지역법제 연구 14-16-⑦-2

# 빅데이터법제에 관한 비교법적 연구

## -미국-

임지봉

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

지역법제 연구 14-16-⑦-2

# 빅데이터법제에 관한 비교법적 연구
## - 미 국 -

임 지 봉

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

# 빅데이터법제에 관한 비교법적 연구

## - 미 국 -

# A Comparative Law study on the Legislation of Big Data

## - United States of America -

연구자 : 임지봉(서강대 법학전문대학원 교수)
Lim, Ji-Bong

2014. 10. 31.

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

# 요 약 문

## Ⅰ. 배경 및 목적

### □ 빅데이터 기술의 의의

○ 컴퓨터시대의 초기단계에서부터 공적 주체와 사적 주체들은 사람들에 대한 디지털 정보를 모아왔다. 컴퓨터 기술이 발전하면 할수록 더 많은 정보들이 디지털의 형태로 축적되어 사업용으로 활용되었다. 예를 들어 디지털 전화카드, 신용카드 거래 기록, 은행 계좌 기록, 이메일 보관함 등이 그것이다. 이러한 디지털 정보들을 모아 대량으로 모아 정보분석을 통해 유의미한 경향을 읽어내는 것이 빅데이터 기술이다.

### □ 연구의 목적

○ 본 연구에서는 미국에서의 빅데이터 활용과 그 정책 및 법제에 대해 살펴보고 빅데이터의 무분별한 사용이 불러올 수 있는 개인정보 침해를 위해 개인정보 보호 관련 정책 및 법제들을 살펴봄을 연구의 목적으로 한다. 이는 우리나라가 앞으로 빅데이터 활용 정책과 법제를 만듦에 있어 타산지석으로 삼고자 하는 것이다. 본 연구의 방법은 빅데이터와 개인정보 보호에 관한 미국의 정책 및 법제들, 그리고 이것들을 분석해놓은 단행본, 보고서, 논문들에 대한 문헌조사를 주된 연구의 방법으로 한다.

## Ⅱ. 주요 내용

□ 미국에서의 빅데이터 활용과 정책 및 법제

○ 빅데이터 '활용'과 관련한 정책 및 법제로는 지식행동화 데이터, 빅데이터 연구와 개발 이니셔티브, 개방형의 표준화된 정부 정보 채택 행정명령, 정부 데이터 개방 실행계획가 있다.

□ 미국에서의 빅데이터 규제와 정책 및 법제

○ 빅데이터의 '규제'와 관련한 정책 및 법제로는 빅데이터 정보환경에서 개인정보의 침해 위험, 온라인 프라이버시 프레임워크, 소비자 프라이버시 권고, 빅데이터와 프라이버시 워킹 그룹 권고, 과학기술자문위원회 권고가 있다.

□ 미국에서의 개인정보 보호 관련 법제

○ 연방프라이버시법을 위시한 공공부문에서의 개인정보 보호 입법과 사적 부문에서의 개인정보 보호입법으로 나누어 살펴본다. 그리고 개인정보 보호와 관련한 세이프하버원칙과 자율규제론에 대해서도 검토해 본다.

□ 빅데이터의 활용과 개인정보 보호의 조화를 위한 미국의 노력

○ 최근 미국에서 이루어지고 있는 빅데이터 기술의 활용과 개인정보 보호의 조화를 도모하기 위한 노력들을 연방거래위원회의 개인정보 보호를 위한 보고서와 오바마 정부의 소비자 프라이버시 권리장전을 중심으로 살펴본다.

## Ⅲ. 기대효과

○ 미국의 경험과 그 경험을 통해 만들어진 정책과 법제에 대한 연구를 통해 우리나라가 앞으로 빅데이터 활용 정책과 법제를 만듦에 있어 많은 시사점을 얻을 수 있을 것이다.

