 결합하여 이용자를 특정할 수도 없다는 이유로 무혐의 처분을 하는 등 수사기관 사이에도 해석에 있어서 혼선이 있다.

Ⅱ. 현행 개인정보 보호 법제의 문제점

1. 빅 데이터 환경 하에서 개인정보 보호 법제의 분석의 필요성

가. 개인정보를 위협하는 빅 데이터

빅 데이터의 핵심적인 개념징표는 앞에서 살펴본 바와 같이 “정보의 집적, 정보의 결합, 정보의 분석”이라고 할 수 있고, ‘정보의 집적’이란 데이터의 양을 고도화한다는 의미이고, ‘정보의 결합’이란 다양한 목적 또는 형태의 데이터를 연결시키는 것을 의미하며, ‘정보의 분석’이란 거대·다양한 데이터를 연결하여 원래 데이터 이상의 효용이나 가치를 창출해 내는 것을 의미한다, 그렇기 때문에 빅 데이터의 처리는 「개인정보 보호법」을 비롯하여 개인정보보호와 관련한 법률이 정보주체의 동의를 전제로 하고 있는 개인식별정보를 수집·가공·편집하는 것뿐만 아니라, 정보주체의 동의를 요하지 아니하거나 정보주체가 존재하지 아니하는 정보를 국내외에 걸쳐 광범위하게 수집한 후에 이에 대하여 빅 데이터 기술을 적용함으로써 사적 또는 공적 영역의 가치 있는 정보를 추출 또는 생성, 가공하는 과정에서 식별가능성있는 정보로 전환될 수 있고, 이를 토대로 특정개인에 대한 지식의 범위를 당해 정보주체도 인식하지 못하는 범위까지 지식화할 가능성이 있다.[109] 즉, 빅 데이터 처리자의 일방적인 프로파일링 또는 데이터마이닝에 의해서 특정개인에 관한 정보가 생성되거나 이를 통해서 인격체인 특정개인의 형상화함으로써 당해 정보주체에 대한 사실에 관한 정보가 생성될 수도 있고, 더 나아가 당해 정보주체의 인격에 대한 왜곡가능성 또는 당해 정보주체가 원하지 않거나 인식조차 하지 못하는 개인화의 가능성도 있는 것이다. 이러한 점에서 빅데이터 시대의 정보주체의 보호를 위한 제도적 접근으로서 현행 개인정보 보호 법제 상의 정보주체의 정보자기통제권과 관련한 규정의 빅 데이터에 대한

109) 미국 시민단체인 “전자프라이버시정보센터”(EPIC)는 “구글의 개인정보 통합정책은 이용자의 개인정보 통제를 약화시키는 반면 광고주들에게 더 많은 개인정보를 부여하는 것인 동시에 명백한 고객정보의 남용이며 소비자 프라이버시에 대한 중대한 위협이다”라고 비판하면서 이러한 정책의 시행의 중단을 구하는 소송을 연방법원에 제기하였다. http://www.yonhapnews.co.kr/bulletin/2012/02/09/0200000000AKR 20120209169200009. HTML <2012. 3. 11. 접속> ; EPIC는 2010년에도 구글의 개인정보 문제를 FTC에 제소한바 있으며 그 결과 지난해 FTC와 구글은 확실한 동의없이 이용자 정보를 사외에서 공유하는 것을 금지하기로 합의를 보았다고도 한다.

적응성여부를 재검토해볼 필요가 있다.

나. 빅 데이터 환경에서 개인정보 보호를 위한 분석대상

정보화시대에 대응한 현행 개인정보 보호법제로는 민간영역과 공공영역의 모든 개인정보처리자를 수범자로 하여 온라인과 오프라인의 모든 개인정보를 대상으로 개인정보의 보호에 있어서 일반법의 기능을 수행하는 「개인정보 보호법」을 비롯하여 정보통신서비스제공자와 정보통신서비스제공자로부터 개인정보를 제공받은 자를 수범자로 하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 전자상거래에 관련한 소비자정보의 보호를 위한 「전자상거래 등에서의 소비자보호에 관한 법률」 등이 있다. 그밖에 민감한 정보로서 법률이 개별적으로 규정하고 있는 것으로는 신용정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호하기 위한 「신용정보의 이용 및 보호에 관한 법률」 및 실지명의에 의한 금융거래의 실시와 그 비밀의 보장 등에 관한 「금융실명거래 및 비밀보장에 관한 법률」, 위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하기 위한 「위치정보의 보호 및 이용 등에 관한 법률」, 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 하는 「통신비밀보호법」, 환자의 진료기록 보호를 규정한 「의료법」 그리고 개인의 행적에 관한 데이터의 집합체라 할 수 있는 개인의 과세정보의 보호를 규정한 「국세기본법」 등이 있다. 이하에서는 공공과 민간영역의 개인정보보호에 관한 일반법적 기능을 수행하는 「개인정보 보호법」을 중심으로 정보주체의 정보자기통제권과 관련한 규정(제2조제1호의 개인정보에 관한 정의규정, 제3조의 개인정보 보호원칙, 제4조의 정보주체의 권리 및 제14조의 국제협력 등)의 빅 데이터 시대의 적응가능성과 그 한계를 살펴보기로 한다.

2. 빅 데이터와 「개인정보 보호법」

가. 「개인정보 보호법」에 의한 정보주체의 보호

민간과 공공을 아우르는 일반법으로서 「개인정보 보호법」은 제2조제1호에서 그 자체로서는 식별성이 없더라도 다른 정보와 결합하여 알아 볼 수 있는 것을 개인정보로 개념정의한 후 제3조에서는 개인정보보호의 원칙으로서 명확한 목적 범위 내에서 최소한 개인정보의 수집(제1항), 목적범위 내의 개인정보처리 및 목적 외 활용금지(제2항), 개인정보의 정확성·완전성·최신성의 보장(제3항), 개인정보의 안전한 관리(제4항), 처리방침의 공개 및 열람청구권의 보장(제5항), 사생활침해를 최소화하는 개인정보처리(제6항), 익명처리의 원칙(제7항) 및 정보처리자의 책임과 의무의 준수에 노력할 의무(제8항) 등을 규정하고 있고, 이를 구현하기 위한 정보주체의 권리에 대하여는 제4조에서 별도로 규정하고 있다. 정보주체의 권리를 정한 제4조에 따르면 정보주체는 개인정보의 처리에 관한 정보를 제공받을 권리(제1호), 개인정보의 처리에 관한 동의여부와 범위를 선택·결정할 권리(제2호), 개인정보의 처리여부를 확인하고 열람할 권리(제3호), 개인정보의 처리정지·정정·삭제 및 파기요구권(제4호) 및 신속한 구제받을 권리(제5호)를 가짐을 알 수 있다.

개인정보보호의 원칙(제3조)와 개인정보주체의 권리(제4조)를 제외하면, 대부분의 규정들은 개인정보의 “수집”을 출발선으로 하고 있고, 정보주체의 “동의”를 전가의 보도와 같이 사용하고 있다. 그러나 빅 데이터 환경 하에서는 수집과 동의에 천착하기 보다는, 후술하는 바와 같이 개인정보의 “생성”과 정보주체에 대한 “고지”에 방점을 두는 접근이 필요하다. 즉, 개인정보의 취득이 개인정보의 “생성”을 통하여 이루어진다는 점을 인식하고, 이를 출발선으로 하는 개인정보의 라이프 사이클을 고려한 제도적 보완이 요구되며, 정보주체로부터 “수집”된 개인정보가 아닌 대량으로 집적된 비식별정보로부터 “생성”되는 개인정보에 대한 정보주체의 알권리와 접근권, 통제권을 실질적으로 확보할 수 있는 제도적 장치를 마련할 필요가 있다.

나. 개인정보의 개념(「개인정보 보호법」 제2조제1호)

「개인정보 보호법」 제2조제1호는 개인정보를 “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"고 함으로써 일정한 개인에 관한 데이터가 정보주체의 정보자기통제권의 대상이 되는 데이터인지 여부의 기준으로서 '살아 있는 개인'과 '정보로부터 해당 개인의 알 수 있거나 다른 정보와 결합하여 쉽게 알 수 있을 것'을 전제로 하고 있다. 이러한 정의 방식은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」[110] 및 「위치정보의 보호 및 이용 등에 관한 법률」[111], 「전자서명법」[112], 「국민의 형사재판 참여에 관한 규칙」[113], 「금융실명거래 및 비밀보장에 관한 법률 시행령」[114] 등 개인정보에 관한 거의 모든 법령에서 동일한 모습을 보이고 있다. 다만, 「신용정보의 이용 및 보호에 관한 법률」은 신용정보를 정의함에 있어서 구체적이고 다양한 식별요소를 도입하여 그 범위를 제한하고 있다.

---

110) 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1. ~ 5. (생 략)
6. "개인정보"란 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.
7. ~ 12. (생 략)
② (생 략)

111) 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. "위치정보"라 함은 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 「전기통신사업법」 제2조제2호 및 제3호에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것을 말한다.
2. "개인위치정보"라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다.

112) 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. ~ 12. (생 략)
13. "개인정보"라 함은 생존하고 있는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

113) 제44조(배심원 등의 개인정보 공개절차) ① 법 제52조에 따른 개인 정보는 배심원·예비배심원 또는 배심원후보자에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호·주소 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.

114) 제6조(거래정보등의 범위) 법 제4조제1항 및 이 영 제5조에서 "금융거래의 내용에 대한 정보 또는 자료"라 함은 특정인의 금융거래사실과 금융기관이 보유하고 있는 금융거래에 관한 기록의 원본·사본 및 그 기록으로부터 알게 된 것(이하 "거래정보등"이라 한다)을 말한다. 다만, 금융거래사실을 포함한 금융거래의 내용이 누구의 것인지를 알 수 없는 것(당해 거래정보등만으로 그 거래자를 알 수 없더라도 다른 거래정보등과 용이하게 결합하여 그 거래자를 알 수 있는 것을 제외한다)을 제외한다.

「신용정보의 이용 및 보호에 관한 법률」상 신용정보의 정의 규정

법	시행령
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. “신용정보”란 금융거래 등 상거래에 있어서 거래 상대방의 신용을 판단할 때 필요한 다음 각 목의 정보로서 대통령령으로 정하는 정보를 말한다.	제2조(정의) ① 「신용정보의 이용 및 보호에 관한 법률」(이하 “법”이라 한다) 제2조제1호 각 목 외의 부분에서 “대통령령으로 정하는 정보”란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 다른 법령에 따라 공시(公示) 또는 공개된 정보나 다른 법령에 위반됨이 없이 출판물 또는 방송매체나 국가·지방자치단체 또는 공공기관(「공공기관의 정보공개에 관한 법률」 제2조제3호의 기관 중 국가기관 및 지방자치단체를 제외한 기관을 말한다. 이하 이 조에서 같다)의 인터넷 홈페이지 등의 공공매체를 통하여 공시 또는 공개된 정보는 제외한다.
가. 특정 신용정보주체를 식별할 수 있는 정보	1. 법 제2조제1호가목의 특정 신용정보주체를 식별할 수 있는 정보: 생존하는 개인의 성명, 주소, 주민등록번호, 외국인등록번호, 국내거소신고번호, 여권번호, 성별, 국적 및 직업 등과 기업(사업을 경영하는 개인 및 법인과 이들의 단체를 말한다. 이하 같다) 및 법인의 상호, 법인등록번호, 사업자등록번호, 본점 및 영업소의 소재지, 설립연월일, 목적, 영업실태, 종목, 대표자의 성명 및 임원 등에 관한 사항(제2호부터 제5호까지의 어느 하나에 해당하는 정보와 결합되는 경우만 해당한다)
나. 신용정보주체의 거래내용을 판단할 수 있는 정보	2. 법 제2조제1호나목의 신용정보주체의 거래내용을 판단할 수 있는 정보: 대출, 보증, 담보제공, 당좌거래(가계당좌거래를 포함한다), 신용카드, 할부금융, 시설대여와 금융거래 등 상거래와 관련하여 그 거래의 종류, 기간, 금액 및 한도 등에 관한 사항
다. 신용정보주체의 신용도를 판단할 수 있는 정보	3. 법 제2조제1호다목의 신용정보주체의 신용도를 판단할 수 있는 정보: 금융거래 등 상거래와 관련하여 발생한 연체, 부도, 대위변제, 대지급과 거짓, 속임수, 그 밖의 부정한 방법에 의한 신용질서 문란행위와 관련된 금액 및 발생·해소의 시기 등에 관한 사항. 이 경우 신용정보주체가 기업인 경우

	에는 다음 각 목의 어느 하나에 해당하는 자를 포함한다. 가. 「국세기본법」 제39조제2항에 따른 과점주주로서 최다출자자인 자 나. 「국세기본법」 제39조제2항에 따른 과점주주인 동시에 해당 기업의 이사 또는 감사로서 그 기업의 채무에 연대보증을 한 자 다. 해당 기업의 의결권 있는 발행주식총수 또는 지분총액의 100분의 30 이상을 소유하고 있는 자로서 최다출자자인 자 라. 해당 기업의 무한책임사원
라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보	4. 법 제2조제1호라목의 신용정보주체의 신용거래능력을 판단할 수 있는 정보: 금융거래 등 상거래에서 신용거래능력을 판단할 수 있는 다음 각 목의 어느 하나에 해당하는 정보 가. 개인의 재산·채무·소득의 총액 및 납세실적 나. 기업의 연혁·주식 또는 지분보유 현황 등 기업의 개황(槪況), 판매명세·수주실적 또는 경영상의 주요 계약 등 사업의 내용, 재무제표(연결재무제표 및 결합재무제표를 포함한다. 이하 같다) 등 재무에 관한 사항과 「주식회사의 외부감사에 관한 법률」에 따른 감사인의 감사의견 및 납세실적
마. 그 밖에 가목부터 라목까지와 유사한 정보	5. 법 제2조제1호마목에 따른 정보로서 다음 각 목의 어느 하나에 해당하는 정보 가. 법원의 금치산선고·한정치산선고·실종선고의 재판, 회생·개인회생과 관련된 결정, 파산선고·면책·복권과 관련된 결정, 채무불이행자명부의 등재·말소 결정 및 경매개시결정·경락허가결정 등 경매와 관련된 결정에 관한 정보 나. 국세·지방세 또는 관세의 체납 관련 정보 다. 벌금·과태료·과징금 또는 추징금 등의 체납 관련 정보 라. 사회보험료·공공요금 또는 수수료 등 관련 정보 마. 기업의 영업에 관한 정보로서 정부조달 실적 또는 수출·수입액 등의 관련 정보 바. 개인의 주민등록 관련 정보로서 출생·사망·이민·부재에 관한 정보, 주민등록번호·성명의 변경 등에 관한 정보

	사. 기업등록 관련 정보로서 설립, 휴업·폐업, 양도·양수, 분할·합병, 주식 또는 지분 변동 등에 관한 정보 아. 다른 법령에 따라 국가, 지방자치단체 또는 공공기관으로부터 받은 행정처분에 관한 정보 중에서 금융거래 등 상거래와 관련된 정보 자. 그 밖에 신용정보주체의 신용등급, 신용조회회사의 신용정보 제공기록 또는 신용정보주체의 신용회복 등에 관한 사항으로서 금융위원회가 정하여 고시하는 정보
2. “개인신용정보”란 신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보를 말한다.	② 법 제2조제2호에서 “대통령령으로 정하는 정보”란 제1항에 따른 신용정보 중 기업 및 법인에 관한 정보를 제외한 개인에 관한 신용정보를 말한다.

한편, 빅 데이터의 처리는 데이터와 데이터간의 연결성을 요소하기 때문에 수집단계에서 개인식별성을 갖추지 아니한 데이터도 사후적으로 특정 개인에 대한 식별을 구현하거나 구현가능성을 현저하게 높일 수 있다는 점을 배제하기 어렵다. 그렇다고 하더라도 처리대상이 되는 데이터의 수집당시로서는 개인식별성이 없을 뿐만 아니라 다른 정보와의 결합을 통한 식별가능성도 없는 경우라면, 특정개인의 동의를 얻는 것이 불가능할 뿐만 아니라 활용가치가 높은 데이터의 재활용을 불합리하게 막는 것으로 되어 바람직하지 않다.

문제는 빅 데이터를 ‘다른 정보와 결합하여 쉽게 알 수 있는’의 요건을 갖춘 것으로 보아야 할 것인가에 있는바, 모든 것은 양면성을 갖는 점, 빅 데이터 기술은 ‘쉽게 알 수 있는’에 해당하는 것으로 보기 어렵다는 점과 우리 헌법 제37조제2항의 비례원칙에 의할 때 빅 데이터에 해당 개인을 알 수 있게 되거나 해당 개인에 관하여 새로운 지식을 더하게 된 경우에는 사후적 동의 내지 개인정보열람권 등으로 해결함이 바람직하다.

빅 데이터 환경은 집적된 큰 규모의 데이터(빅 데이터)를 정보의 결합 또

는 분석 등 고객이 요구하는 정보를 얻어내는 과정(빅 데이터 처리)을 거쳐 가치 있는 정보를 도출하게 된다. 빅 데이터의 수집과정에서 식별정보 또는 식별가능정보를 대상으로 하는 경우에는 「개인정보 보호법」에 따른 개인정보에 해당하므로 원칙적으로 동의의 대상이 됨에는 이론이 없으며, 이는 빅 데이터 처리를 거쳐 추출된 정보가 식별정보 또는 식별가능정보 여부와는 무관하다. 다만, 이의 이용 또는 제공 등에 있어서 개인정보로서 보호의 대상에 해당하는가 만이 문제가 된다. 이와 반대로 식별정보 또는 식별가능정보에 해당하지 아니하는 빅 데이터를 수집하는 경우에는 「개인정보 보호법」의 개인정보의 정의의 문리해석 상 개인정보에 해당하지 아니하는 것으로 볼 것이고, 빅 데이터 처리를 거쳐 추출 또는 생성된 정보가 식별 또는 식별가능 정보가 아니라면 이의 이용 또는 제공 등에 있어서도 개인정보 보호와는 무관하게 된다. 그러나 식별정보 또는 식별가능정보에 해당하지 아니하는 빅 데이터를 수집하고, 이들 데이터를 대상으로 빅 데이터 처리과정을 거쳐 식별정보 또는 식별가능정보를 생성해 내는 경우에는 수집단계에서는 개인정보에 해당하지 아니하더라도 이용 또는 제공 등의 단계에서는 개인정보에 해당할 수 있다. 즉, 빅 데이터 처리자는 빅 데이터 처리를 통해서 개인정보를 생성함으로써 동의가 전제되지 않는 개인정보를 기록 또는 저장, 보유하게 되고, 이를 가공 또는 편집하거나 이용·제공하게 된다. 빅 데이터는 프로파일링 또는 데이터 마이닝 등 그 처리과정을 통해 비식별정보가 식별정보로 변화·전환될 가능성이 있고, 이 경우에는 식별정보의 수집을 위한 사전 동의를 요구하기 어렵게 된다. 빅 데이터 환경의 도래로 개인정보 여부를 판단함에 있어서 '다른 정보와의 결합의 용이성'에 따른 개인식별가능성뿐만 아니라 빅 데이터 처리 즉, '집적정보의 가공·편집'에 따른 개인식별가능성이라는 측면을 고려하여야 하는 상황이 된 것이다.