주제어 : 빅데이터, 개인정보, 프라이버시 보호, 연방프라이버시법, 프라이버시 영향평가제도, 세이프하버원칙, 온라인 프라이버시

# Abstract

## Ⅰ. Background and objective

□ Background

○ Since early in the computer age, public and private entities have assembled digital information about people. As computing power increased, more and more business applications turned into digital forms. Big-data was born by the development of the digital technology

□ Objective

○ This study aims at examining the laws and policies in the United States to develop and regulate the big-data technology. In addition, it also studies the laws and policies in the United States to protect the personal data as the limit of big-data use.

## Ⅱ. Contents

□ Laws and Policies in the United States to develop the big-data technology

□ laws and policies in the United States to develop and regulate the big-data technology

□ laws and policies in the United States to protect the personal data as the limit of big-data use

□ Efforts by the United States to harmonize the use of big-data skill with the privacy rights

## Ⅲ. Expectation

□ By studying the laws and polices of the United States enacted from the experiences on the big-data, we can get lessons in enacting korean laws and polices on the big-data regulation.

Key Words : Big-data, Personal Data, Privacy Protection, Federal Privacy Act, Privacy Impact Assessment, Safe Harbor Principles, On-line Privacy

# 목 차

# 제 1 장 서 론

컴퓨터시대의 초기단계에서부터 공적 주체와 사적 주체들은 사람들에 대한 디지털 정보를 모아왔다. 컴퓨터 기술이 발전하면 할수록 더 많은 정보들이 디지털의 형태로 축적되어 사업용으로 활용되었다. 예를 들어 디지털 전화카드, 신용카드 거래 기록, 은행 계좌 기록, 이메일 보관함 등이 그것이다. 이러한 디지털 정보들을 모아 대량으로 모아 정보분석을 통해 유의미한 경향을 읽어내는 것이 빅데이터 기술이다.[1)]

바야흐로 세계 여러나라들은 빅데이터의 높은 활용성을 인지하기 시작했다. 그리고 빅데이터에 대한 육성계획을 앞다투어 발표하고 있다. 우리나라에서도 이러한 빅데이터에 대한 관심이 늘고 수요가 증가하고 있다. 특히 우리나라는 빅데티어 활용을 가능케 하는 정보통신 기반이 세계 어느 나라보다도 잘 갖추어져 있지만, 빅데이터 관련 인력의 부족과 행정적·입법적인 불비로 빅데이터의 활용 속도가 턱없이 느린 편이다. 또한 우리나라는 세계 어느 나라보다도 강력한 개인정보 보호법령을 갖고 있어 빅데이터 활용을 원하는 기업이나 정부에게 적지 않은 걸림돌로 작용하고 있다.

미래창조과학부는 2013년 12월 11일에 ICT분야의 새로운 패러다임으로 국가사회 경쟁력 향상의 원동력으로 급부상 중인 빅데이터의 각계 활용을 촉진하고 관련 사업을 육성하기 위한 빅데이터 산업 발전 전략을 관계 부처 합동으로 발표하였다.[2)] 빅데이터의 활용은 앞으로 효율적인 마케팅 전략을 세움에 있어 중요하게 사용되어질 것이고 따라서 산업발전과 경제적 도약의 굳건한 발판이 될 것으로 예상된다.

---

1) Executive Office of the President & President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective,* May 2014, p.19

2) 정필운, "미국의 빅데이터 정책 및 법제", 『빅데이터 법제 제1차 워크숍 자료집』, 한국법제연구원, 2014, 1면.

특히 빅데이터 기술의 활용을 선도하고 있는 미국에서는 시장활동이 오프라인을 기반으로 하던 것에서 온라인 기반으로 전환되고 있고, 미국 경제활동의 패러다임도 클라우드 컴퓨팅이나 위치 기반 서비스 등을 중심으로 전환되고 있어, 이러한 경제의 지속적인 발전을 위해서는 빅데이터 기술을 포함한 소비자의 기술 네트워크에 대한 신뢰의 확보가 중요한 과제로 떠오르고 있다.[3)]

이에 다음에서는 미국에서의 빅데이터 활용과 그 정책 및 법제에 대해 살펴보고 빅데이터의 무분별한 사용이 불러올 수 있는 개인정보 침해를 위해 개인정보 보호 관련 정책 및 법제들을 살펴봄을 연구의 목적으로 한다. 이는 우리나라가 앞으로 빅데이터 활용 정책과 법제를 만듦에 있어 타산지석으로 삼고자 하는 것이다. 본 연구의 방법은 빅데이터와 개인정보 보호에 관한 미국의 정책 및 법제들, 그리고 이것들을 분석해놓은 단행본, 보고서, 논문들에 대한 문헌조사를 주된 연구의 방법으로 한다.