비록 「개인정보 보호법」 제2조 제2호는 처리를 "개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다"고 함으로써 개인정보의 수집은 물론 생성도 포함하는 것으로 정의하고 있지만, 이는 용어 정의에 그칠 뿐 실질관계를 규율하는 규정 어디에서도 개인정보의 생성에 관하여 다루고 있지 아니하다.[115] 이에 반하여 「신용정보의 이용 및 보호에 관한 법률

」은 신용정보가 수집의 대상일 뿐만 아니라 생성의 대상이라는 점을 예상하고 있다. 즉, 동법 제2조 제8호는 신용조회업무를 “신용정보를 수집·처리하는 행위, 신용정보주체의 신용도·신용거래능력 등을 나타내는 신용정보를 만들어 내는 행위 및 의뢰인의 조회에 따라 신용정보를 제공하는 행위”로 정의함으로써 신용정보의 생성을 포함하고 있다.[116] 따라서 신용정보를 생성하는 행위는 「신용정보의 이용 및 보호에 관한 법률」에 따른 신용조회업무로서 이를 업으로 하고자 하는 경우 금융위원회의 신용조회업 허가를 받아야 한다.[117]

다. 개인정보 보호 원칙(「개인정보 보호법」 제3조)

「개인정보 보호법」 제3조는 8개의 개인정보보호의 원칙을 제시하고 있는 바, 종래 OECD(Organization for Economic Cooperation and Development)가 발표한 프라이버시 가이드라인(Privacy Guideline)에 포함되어 있는 8가지 원칙과 유사하다. OECD의 8원칙으로는 수집제한의 원칙, 내용정확의 원칙, 목적명확의 원칙, 이용제한의 원칙, 안정성 확보의 원칙, 개인정보정책 등의 공개원칙, 정보주체의 참여 원칙, 수집기관 책임의 원칙이 있다. 이러한 개인정보의 수집과 통제 등 개인정보 프라이버시 권리에 대한 기본 정책방향 또는 원칙을 FIPPs(Fair Information Practice Principles)이라고 하는데, 결국 「개인정보 보호법」 제3조는 우리나라 개인정보보호에 관한 FIPPs를 제시하고 있는 것이다.

특히, 같은 법 제3조제1항은 “개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다”라고 최소수집의 원칙을 규정하고 있

115) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 정보통신서비스 제공자의 개인정보 관련 업무위탁에 관하여 규정하고 있는 제25조에서 위탁업무의 예시로서 수집·보관·처리·이용·제공·관리·파기 등을 열거하고, 이를 “취급”으로 약칭하고 있다. 즉, 개인정보의 “취급”이 수집·보관·처리·이용·제공·관리·파기 등을 포함하고 있는 것으로 기술하고 있고, 「개인정보 보호법」과 달리 “처리”는 수집 또는 이용, 제공 등과 병렬적인 개인정보 취급업무의 일종으로 보고 있다.

116) 이 뿐만 아니라 신용정보제공·이용자를 ‘고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 “만들어 낸 신용정보”를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자 … ’로 정의함으로써 신용정보의 생성을 염두에 두고 있다.

117) 「신용정보의 이용 및 보호에 관한 법률」 제4조

다.[118] 과도하고 필요 이상으로 개인정보를 수집하는 것이 원칙적으로 금지된다는 의미로서 빅 데이터의 개념 안에는 정보수집의 극대화를 통한 최대한의 정보 집적 및 관리를 내포하고 있다는 점에서 향후 필요한 범위에 대한 해석이 논란이 될 것으로 보인다.

빅 데이터의 현상을 긍정적으로 인정하고, 또 정보의 대용량화를 통한 빅 데이터가 미래의 금광이 될 것이라는 예찬론자의 지지를 받아들인다면, 데이터의 극대화를 미덕으로 하는 빅 데이터가 과연 어떻게 수집 데이터의 최소화를 미덕으로 하는 같은 법 제3조 제1항의 최소수집의 원칙과 조화로울 수 있는지 의문이 생길 수밖에 없다.[119]

라. 정보주체의 권리(「개인정보 보호법」 제4조)

「개인정보 보호법」 제4조 제2호는 개인정보주체에 대하여 '개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리'를 인정하여, 기업의 개인정보 처리범위를 결정하고 선택할 수 있는 '옵트인'(Opt-in) 제도를 전제로 하고 있다. 그런데, 빅 데이터는 다른 영역에서 발생한 데이터의 결합, 다른 루트에서 수집된 데이터의 자유로운 조합 내지 데이터간의 연결을 전제로 하고, 빅 데이터의 목적인 새로운 지식의 창출은 데이터의 결합과정에 대한 규제가 최소화되고 자유로운 대용량 데이터의 결합이 어느 정도 인정되어야 가능하게 된다. 다른 한편으로는 개인정보주체가 그 자체로서는 식별성이 없는 정보에 대한 결합의 여부나 결합의 범위를 결정하여 선택하고, 그 결과 개인정보 주체마다 결합정도를 따로 따로 정해야 한다면, 결합비용이나 유지비용 때문에 빅 데이터의 실현은 거의 불가능할 수 있다.

특히나 개인정보처리자의 개인정보를 '수집'함에 있어서 사전 동의 획득의

---

118) 「개인정보 보호법」 제3조의 개인정보 보호 원칙은 제1항부터 제8항까지에서 개인정보의 처리와 관련하여 처리목적의 명확화(제1항) 및 목적범위 내 적합 처리(제2항), 개인정보의 정확성, 완전성 및 최신성(제3항), 안전관리(제4항), 공개와 권리보장(제5항), 사생활의 최소침해(제6항), 익명처리(제7항), 책임과 의무의 준수(제8항)을 규정하고 있다. 그러나 최소성의 원칙을 정한 제1항은 '(처리) 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 "처리"하여야' 함을 규정한 것이 아니라, '(처리) 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 "수집"하여야 한다'고 함으로써 최소처리의 원칙이 아닌 최소수집의 원칙을 규정하고 있다. 이는 모두 개인정보를 "처리"함에 있어서 개인정보처리자가 개인정보 보호를 위하여 준수하여야 할 원칙을 정한 제3조의 다른 규정과 달리 유일하다.

119) 김경환, 위의 글.

무를 명시적으로 규정하고 있는 제15조와 달리, 개인정보의 수집은 물론 생성을 포함하는 '처리'에 관한 동의를 선택·결정할 권리(제4조 제2호)는 빅 데이터 처리의 과정에서 그 적용의 시점과 범위의 경계를 명확히 하기 어렵다.

다만, 최소처리의 원칙이 아닌 최소수집의 원칙을 정하고 있는 제3조 제1항과 달리, 제4조는 개인정보의 "처리"에 관한 정보를 제공받을 권리(제1호)와 개인정보의 "처리"에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리(제2호) 등을 규정함으로써 개인정보가 수집된 경우뿐만 아니라 빅 데이터 처리자가 비식별정보를 가공·편집·결합함으로써 식별정보가 생성된 경우까지 포함하게 된다. 즉, 빅 데이터 처리자가 대량의 비식별정보를 가공처리함으로써 개인정보가 생성된 경우에도 정보주체는 "개인정보의 처리에 관한 정보"에 해당하는 사실 즉, 자신의 개인정보가 생성되었다는 사실을 제공받을 권리를 가지게 된다(제1호). 또한, 빅 데이터 처리자가 개인정보를 생성하는 빅 데이터 처리과정에 관한 동의여부와 그 범위 등을 선택하고 결정할 권리를 가진다(제2호). 즉 정보주체는 빅 데이터 처리자가 비식별정보를 가공·편집·결합함으로써 개인정보를 생성하는 처리 행위에 대한 동의권을 가진다. 그러나 빅 데이터 처리자의 빅 데이터 처리과정을 거치기 전까지는 개인정보에 해당하지 않는 비식별정보의 경우에는 그 동의권자를 특정하기 어렵고, 가공·편집·결합 전의 비식별정보로부터 각 정보주체별로 이를 식별하여 빅 데이터 처리를 하는 것은 용이하지 아니하다. 따라서 정보주체의 동의권 즉, 동의 여부와 그 범위를 선택·결정할 권리는 사전에 이를 행사하기에는 제약이 따른다. 따라서 비식별정보가 빅 데이터 처리자의 가공·편집·결합으로 식별정보화하는 경우 이때로부터 정보주체의 동의권을 적극적으로 보장할 필요가 있다. 이를 위해서는 "개인정보의 처리에 관한 정보"로서 자신의 개인정보가 생성되었다는 사실을 제공받을 권리를 확보할 필요가 있다.

그러한 점에서 개인정보에 대한 빅 데이터기술의 적용을 전제하지 아니한 경우에는 정보주체의 동의권을 '옵트인'형태로 그대로 두되 계약상 빅 데이터 기술의 적용이 포함되어 있다면 빅 데이터를 적용한 때마다 추가로 '옵트아웃'(Opt-out)을 적용함이 바람직하다.[120]

120) 같은 취지, 김경환, 앞의 글.

마. 개인정보의 취득

「개인정보 보호법」 제2조 제2호는 개인정보의 처리를 '개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위'로 정의하고 있다는 점에서 「개인정보 보호법」은 개인정보의 수집과 생성을 구분하는 것으로 보아야 한다. 따라서 빅 데이터 처리자가 개인정보를 취득하는 경우는 개인정보를 수집하는 경우와 개인정보를 생성하는 경우 등으로 나눌 수 있다.

「개인정보 보호법」은 개인정보 수집의 실체적 요건으로서 개인정보를 수집할 수 있는 6가지 경우를 적시하고 있다(제15조 제1항). 즉, ① 정보주체의 동의를 받은 경우 또는 ② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 ③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 ④ 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우 ⑤ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 ⑥ 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우(이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한함)에 한하여 개인정보의 수집을 허용하고, 이를 위반하여 개인정보를 수집한 경우에는 5천만 원 이하의 과태료를 부과하도록 규정하고 있다(제75조 제1항 제1호). 또한, 개인정보 수집의 형식적 요건으로서 수집에 대한 동의를 받을 때 필수적 고지사항을 적시하고 있다(제15조 제2항). 즉, 개인정보 수집에 대한 동의를 받을 때에는 ① 수집·이용 목적과 ② 수집 대상 항목 ③ 보유·이용 기간 ④ 동의 거부권의 존재사실 및 동의거부에 따른 불이익의 내용을 고지하여야 하며, 이를 위반하는 경우 3천만 원 이하의 과태료를 부과하도록 규정하고 있다(제75조 제2항).

이에 반하여 「개인정보 보호법」은 빅 데이터 처리자가 비식별정보를 가

공·편집·결합함으로써 개인정보를 생성하는 경우 그 허용 여부와 실체적·형식적 요건에 대하여 전혀 규율하고 있는 바가 없다. 빅 데이터 처리자가 정보주체의 동의권의 지배를 받지 아니하는 비식별정보를 대량집적하고 이러한 대량집적정보의 가공·편집·결합을 통해 개인식별정보를 생성할 수 있는지 또는 생성의 요건과 그 한계 등을 규정하지 아니함으로써 혼란을 야기하고 있다. 한편, 「개인정보 보호법」 제20조는 정보주체 이외로부터 "수집"한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 ① 수집 출처 및 ② 처리 목적 ③ 처리의 정지요구권이 있다는 사실을 고지하여야 함을 규정하고 있다. 즉, 개인정보를 정보주체로부터 수집하는 경우에는 사전 동의를 얻도록 하고, 정보주체 이외로부터 수집하는 경우에는 정보주체의 요구에 따라 사후적으로 고지하도록 하고 있는 것이다.

생각건대 「개인정보 보호법」이 제2조 제2호의 "처리"가 개인정보의 생성을 포함하고 있다는 점과 동법이 개인정보의 생성을 제한하는 규정을 마련하고 있지 않다는 점에서 빅 데이터 처리에 의한 개인정보의 생성이 금지되는 것으로 볼 것은 아니하고 할 것이다. 다만, 「개인정보 보호법」 제4조는 정보주체의 권리로서 "개인정보의 처리에 관한 정보를 제공받을 권리"를 규정하고 있으므로, 빅 데이터 처리자는 개인정보를 생성하는 경우 그 정보주체에게 이를 통지하여야 하는 것으로 볼 것이다. 이때 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)와 같이 "정보주체로부터 수집"한 것이 아닌 개인정보의 취득에 관하여 고지의무를 규정할 필요가 있다고 할 것이다.

바. 이용·제공

개인정보의 이용에 관하여 「개인정보 보호법」은 "수집 목적의 범위" 내에서 이용할 수 있고(제15조 제1항), "수집목적의 범위"를 초과하여 이용하여서는 아니 된다고 규정하고 있다(제18조 제1항). 이를 위반하여 개인정보를 이용하는 경우에는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처하도록 하고 있다(제71조). 이에 반하여 개인정보의 취득경로가 수집이 아니라 생성의 경우에 이를 이용할 수 있는지 여부와 그 요건 및 한계 등에 대한 규정

을 마련하고 있지 아니하다. 앞서 살펴본 바와 같이 빅 데이터 처리에 의한 개인정보의 생성이 금지되는 것이 아니라고 하면, 개인정보의 생성은 이의 이용을 전제로 하는 것으로 이해하여야 한다는 점에서 생성된 개인정보의 이용도 허용되는 것으로 보아야 할 것이다. 그러나 수집목적에 따라 제한되는 "수집된 개인정보의 이용"과 달리 「개인정보 보호법」은 "생성된 개인정보의 이용"의 요건과 한계에 대해서 침묵하고 있다. 생각건대 「개인정보 보호법」 제18조 제2항[121]이 수집목적 외의 이용을 위한 요건으로서 "정보주체의 별도의 동의" 등을 요구하고 있다는 점에 비추어 볼 때, 사전 동의를 받지 않은 "생성된 개인정보의 이용"을 위해서는 원칙적으로 정보주체의 동의를 받아야 하는 것으로 보아야 할 것이다.

개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 제3자에게 제공·공유할 수 있다(제17조 제1항).[122] 이때 ① 개인정보를 제공받는 자와 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익의 내용을 정보주체에게

---

121) 제18조(개인정보의 이용·제공 제한) ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.
1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

122) 이 외에 ① 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 및 ② 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, ③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우에 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우에는 제3자에 개인정보를 제공할 수 있다.

알려야 한다(동조 제2항). 한편 「개인정보 보호법」은 “생성된 개인정보의 제공”에 대하여 별도의 명시적 규정을 마련하고 있지는 않지만, 빅 데이터 처리를 통하여 생성된 개인정보의 제3자 제공의 요건과 한계를 수집된 개인정보의 제3자 제공과 달리 정할 필요는 없을 것이므로, 빅 데이터 처리를 통하여 식별정보로 가공된 경우에도 제3자 제공을 위해서는 제17조부터 제19조까지의 규정의 적용을 받는 것으로 볼 것이다.

사. 위탁

빅 데이터 처리자가 빅 데이터 처리 업무를 제3자에게 위탁하는 경우에 「개인정보 보호법」 제26조의 적용을 받는지에 대한 검토가 필요하다.

먼저 빅 데이터 처리자가 “개인정보”의 처리 업무를 제3자에게 위탁하는 경우에는 「개인정보 보호법」 제26조의 적용을 받는다는 점은 명확하다. 즉, 개인정보의 처리 업무 위탁은 문서에 의하여야 하며, 그 문서는 ① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항과 ② 개인정보의 기술적·관리적 보호조치에 관한 사항 ③ 위탁업무의 목적 및 범위 ④ 재위탁 제한에 관한 사항 ⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 ⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항 ⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항을 포함하여야 한다(제26조 제1항). 또한, 개인정보처리 업무의 위탁자는 위탁업무의 내용과 개인정보처리 업무의 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하여야 한다(동조 제2항). 위탁자는 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다(동조 제3항).

다음으로 대량의 비식별정보를 집적한 자가 제3자에게 빅 데이터 처리 업무를 위탁하는 경우 즉, 비식별정보를 보유한 자가 제3자에게 당해 정보를 가공·편집·결합하게 함으로써 개인정보를 생성하는 경우에는 위탁업무의 대상이 정보가 비식별정보라는 측면에서 제26조의 적용 대상이 아니라는 견해가 있을 수 있으나, “개인정보의 처리”는 개인정보의 생성을 포함하므로 개인정보 처리 업무의 위탁으로 보아야 할 것이다. 따라서 빅 데이터 처리 업

무를 제3자에게 위탁하는 경우에는 문서에 의하여야 하고, 정보공개 및 수탁자의 교육·감독 등의 책임을 지는 것으로 보아야 한다.

한편, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 개인정보 관련 업무의 위탁에 관하여 이용자의 동의를 받도록 규정하고 있다. 동법 제26조는 개인정보의 취급위탁을 규정하면서 위탁업무를 “수집·보관·처리·이용·제공·관리·파기 등”으로 열거하고 있다. “수집·보관·처리·이용·제공·관리·파기 등”을 예시적 규정으로 보고, 빅 데이터 처리를 통한 개인정보의 생성에 관한 업무도 개인정보의 취급업무의 일종으로 본다면, 비식별정보를 대상으로 하는 빅 데이터 처리 업무를 제3자에게 위탁하는 자가 정보통신서비스 제공자인 경우에는 이용자에게 법정사항을 고지하고 동의를 받아야 할 것이다. 그러나 식별정보 또는 식별가능정보를 포함하는 빅 데이터 처리업무를 제3자에게 위탁하는 경우를 별론으로 하면, 빅 데이터 처리과정을 거치지 아니하여 개인정보가 생성되기 이전의 단순한 비식별정보의 집적상태에서 정보주체를 특정하여 빅 데이터 처리업무의 위탁에 대한 사전 동의를 구하는 것은 불가능하다. 업무위탁에 대한 형식적인 동의를 구하도록 하기 보다는, 앞서 개인정보의 취득과 이용·제공에서 살펴 본 바와 같이 업무위탁에 의한 개인정보의 생성에 대하여 사후적으로 그 사실을 고지하도록 하고 그 이용에 대한 정보주체의 권리를 실질적으로 확보할 수 있도록 하는 방안을 마련하는 것이 바람직하다.

아. 보존 및 파기

개인정보 주체의 개인정보자기결정권 보장 차원에서 개인정보 삭제 요청이 있거나 제공되는 서비스가 종료될 경우 사업자는 정당한 또는 합리적인 사유가 없을 경우 지체 없이 이용 중인 개인정보를 즉시 삭제하여야 하며, 서비스 이용자에게 제공된 개인정보가 완전하게 파기 되었는지, 향후 법률적 분쟁 발생 시 법률적 요구사항을 충족하도록 관리되고 있는지 보증할 수 있어야 한다.