3) 김상겸 외 5인,『개인정보보호법 정비방안 연구』, 한국인터넷법학회, 2012년 12월, 30면

# 제 2 장 미국에서의 빅데이터 활용과 그 정책 및 법제

빅데이터는 우선 그 '활용'을 위한 미국 정부의 정책과 연방의회나 주의회가 이를 입법화한 법제들이 먼저 나타났다. 빅데이터의 활용은 행정 혁신과 산업 활성화라는 긍정적 측면과 함께 개인정보, 기업비밀과 국가기밀 침해라는 부정적 측면을 다 가지고 있다.[4)]

## 제 1 절 지식 행동화 데이터(Data to Knowledge to Action)

미국 유명 하이테크 기업, 제약사, 연구소 등 90개 이상의 기관이 참여하는 신규 빅데이터 프로젝트를 만들었으며 분야도 지리정보학에서 경제학, 의학, 언어학으로 폭이 넓어지고 있다. 예를 들자면, 미국 항공우주국과 아마존은 지구과학영역에서 협력연구를 촉진하기 위해 지구 관측 데이터를 아마존의 클라우드 저장서비스인 '공적 데이터'(Amazon Web Services Public Data Set)에 축적하고 '나사 지구교환 프로그램 플래폼'(NASA Earth Exchange Platform)을 구출해서 클라우드 서비스를 제공하고 있다.

## 제 2 절 빅데이터 연구와 개발 이니셔티브

2012년 3월 29일에 대통령 직속 과학기술정책실의 주도 하에 '빅데이터 연구 및 개발 이니셔티브'(Big Data Research and Development Initiative)가 발표되었다.[5)]

---

4) 정필운, 앞의 글, 1면.
5) 정필운, 위의 글, 2면

또한 미국 국방부, 국방연구원, 에너지부, 지질조사원, 국립과학재단, 국립보건원의 여섯 개 연방정부 부처와 기관은 빅데이터 진흥을 위해 2억 달러의 예산을 들여, 대용량 데이터의 수집, 저장, 가공, 관리, 분석 공유에 필요한 최첨단 핵심 기술의 확보, 첨단 기술을 활용하 노가학기술 발전의 가속, 국가안보 강화, 교수학습 변화의 도모, 빅데이터 기술 개발과 활용을 위한 인력 양성의 촉진 등의 목적으로 사용하였다.[6)]

## 제 3 절 개방형의 표준화된 정부정보 채택 행정명령

오바마 대통령은 2013년 5월에 효율적이고 투명한 정부 구현과 민간의 정부 정보 활용을 위해 개방형의 표준화된 데이터를 정부 정보 형식으로 채택하는 행정명령을 발포하였다. 미국은 이처럼 정부 벙조의 개방을 위해 정책적인 노력을 기울이고 있으며 이 분야에서 영국에 이어 세계 2위의 수준을 유지해오고 있다.[7)]

## 제 4 절 정부 데이터 개방 실행계획

미국은 2014년 5월 9일에는 정부 거버넌스 혁신과 데이터 개방 촉진을 위해 '정부데이터 개방 실행계획'(U.S. Open Data Action Plan)을 발표했으며 2014년부터 2년간 첫째, 찾기 쉽고 기계가독성이 있는 방식으로의 데이터 공개, 둘째, 시민의 의견에 따라 데이터 개방의 우선순위 결정, 셋째, 혁신가 지원과 피드백에 기반한 데이터 개방 향상, 넷째, 우선순위가 높은 데이터의 지속적 개방의 네 가지 원칙에 따라 데이터를 개방하기로 하였다.