우선 분야별 개별 법률에 의한 개인정보 보존연한이 상이하여 획일적으로 단일화된 보존 정책을 적용하기 어려우며, 빅 데이터 처리자는 정보주체와의

계약관계 종료 또는 이용자에게 제공되는 서비스가 종료된 이후에도 현행 개별 법률에 따라 개인정보를 보존하고 관리하여야 한다.[123]

<표 6> 법률에 의한 개인정보 보존 연한[124]

법률	내용	보존연한
신용정보의 이용 및 보호에 관한 법률	제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존) ② 신용정보회사등은 다음 각 호의 사항에 대한 기록을 3년간 보존하여야 한다. 1. 의뢰인의 주소와 성명 또는 정보제공·교환기관의 주소와 이름 2. 의뢰받은 업무 내용 및 의뢰받은날짜 등	3년
국세 기본법	제85조의3(장부 등의 비치와 보존) ② 제1항에 따른 장부 및 증거서류는 그 거래사실이 속하는 과세기간에 대한 해당 국세의 법정신고기한이 지난날부터 5년간 보존하여야한다. 다만, 제26조의2제1항 제5호에 해당하는 경우에는 같은 호에 규정한 날까지 보존하여야 한다.	5년
특정 금융거래정보의 보고 및 이용 등에 관한 법률	제4조(불법재산 등으로 의심되는 거래의 보고 등) ④ 금융회사등은 제1항 또는 제2항에 따라 보고를 하였을 때에는 대통령령으로 정하는 바에 따라 그 보고와 관련된 다음 각 호의 자료를 보고한 날부터 5년간 보존하여야 한다.	5년
통신비밀 보호법	제13조(범죄수사를 위한 통신사실 확인자료제공의 절차 ⑦ 전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장에게 통신사실 확인 자료를 제공한 때에는 자료제공현황 등을 연 2회 방송통신위원회에 보고하고, 당해 통신사실 확인자료 제공 사실등 필요한 사항을 기재한 대장과 통신사실 확인자료 제공요청서등 관련 자료를 통신사실 확인 자료를 제공한 날부터 7년간 비치하여야 한다.	7년
상법	제33조(상업장부등의 보존) ① 상인은 10년간 상업장부와 영업에 관한 중요서류를 보존하여야 한다. 다만, 전표 또는 이와 유사한 서류는 5년간 이를 보존하여야 한다.	5년
전자상거래등에	제6조(사업자가 보존하는 거래기록의 대상등) ① 법 제6조제3	6월-5년

123) Bruce Robertson, “Top Five Cloud‐Computing Adoption Inhibitors”, Gartner Research, ID Number. G00167920, May 2009.

124) 유우영/임종인, 클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구, 한국정보보호학회, 정보보호학회논문지 22(2), 2012.4, 342면.

서의 소비자보호에 관한 법률시행령	항의 규정에 의하여 사업자가 보존하여야할 거래기록의 대상·범위 및 기간은 다음 각 호와 같다. 다만, 통신판매중개자는 자신의 정보처리시스템을 통하여 처리한 기록의 범위내에서 다음 각 호의 거래기록을 보존하여야 한다. 1. 표시·광고에 관한 기록 : 6월 2. 계약 또는 청약철회 등에 관한 기록 : 5년 3. 대금결제 및 재화 등의 공급에 관한 기록 : 5년 4. 소비자의 불만 또는 분쟁처리에 관한 기록 : 3년	
정보통신망이용촉진 및 정보보호등에 관한법률시행령	제66조의8(거래기록의 보존기간 및 방법) ① 통신과금서비스제공자는 법 제58조제4항 및 제5항에 따라 다음 각 호의 사항에 관한 기록을 해당거래를 한 날부터 1년간 보존하여야한다. 다만, 건당 거래 금액이 1만원을 초과하는 거래인 경우에는 5년간 보존하여야 한다.	1년, 5년

다음으로 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다(「개인정보 보호법」 제21조). 이때 보유기간이란 동법 제15조 제2항 제3호의 “개인정보의 보유 기간”으로서, 개인정보의 수집에 대한 동의의 내용에 포함된 것으로 해석하여야 할 것이다. 그런데 앞서 살펴본 바와 같이 빅 데이터 처리에 의하여 개인정보가 생성되는 경우에는 수집에 따른 동의가 존재하지 아니하기 때문에 제15조 제2항 제3호의 “개인정보의 보유기간” 또한 존재하지 아니하게 된다. 그러나 제21조의 “보유기간의 경과”와 “개인정보의 처리 목적 달성”은 “개인정보가 불필요하게 되었을 때”의 예시라고 할 것이므로, 빅 데이터 처리를 통하여 생성된 개인정보가 불필요하게 된 때에는 지체 없이 그 개인정보를 파기하여야 한다. 또한, 제4조[125]는 정보주체의 권리의 하나로서 개인정보의 파기를 요구할 권리를 인정하고 있으므로, 빅 데이터 처리에 의하여 생성된 개인정보의 경우에도 이의 삭제를 정보주체가 요구하는 경우에는 빅 데이터 처리자는 이를 삭제하여야 할 것이

125) 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.
1. 개인정보의 처리에 관한 정보를 제공받을 권리
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리

다.

자. 국제협력(「개인정보 보호법」 제14조)

“정보의 집적, 정보의 결합, 정보의 분석”을 징표로 하는 빅 데이터는 데이터 소재지의 초공간성을 내용으로 하는 클라우드 컴퓨팅 환경과 어우러져 오프라인상 국내외로 산재되어 있는 개인에 관한 식별 또는 비식별 정보에 대한 정보의 결합을 내용으로 할 수 밖에 없다. 이와 관련하여 현행 「개인정보 보호법」 제14조 제1항은 “정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 한다”고 하고, 동조 제2항에서는 “정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다”고 하여 정부에 대한 시책 마련 의무만을 규정하고 있다.

생각건대, 빅 데이터와 클라우드 컴퓨팅에 의하여 물리적 경계를 초과하는 데이터의 이동과 결합이 범지구적으로 행하여지고 있고 그 점에서 동법 제14조 제1항에서 말하는 ‘국제적 환경에서의 개인정보 보호수준을 향상시키기 위하여’라는 요건을 구비된 것으로 보아야 한다. 따라서 정부로서는 빅 데이터에 의한 개인에 관한 식별 또는 비식별 정보의 집적과 결합을 통해 생성되게 되는 개인동의권을 벗어난 개인화나 개인정보의 오·남용 등에 대응하기에 필요한 시책을 마련하여야 하며, 이러한 시책으로는 기존의 개인정보에 대한 정보통제권(열람·정정·차단 및 삭제요구권) 이외에 빅 데이터 환경에 합당한 개인정보의 국외이전에 대한 개념의 법정화와 국내외에서 야기될 수 있는 개인정보의 오·남용에 대한 민·형사상의 준거법 결정문제 등에 대한 정부의 시책마련이 매우 중요하다고 할 것이다.[126)]

(1) 개인정보의 물리적 저장 위치

개인정보를 수집 이용하는 사업자가 빅데이터 서비스를 이용하여 이용자에게 서비스를 제공할 경우 이용자의 개인정보가 보관되는 데이터 보관의

126) 예컨대, 미국와 EU국가가 중심이 되어 2012년 현재 32개국이 비준한 “사이버범죄조약”을 우리도 비준하여 조약 비준국간에는 동일한 법위반에 대한 동일한 규범을 적용함으로써 정보주체의 권리를 보호하는 것이 그 예라고 하겠다.

지리적 위치의 다양성으로 인하여 개인정보보호와 관련된 법률적 이슈가 발생할 경우 서버 위치 중심의 법률적 관할권 결정이 어려울 수 있다. 개인정보 소유 주체인개인의 개인정보자기결정권을 보호하기 위한 조건을 갖추기 위하여 빅데이터 서비스를 제공하는 다국적 기업 또는 국가 간에 국제적 협력에 대한 문제가 발생할 가능성이 크다.[127]

(2) 개인정보의 국외 이전

개인정보의 국외 이전이란 개인정보가 국내에만 머물지 않고 해외에 위치한 서버에 저장되는 것으로서 이러한 경우 정보의 주체의 자기결정권의 보호와 내국인의 개인정보호보에 관한 심도 있는 정책적 고려가 필요하다고 할 것이다. 이에 우리 「개인정보 보호법」 제14조는 정부로 하여금 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련토록 하고 있으며, 특히 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하도록 규정하고 있다. 또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」[128] 제63조는 원칙적으로 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결을 금지하고 있다. 또한 정보통신서비스 제공자등은 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다. 이때 동의를 받기 위해 정보통선서비스 제공자는 이용자에게 ㉠ 이전되는 개인정보 항목, ㉡ 개인정보가 이전되는 국가, 이전일시 및 이전방법, ㉢ 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다), ㉣ 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간을 고지하여야 한다. 이를 통해 동의를 받아 개인정보를 국외로 이전하는 경우 정보통선서비스제공자 등은 ㉠ 개인정보보호를 위한 기술적·관리적 조치, ㉡ 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항, ㉢ 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치를 하여야 한다. 또한 정보통신서비스 제공자등은 이러한 보호조치의 사항을 개인정보를

127) Bruce Robertson, “Top Five Cloud‐Computing Adoption Inhibitors”, Gartner Research, ID Number. G00167920, May 2009; 이창범, “클라우드컴퓨팅 활성화를 위한 법제도 개선방안 연구”, 한국인터넷진흥원 연구보고서, 2010; 유우영/임종인, 전게논문, 341면.

128) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」[법률 제11048호, 2011.9.15]

국외에서 이전받는 자와 미리 협의하고, 이를 계약내용 등에 반영하여야 한다.[129]

차. 영향평가

'개인정보 영향평가'(PIA, Privacy Impact Assessment)란 개인정보 수집·활용이 수반되는 사업 추진시 개인정보 오남용으로 인한 프라이버시 침해 위험이 잠재되어 있지 않는지를 조사·예측·검토하고 개선하는 제도이다. 개인정보 영향평가제도의 목적은 평가대상 시스템 활용에 따른 잠재적 위험을 평가하여 개인정보 침해에 따른 피해를 줄일 수 있는지를 미리 검토·반영하는 것이다.[130] 2012년 General Data Protection Regulation 안[131]은 일정한 경우[132]에 개인정보 영향평가를 실시하도록 하는 규정을 포함하고 있다.

개인정보 영향평가를 규정하고 있는 「개인정보 보호법」 제33조는 일정한 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가

129) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」[대통령령 제24102호, 2012.9.14]

130) 행정안전부, 「개인정보 보호법령 및 지침·고시 해설」, 2011, 255~256면

131) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

132) Article 33 Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1:
   (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;
   (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
   (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;
   (d) personal data in large scale filing systems on children, genetic data orbiometric data;
   (e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).
3. ~ 7. (생 략)

를 하도록 의무화하고 있지만, 의무적 영향평가 시행대상은 공공기관으로 제한된다. 그 외의 개인정보처리자에 대해서는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 영향평가를 하기 위한 노력만을 규정하고 있을 뿐이다. 그러나 빅 데이터 환경에서 방대한 양의 데이터가 데이터 마이닝이나 프로파일링 등 다양한 분석과정을 거치면 특정개인의 식별성 뿐만 아니라 많은 수의 개인에 대한 식별과 속성, 성향 등 다면적·심층적 정보의 가공이 가능하다는 위험성을 고려할 때, 일정한 요건의 빅 데이터 처리에 대한 개인정보 영향평가제 도입을 검토할 필요가 있다.

Ⅲ. 개인정보 보호법의 개선방안

1. 개인정보보호법제의 패러다임 전환

개인정보보호법제를 선도했던 EU의 최근 입법 동향과 미국의 법정책 동향을 살펴보면, 과거보다 상대적으로 서로의 관점을 채택하는 경향으로 보인다. 즉, EU의 경우에는 보호를 주된 관심사로 두었던 입장으로부터 글로벌 시장에서의 개인정보의 유통의 불가피성을 고려하여 '안전한 활용'을 위한 개인정보보호의 관점으로 보호와 유통의 조화를 꾀하려는 입장으로 미세하지만 변화되었던 것으로 보인다. 반면, 미국도 정보의 집적과 그로 인한 국민에 대한 침해 가능성을 고려하고 EU를 비롯한 각국의 프라이버시 관심사가 증대함에 따라 개인정보 '보호'의 관점을 법제화하려는 시도가 나타나고 있으며, 특히 소비자의 개인정보보호나 프라이버시보호라는 관점에 초점을 맞추고 있다. 이처럼 개인정보에 대한 극명한 대비를 이루었던 EU와 미국도 개인정보의 '보호'와 '활용'에 대한 서로의 관점을 점진적으로 수용해가고 있는 것으로 볼 수 있고, 현대의 스마트 빅데이터 시대의 불가피한 방향으로 보인다. 반면, 우리의 개인정보 보호법은 1995년 EU 개인정보보호지침을 모델로 하여 각국의 입법례와 우리나라의 법인식을 바탕으로 제정된 것으로 평가할 수 있는데, 2012년 발표된 EU의 새로운 규정(안)이나 지침(안)의 입장과 미국의 개인정보보호 법정책 동향의 최신 관점이 충분히 고려되지 못

한 면이 있는 것으로 보인다. 또한 이 글에서 살펴본 것처럼 일정한 부작용이 존재할 지도 모르지만 현재 무역기반의 경제를 가지고 있는 우리나라에서의 글로벌 관점의 법제의 구축과 스마트 빅데이터 환경의 전개에 따른 경제적 파급효과와 부작용을 최소화하여 국민의 권리를 보호할 필요성 등을 종합적으로 고려할 때 기본적인 입장은 국민의 개인정보의 보호에 있지만 적정 수준의 규제를 통하여 '안전한 활용'을 도모하는 것도 매우 중요하다. 결론적으로 강력한 처벌규정과 함께 광범위한 규제로 작용하고 있는 '보호' 중심의 현행 개인정보 보호법을 개인정보에 대한 보호와 활용의 적정한 조화, 특히 안전한 활용을 촉진할 수 있는 방향으로 법제를 개선해 나가는 것이 무엇보다도 중요하다고 하겠다. 다만, 글로벌 스탠다드와의 조화를 꾀하는 과정에서 유의할 점은 해외의 개인정보보호법제 전체를 검토하여 전체적 맥락에서 개별 규정들이 보호를 강화하는 것인지 완화하는 것인지에 대한 균형잡힌 검토를 바탕으로 국내 법제와의 입체적 비교를 통하여 우리에게 적합한 개선안을 도출해야 한다는 점이다.

2. 개인정보 개념 정의 개선

빅 데이터로 인하여 개인정보가 침해되는 일은 없어야 할 것이지만, 개인정보 보호에 치중한 나머지 개인정보의 범위를 지나치게 넓고 강력하게 보호하여 빅 데이터 등 관련 산업의 발전을 저해하여서도 안 된다. 빅 데이터의 성공여부는 바로 '개인정보 보호법 제2조 제1호 중 괄호에 해당하는 정보를 얼마나 많이 수집·분석할 수 있느냐'에 달려있다고 해도 과언이 아니다. 그러나 현행법의 해석으로는 부진정 개인정보(또는 쪽 개인정보)를 정보주체의 동의 없이 수집·제공하기만 하여도 과태료나 형사처벌을 받을 수 있는 상황이다. 실무적으로도 개인정보 개념과 범위의 모호성, 괄호에서 말하는 용이한 결합가능성의 의미·판단기준·판단주체에 관하여 소관부처·사정당국·학계·법조계 사이의 견해가 일치하지 아니한 상태이다.

이러한 점을 고려하여 개인정보의 개념정의에 대한 개선방안에 대하여는 두 가지 방향을 상정할 수 있다. 제1안은 개인정보의 개념정의를 대폭 확대하는 방안이다. 이는 개인정보보호법의 제정 취지가 개인정보보호의 사각지대를

제거한다는 점을 기초로 새롭게 제기되거나 현행 법률이 미처 예상하지 못했던 프로파일링을 기초로 한 빅데이터에 대한 효과적 규율이 어렵기 때문에 개인정보의 개념을 확대하여야 한다는 입장이다. 이는 최근 EU 일반정보보호규정(안)의 입장과 흐름을 같이 한다. 즉, EU 일반정보보호규정(안)은 정보주체와 관련된 모든 정보(information)[133]이라고 하여 개인정보의 범위를 매우 넓혔고, 식별성 요건은 정보주체의 정의로 이동하였다. 다만, EU 일반정보보호규정(안)은 과징금 외에 형사벌을 규정하고 있지 않고, 형사벌은 각국의 국내법에 맡기고 있다는 점에서 주의하여야 한다. 만일 제1안에 따라 개인정보의 개념정의를 확대한다면, 형사처벌과의 관계에서 형사처벌 대상을 제한하여 불필요한 처벌의 확대를 막아야 한다. 반면 제2안은 현행 개인정보의 정의가 너무 넓고 이와 연동되는 형사처벌의 대상이 너무 광범위하여 일반 국민을 잠재적 범죄자로 만들 수 있다는 비판을 고려하여, 개인정보보호법의 적용범위를 제한할 필요가 있다는 점을 근거로 한다. 이에 의하면 해당 정보만으로 개인을 직접 식별할 수 있는 것만을 개인정보로 본다. 이 입장에 따르면 형사처벌 규정에 대한 개정은 불필요하거나 개정이 필요한 범위가 제한적이다.

국민과 기업의 예측가능성과 법적안정성을 보장하고, 빅 데이터 산업의 육성을 위해서라도 법개정을 통해 괄호 부분을 삭제할 필요가 있다고 판단되는 바 이에 관한 심도있는 논의를 거쳐 개정방향을 정하여야 한다.

3. 프로파일링 거부권 선언 및 고지 의무의 신설

빅데이터의 가장 심각한 문제의 하나는 무수히 많은 데이터로부터 조합된 개인에 관한 새로운 정보의 생성과 취득으로부터 자칫 편향되거나 잘못된 개인의 평가가 이루어질 수 있고, 그에 따라 잘못된 영향을 미칠 수 있다는 점이다. 그런데 이는 실제 빅데이터의 운용 과정에서 어느 정도의 깊이와 세밀함으로 분석과 평가가 이루어지는가에 따라 그 부정적 영향의 정도에 큰 차이를 나타낼 수 밖에 없다. 때문에 이를 일률적으로 제한하거나 억제할 수

133) 기본 용어로는 개인정보(personal data)라고 하였지만, 그 정의에서는 개인과 관련한 모든 정보(information)라고 하여 처리가능한 데이터가 아닌 포괄적으로 정보를 의미하는 것으로 규정함으로써 규정(안)의 적용대상을 확장하고 있다.

는 없고, 다만 정보주체가 그러한 프로파일링을 통하여 본인에게 미칠 수 있는 악영향에 대한 고지를 받을 수 있도록 개인정보처리자에게 고지의무를 신설하고, 아울러 이를 반대하는 정보주체에게 프로파일링 거부권 인정하는 방향으로 법제의 개선이 필요하다. 이처럼 프로파일링 거부권을 인정하는 방향으로 개정하는 경우에는 실질적으로 개인정보처리자가 프로파일링 거부권과 제공하는 서비스의 해지나 탈퇴를 연동시킬 가능성이 매우 높다. 이는 프로파일링 거부권을 형해화시킬 수 있다. 이를 막기 위하여 프로파일링 거부권 행사에도 불구하고 기본적인 서비스의 제공은 계속되도록 개인정보처리자에게 의무를 부과하는 방안도 고려해볼 수는 있다. 그런데 이는 특히 영리목적의 개인정보처리자가 주로 프로파일링을 마케팅이나 신규서비스의 개발목적으로 사용하는 경우가 많은데, 프로파일링 거부권을 강력하게 보장함으로써 개인정보처리자의 영업의 자유를 과도하게 제한함으로써 헌법상 보장된 권리를 제한하는 결과로 귀결될 위험성도 있다. 따라서 프로파일링 거부권을 명문으로 규정하더라도 프로파일링 거부권 행상 대한 합리적인 예외를 설정하는 것이 필요하다.