6) 정필운, 위의 글, 3면.
7) 정필운, 위의 글, 6면

## 제 5 절 소 결

미국은 일찍이 빅데이터 기술의 가능성에 주목하여 ‘빅데이터 연구 및 개발 이니셔티브’ 등 예산을 수반한 일련의 진흥정책을 수립하여 공공부문과 민간부분에서 광범위한 기술 연구에 매진하고 있으며 이러한 연구성과를 다양한 영역에 적용하고 있다. 또한 이를 통하여 산업 활성화를 기하고 국가기관의 일하는 방식을 혁신하는데 활용하고 있다.[8)]

8) 정필운, 위의 글, 18면

# 제 3 장 미국에서의 빅데이터 규제와 그 정책 및 법제

## 제 1 절 빅데이터 정보환경에서 개인정보의 침해 위험

2011년에 가트너사(Gartner)의 조사에 의하면, 미국 기업 최고경영자들은 빅데이터 및 클라우드 컴퓨팅 환경에서 벙보보안 및 개인벙보 침해에 대하여 가장 큰 우려를 갖고 있는 것으로 나타났다. 전통적인 정보화 역기능인 개인정보 등을 포함한 정보 내용 이슈, 정보보안, 정보격차 등 중에서 빅데이터 정보환경에서 가장 현실적으로 큰 문제가 되고 있는 역기능은 역시 개인정보의 침해이다. 실제 미국에서도 이에 대한 우려가 가장 크며 개인정보 침해에 대한 규제 정책 과 법제가 나타나기 시작하고 있는 추세이다.[9)]

이러한 빅데이터 정보환경에서 개인벙보 침해에 대한 선진적 연구도 속속 나타나고 있다. 빅데이터 활용에 따라 개인벙조가 왜 문제되는지, 구체적으로 기존의 개인벙보 보호와 어떤 변화 양상이 있는지 등에 대한 선진적 연구들이 그것이다. Dineil J. Solove와 Paul M. Schwartz의 저서인 「정보프라이버시법」이 그 한 예이다.[10)]

## 제 2 절 온라인 프라이버시 프레임워크

오바마 행정부는 2012년 2월 23일에 2010년 발표된 상무부 소속 인터넷정책TF의 그린페이퍼를 기초로 해서 '온라인 프라이버시 프레임워크'(Consumer Data Privacy(Green Paper) in a Networked World: A

9) 정필운, 위의 글, 8면

10) Dineil J. Solove & Paul M. Schwartz, Information Privay Law, 4th ed., Wolters Kluwer Law &Business, 2011.

Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy)를 발포하였다. 이 온라인 프라이버시 프레임워크의 주요내용은 첫째, 7대 원칙으로 구성된 소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights), 둘째, 개인정보보호와 관련한 개별 법률의 정비 및 연방거래위원회로 개인정보보호법의 집행권 통일, 셋째, 사업자단체, 소비자단체 등 다양한 이해관계인의 합의를 바탕으로 권리장전의 내용을 구현한 분야별 '개별 지침'(code of conduct) 개발, 넷째, 국가간 정보 흐름의 장벽을 낮추기 위한 국제적 협력 등이다.[11]

## 제 3 절 소비자 프라이버시 권고

미국 연방거래위원회는 2012년 3월 26일에 프라이버시 정책담당자와 사업자들을 위한 프라이버시 보호를 위한 가이드라인으로서 '급변하는 시대의 소비자 프라이버시 보호'(Protecting Consumer Privacy in an Era of Rapid Change)라는 권고를 발포하였다. 이 소비자 프라이버시 권고는 첫째, 온라인 추적차단기능(Do-Not-Track)의 의무화, 둘째, 개인정보처리에[ 대한 소비자의 선택권 보장, 셋째, 모바일 서비스의 프라이버시 관행 개선, 넷째, 대형 플랫폼 사업자의 개인정보보호 의무 등이다.[12]