4. 개인정보처리자에 대한 단계적 규제

개인정보 보호법은 시정조치(제64조), 벌칙(제70조부터 제73조), 과태료(제75조)에 따라 개인정보처리자의 법 준수를 강제하고 있는데, 개인정보 보호법상의 각종 의무 규정들이 침해의 정도나 가벌성 등을 고려하지 않고 포괄적으로 규정되어 있어서 벌칙 규정을 형식 논리에 따라 엄격하게 적용하는 경우에는 자칫 과도한 규제가 이루어질 수 있으며, 전국민을 잠재적인 법위반자로 만들 우려도 없지 않다. 또한 벌칙의 대상이 되는 위법행위의 경우에 즉시 형벌을 과하기보다는 개인정보처리자가 가능한 법을 준수할 수 있도록 유도하는 단계적 처벌 규정을 두고, 위법행위로 인한 개인정보처리자의 이익을 제거하여 위법행위를 예방하기 위한 실효성 있는 조치로서 과징금 제도를 도입할 필요가 있다. 결론적으로 시정권고 또는 시정명령 – 과태료 또는 과징금 – 형사처벌의 단계를 원칙으로 하고, 불가피하거나 가벌성이 높은 경우에만 예외적으로 형사처벌을 인정하는 것이 바람직하다.

5. EU 국외이전 규범과의 정합성 강화

가. 추진방향

(1) 한-EU간 Safe Harbor 협약 체결방법

국가차원에서 한국 및 EU간 Safe Harbor 협약을 체결하게 되면 국내기업은 Safe Harbor 기준을 충족하였다고 신고만 하면 EU법의 적용을 면제받는 것이다. 간단한 절차이고, 그 절차에 소요되는 시간이 적어진다는 점에서 가장 유리한 제도이지만, EU와 이러한 협약을 체결한 국가는 현재 미국이 유일하다. 따라서 EU가 우리나라가 Safe Harbor 조약을 체결할 가능성은 높지 않아 보인다.

(2) 개인정보보호작업반 심사를 거쳐 국가 차원의 승인방법

EU지침 제29조에 의하여 설치된 개인정보보호작업반(Article 29 Data Protection Working Party: 이하 "개인정보보호작업반"이라 함)의 승인을 받는 방식이다. 신청국가가 EU에 승인을 신청하면 개인정보보호작업반의 심사를 거쳐 승인을 받는 방식이다. 개인정보보호작업반은 신청국가가 개인정보를 '적절한 수준(adequate level)'으로 보호하고 있는지 심사하여 결과를 EU에 권고하면 EU가 그 승인여부를 결정하게 되는데, 심사시 신청국가의 국내법과 EU 정보보호법을 비교 평가하게 된다. 국가가 EU 산하 개인정보보호작업반 심사를 거치고 국가차원에서 승인을 받게 되면 국내 정보보호법을 준수할 때 EU로부터 개인정보를 가져오는 것이 허용된다는 것이다. 개인정보보호작업반심사를 통해 승인 받은 국가로는 아르헨티나, 오스트레일리아, 캐나다, 이스라엘, 스위스 등이 있다.

나. 적합성평가기준

우리나라에서는 현재 개인정보 보호법이 시행되고 있고, 위의 개선방향 중 개인정보보호작업반심사를 받는 방향으로 대비해야 할 것이다. Safe Harbor 협약은 유리하기는 하지만 체결가능성이 낮고, 체결까지 걸리는 시간이 지나치게 오래 걸리는 단점이 있기 때문이다.

개인정보보호작업반에서는 1998년 7월 24일 'EU 개인정보보호지침 제25조 및 제26조의 적용에 따른 제3국에 대한 개인정보의 이전'이라고 하는 실무작업보고서(working document)를 작성하였다. 동 지침에 의하면 EU에서는 위에서 본 1980년의 OECD 가이드라인에서 정한 개인정보보호 8원칙을 반영하여 다음과 같은 원칙을 정하였다.

① 목적 제한(purpose limitation)의 원칙: 개인정보는 특정 목적을 위하여 처리되고 이용되며, 이전 목적에 반하지 않는 한 유통될 수 있다.

② 정보의 질, 비례(data quality and proportionality)의 원칙: 정보는 정확하여야 하며 필요하면 갱신되어야 한다. 정보는 이전·처리의 목적과 관련하여 적절하고 과도하지 않아야 한다.

③ 투명성(transparency)의 원칙: 개인은 정보가 처리되는 목적과 제3국에서 당해 정보를 관리하는 주체, 기타 공정성을 확보할 수 있는 정보를 알 수 있어야 한다. 유일한 예외는 EU지침 제11조 2항과 제13조에 규정되어 있다.

④ 안전성(security)의 원칙: 정보를 관리하는 자는 정보처리상의 위험에 비추어 적당한 기술적 및 관리적 보안조치를 취하여야 한다. 그의 감독 하에 정보를 취급하는 자도 정보관리자의 지시를 따라야 한다.

⑤ 열람·정정·거부(rights of access, rectification and opposition)의 권리: 정보의 주체는 그에 관한 모든 정보를 열람할 수 있어야 하며, 부정확한 정보는 이를 정정하고, 일정한 경우에는 그에 관한 정보의 처리를 거절할 수 있어야 한다.

⑥ 정보이전의 제한(restrictions on onward transfers): 개인정보를 수령한 자가 이를 다시 전송하고자 할 때에는 제2의 정보수령자가 적절한 수준으로 이루어지는 개인정보보호의 규정의 적용을 받고 있어야 한다. 유일한 예외는 지침 제26조 제1항에 규정되어 있다.

EU는 위의 원칙에 추가하여 현실적으로 문제가 자주 일어나는 민감한 정보, 불특정 다수의 잠재고객에 대한 다이렉트 마케팅(DM), 그리고 컴퓨터에 의하여 자동적으로 정보이전이 정해지는 경우에 대비하여 다음과 같은 원칙을 보완하였다.

① 민감한 정보(sensitive data): 인종·정치사상·신조·건강 등 민감한 정보에 대하여는 정보주체의 명시적인 동의를 요하는 등 추가적인 보호장치가 있어야 한다.

② 다이렉트 마케팅(direct marketing): DM 목적으로 정보를 처리하는 경우에는 정보주체가 언제든지 자신의 정보를 제외시킬 수 있어야 한다.

③ 자동적인 결정(automated individual decision): 정보이전의 목적이 자동적인 결정으로 이루어지는 경우 개인은 이러한 결정의 로직을 알아야 하며 개인의 이익을 보호하기 위한 다른 조치가 취해져야 한다.

EU는 아울러 정보주체의 권리행사와 구제를 위하여 다음 세 가지의 절차 및 집행요건도 마련하였다.

① 정보주체가 자신의 권리와 행사방법을 잘 알고, 정보처리자가 개인정보보호규정을 충분히 지킬 수 있어야 하며, 위반시의 제재수단이 잘 갖추어져 있을 것

② 정보주체가 자신의 권리를 행사함에 있어 관련기관·단체로부터 지원 및 조력을 받을 수 있을 것

③ 보호규정 위반시에는 피해자에게 독립적인 분쟁해결 또는 중재 시스템 등 적절한 구제수단이 제공될 것

6. 국외이전 관련 자율규제 유도 방안

글로벌 빅데이터 시대에서 우리나라가 글로벌 경쟁력을 강화하면서도 개인정보에 대한 적정한 보호수준을 유지하기 위해서는 국외이전에 대한 특별한 규제를 강화하는 것보다는 국외이전에 대한 자율적인 규제를 유도하여 글로벌 스탠다드를 정립하고 실행해 가는 것이 훨씬 빠르고 현실적인 방안이 될

것이다. EU의 경우에는 자율규제 유도의 일환으로 적합성평가의 적합성 충족기준으로서 BCR(Binding Corporate Rule)을 승인하고 있는데,[134] 이는 기업 측의 자율적인 규제에 법적 효과를 부여하여 개인정보의 국가간 유통을 허용하는 것이다.

이상과 같은 자율규제의 유도를 위하여 국내 개인정보처리자가 국외로 개인정보를 이전하고자 하는 경우에 그 적정성을 스스로 판단할 수 있도록 민간 자율 혹은 정부와의 협력에 의하여 사전에 준비된 자율평가표를 작성토록 하고, 이를 정보주체가 열람할 수 있도록 공개하도록 공동규제체계를 정립할 필요가 있다. 또한 EU의 일반정보보호규정(안)과 같이 일정한 요건을 갖춘 BCRs에 대하여 법준수와 동일한 효과를 인정하는 방안도 인정할 필요가 있다. 이는 특히 개인정보 보호법의 형식적 엄격성을 완화하는 데에도 도움이 될 것이다.

7. 인증제 개선

개인정보 보호법 제2조 제1항 제1호의 괄호부분을 삭제하거나 계속 보관의 근거를 마련함으로서 빅 데이터 발전을 위한 최소한의 기반을 마련하더라도, 개인정보 보호를 위하여 단계별로 익명성을 보장해 줄 수 있는 제도적·기술적 장치를 마련할 필요가 있다. 현행 개인정보 보호법이나 정보통신망법에 따르더라도 통계 등의 목적을 위하여 익명화된 정보의 경우에는 개인정보로 보지 않고 있다. 이를 위한 방법으로 일반인이 안심할 수 있도록 빅 데이터를 활용하는 기업의 개인정보 관리 수준을 검증하는 '개인정보보호관리체계(PIMS)' 인증제를 개선하는 방안을 검토할 필요가 있다.

8. 분리보관의무 명시

주요 개인정보파일의 분리보관의무(Separation Principle)를 명시하여 주민번호 등 고유식별정보나 민감정보, 금융정보 등 중요 개인정보파일에 대한 분리보관의무를 명시할 필요가 있고, 개인정보파일과 다른 정보와의 결합가

134) 최경진, 전게 "개인정보 국외이전에 관한 합리적인 법제 개선방안", 55-75면 참조.

능성에 대한 고지의무를 명시할 필요가 있다.

9. 개인정보 보유기간제도 개선

앞서 본 바와 같이 개인정보 보호법이나 정보통신망법은 개인정보의 보유기간경과, 보유 목적 달성 등의 경우에 있어서 즉시 파기를 규정하고 있고(개인정보 보호법 제21조, 정보통신망법 제29조), 위반시 과태료를 부과하도록 하고 있는데(개인정보 보호법 제75조 제2항 제4호, 정보통신망법 제76조 제1항 제4호), 이는 대량의 데이터를 수집·분석하여 유의미한 정보를 도출함을 목적으로 하는 빅 데이터의 특성과 상치되는 것이다(빅 데이터 활용을 고려하여 보유기간 중 익명화 조치를 하여 별도로 보유하고 있다면 모르겠으나, 보존기간 경과 후 익명화를 하는 경우에는 규범적으로 법위반 상태가 발생할 수밖에 없다).

개인정보 보호법은 제21조 제1항 단서에서 “다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.”라는 예외규정을 마련하고 있고, 제3항에서 “개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.”라고 규정하고 있다. 그러나 현행법상으로는 빅 데이터와 관련하여 개인정보의 보존을 허용하는 법률이 현재는 마련되어 있지 않고,[135] 같은 조 제3항 역시 제1항 단서에 따라 법령에 근거하여 계속 보존하는 경우를 전제하므로 빅 데이터를 위한 데이터의 계속 보존의 근거가 될 수 없다.

향후 개인정보 보호법을 개정하여 법령의 근거가 없더라도 익명화 조치를 취할 경우 계속 보존할 수 있도록 하거나, 빅 데이터 육성을 위한 법령을 제정함으로써 문제를 해결해야 할 것으로 보인다.

10. 거버넌스의 체계적 일원화

135) 최근 미국과 EU는 항공기 이용승객 정보에 관한 보존 협의를 통해, 미국 국토안보부는 수집한 승객의 정보를 여행 6개월 뒤 익명화하여 5년간 보관하고, 휴면데이터베이스로 옮겨 10년 간 더 보관하는 방안을 협의하고 있다.

빅데이터 시대의 개인정보는 더 이상 특정 영역에만 머물러 있는 것이 아니라 온라인, 오프라인, 금융, 의료, 국내, 해외 등 다양한 분야에 걸쳐서 동일한 정보주체에 대한 개인정보보호의 문제가 야기된다. 또한 EU의 적합성 평가를 추진하는 때에도 장애가 될 수 있는 절차적 측면에서의 문제 즉, 독립된 감독기구의 요건을 충족하기 위해서도 거버넌스의 체계적 일원화가 요구된다. 따라서 개인정보보호에 대한 일원화된 규제체계를 정립할 필요가 있다. 이 때 어느 정도까지 규제권한을 집중할 것인가에 대하여는 논의가 필요하지만, 설령 분야별 특수성을 고려한 법규범의 운용과 각 분야별 규제체계는 유지한다고 하더라도 적어도 정보주체가 개인정보 피해로부터 사전적 예방 또는 사후 구제를 받는데 일원화된 체계를 활용하여 국내외적인 대응을 할 수 있도록 하는 것이 필요하다.

제5장 결 론

정보화 사회에서의 정보가치는 자료나 단편정보가 아니라 그것들을 모아 놓은 데이터베이스 안에 숨어 있는 정보가 더 큰 가치를 가진다. 수많은 자료와 단편정보들이 많으면 많을수록 융합분석 결과정보에 대한 확률적 신뢰성이 커진다. 세계 각국은 빅 데이터의 활용성을 인지하여 육성 계획을 경쟁적으로 발표하고 있다. 우리나라도 빅 데이터에 대한 관심과 수요가 점차 늘어나고 있고 빅 데이터와 관련된 정보통신 기반 역시 세계에서 유래를 찾아볼 수 없을 정도로 갖춰져 있으나 관련 인력의 부족, 입법적·행정적 조치의 미비로 인하여 그 발전 속도가 매우 더디다. 또한 세계에서 유래를 찾아 볼 수 없는 강력한 개인정보 보호 법령으로 말미암아 빅 데이터를 활용하려는 정부나 기업은 위법의 위험을 감수해야 한다.

빅 데이터는 하나의 공공서비스이자 산업으로 거스를 수 없는 세계적 추세가 되었을 뿐 아니라 빠른 속도로 발전하고 있다. 기술의 발전화 현실적 필요성을 고려하지 않은 입법과 행정조치는 국가와 사회의 발전에 저해가 될 뿐이다. 어떤 제도나 기술이 항상 효용만 있을 수는 없다. 우리에게 남겨진 과제는 그것이 궁극적으로 국민의 권익 향상에 합하는 것인지 판단하고 어떻게 하면 효용을 높이고 부작용을 줄이는 것이냐를 고민하여 해결책을 찾는 것이다.

법과 기술의 괴리, 법과 현실의 괴리가 점점 커질수록 그로 인한 피해는 고스란히 국민의 몫이 된다. 따라서 환경변화에 대응하면서도 국민의 권익을 보호하고 개인정보처리자의 활동을 최대한 보장할 수 있는 균형 잡힌 법제도의 구축이 절실하다.

참고문헌

1. 국내문헌

윤미림, “빅데이터 비즈니스 활용과 과제” 한국정보산업연합회 Issue Report, 2012

이용수, “스마트혁명 시대 빅데이터 활용과 프라이버시 사이의 충돌에 관한 연구”, 경원대학교 소프트웨어대학원, 2011

안창원/황승구, 빅 데이터 기술과 주요 이슈, 정보과학회지, 제30권 제6호, 2011

강만모/박상무/김상락, 빅 데이터가 여는 미래의 세상, 한국정보과학회, 정보과학회지 제30권 제6호, 2012.6

이명진/김우주, 빅 데이터를 위한 고급분석 기법과 지원 기술, Entrue Journal of Information Technology, 제11권 제1호, 2012

정병권 외 2명, "미래사회와 빅 데이터(Big data) 기술", IT기획시리즈, 정보통신산업진흥원, (2012년)

조성우, “Big Data 시대의 기술”, KT종합기술원, (2011년 10월 05일)

한국인터넷진흥원, 「민간 기업의 빅데이터 도입 증가 추세 – 관련 전문가 부족이 빅테이터 활용의 최대 장벽」, 주간 인터넷 동향, 2012. 9.

장영재, 「아마존닷컴, 현대의 서점 아저씨」(2012년), 비즈니스북스

박대하/백태석, 클라우드 컴퓨팅 개인정보보호 연구동향과 과제, 한국정보보호학회, 정보보호학회지 21(5), 2011.8.

신덕호, 유비쿼터스 컴퓨팅 환경에서의 개인정보보호정책 발전에 관한 연구, 단국대학교 석사학위논문, 2009

한국인터넷진흥원, 개인정보 국외이전 관련 법률정비 방안 연구(2012.11.)

최경진, 잊혀질 권리 – 개인정보 관점에서, 정보법학 제16권제2호(2012)

최경진, “개인정보 국외이전에 관한 합리적인 법제 개선방안”, 개인정보보호 법제정비 연구포럼 토론회(201212.7.) 자료집

이광현, 국경간 개인정보 이전과 보호 : EU와 영국, 미국의 사례를 중심으로, 선진상사법률연구, 제50호, 2010

한국인터넷법학회, 개인정보 보호와 적정 활용의 조화를 위한 제도 도입 연구, 법제처, 2009
권녕성, 헌법학원론, 법문사, 2007
김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 공법연구, 제29집제3호
이인호, "정보사회와 개인정보자기결정권", 중앙법학 창간호, 1999
한위수, "사생활비밀의 보호 - 그 공법적 측면"(한국법학원 2003. 12. 8. 개최 심포지엄, "사생활비밀의 보호" 발표논문)
성낙인, 「헌법학」, 법문사 제7판
정종섭, 「헌법학원론(제2판)」, 박영사, 2007
정영화, "인터넷상 개인정보유통의 오남용에 관한 법제연구", 「인터넷·언론·법」, 한국법제연구원, 2002
행정안전부,「개인정보 보호법령 및 지침·고시 해설」, 2011

2. 국외문헌

Global Agenda Council on Emerging Technologies, << The top 10 emerging technologies for 2012 >>, World Economic Forum, Feb 15th 2012.
James et. al., Big data: The next frontier for innovation, competition and productivity, McKinsey & Company, 2011
John Gantz & David Reinsel, << Extracting Value from Chaos >>, IDC IVIEW June, 2011
Richard et. al., Big Data: What It Is and Why You Should Care, IDC, June 2011
James Manyika & Michael Chui, “Big data: The next frontier for innovation, competition, and productivity”, McKinsey Global Institute, (2011.05)
Doug Laney, “3D Data Management: Controlling Data Volume”, Velocity, and Variety, Gartner, February 2001

Paul C. Zikopoulos, Chris Eaton, Dirk deRoos, Tom Deutsch, and George Lapis, “Understanding Big Data”, Paul Zikopoulos, 2012

Oracle, “Oracle: Big Data for the Enterprise”, Oracle White Paper, January 2012

Jane Winn, "Intensification of Personal Information Protection by the Development of Big Data and SNS in the USA", "2101 International Conference on Recent Trend of Personal Information Protection", 2012.11.1.

James G. Kobielus, Connie Moore, Brian Hopkins, and Shannon Coyne, “Enterprise Hadoop: The Emerging Core Of Big Data”, Forrester, October 2011

Smedinghoff. T. J., 「Online law the SPAs legal guide to doing business on the internet」, The Software Publishers Association, 1996

船越一行, 「情報とプライシーの權利」, 北樹出版, 2001

藤原靜雄, 「逐條個人情報保護法」, 弘文堂, 平成 15年