## 제 4 절 빅데이터와 프라이버시 워킹 그룹 권고

2014년 5월 1일에 '빅데이터와 프라이버시 워킹 그룹'(Big Data and Privacy Working Group)은 2014년초에 오바마 대통령이 제기했던 질문에 답하기 위해 빅데이터가 제시한 기회와 도전을 평가하고, 새로운

11) 정필운, 위의 글, 10면
12) 정필운, 위의 글, 12면

정책을 개발하기 위한 구체적은 권고를 발포하였다.[13]

이 권고의 주요내용은 다음과 같다. 첫째, 소비자는 자신의 개인정보가 어떻게 사용되는지에 대해 명확하고 이해가능하며 합리적인 기준을 얻을 자격이 있으므로 '소비자 프라이버시 권리장전'을 개정하고, 둘째, 행정부의 2011년 사이버보안 법안 제출에 따라 국가 데이터 위반 표준을 제공하기 위한 '데이터 위반 법안'을 통과시키고, 셋째, 프라이버시는 세계적인 가치이므로 미국 이외의 사람에게로 개인정보 보호를 확장하며, 넷째, 학생들의 데이터가 공유되거나 부적절하게 사용되는 것으로부터 학생들을 보호하면서도 학습 향상을 위해 사용되도록 노력하고, 다섯째, 연방정부는 보호계층에 차별적인 영향을 미칠 빅데이터 분석에 의해 용이하게 결과를 확인하고 사례를 식별할 수 있는 전문 기술을 구축해야 하기 때문에 차별을 중당하기 위한 기술의 전문성을 확장하며, 여섯째, '온라인의 보호표준'을 보장하기 위해 '전자 통신 프라이버시법'(The Electronic Communications Privacy Act)을 개정할 것을 권고했다.[14]

## 제 5 절 과학기술자문위원회 권고

대통령 직속 과학기술자문위원회(The President's Council of Advisors on Sicence and Technology)는 20114년 5월에 빅데이터 이용에 뜻른 개인정보 침해를 막기 위해 '빅데이터와 프라이버시: 기술적 관점'이라는 보고서를 박한하고 개인정보 정책을 권고했다.[15]

그 주된 내용은 첫째, 빅데이터의 수집과 분석이 아니라 빅데이터의 실제 사용에 정책을 집중해야 한다는 것, 둘째, 정부즤 정책과 규제는 개인정보보호정책의 메커니즘을 기술하는 것보다는 목적을 분명히 하

13) 정필운, 위의 글, 13면
14) 정필운, 위의 글, 14면
15) 정필운, 위의 글, 15면

는데 초점을 맞추어야 한다는 것, 셋째, 과학기술정책실, 미국 'IT R&D 프로그램'의 조정과 촉진을 통하여 개인정보 관련 기술의 연구가 강화되어야 하고 이러한 기술을 사회과학에 알려야 한다는 것, 넷째, 과학기술정책실은 교육기관과 직능단체와 공동으로 개인정보 보호와 관련된 교육 및 직업훈련 기회를 촉진해야 한다는 것, 다섯째, 미국이 국내외적으로 개인정보 보호 기술의 사용을 촉진하도록 리더쉽을 발휘해야 한다는 것이다.[16]

## 제 6 절 소 결

위에서 본 바와 같이 미국은 최근 빅데이터 정보환경의 역기능 중 특히 개인정보에 주목하면서 그 침해가 현실화되지 않도록 여러 규제 정책을 수립하고 이를 법제화하려는 동향을 보여주고 있다.[17]

16) 정필운, 위의 글, 16면
17) 정필운, 위의 글, 18면

# 제 4 장 미국에서의 개인정보 보호 관련 법제

미국은 영국, 독일, 이탈리아, 스페인, 핀란드 등 유럽국가들이나 호주 및 뉴질랜드와는 달리 정보통신분야의 개인정보보호에 관한 법률을 기본법으로 마련하고 있는 나라는 아니다. 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.[18)]

미국의 개인정보 보호 법제로는 연방정부가 보유하고 있는 개인정보들에 대한 보호법규인 1974년의 프라이버시법(Privacy Act)과 각각의 주정부 단위로 규정된 프라이버시 관련 주법들이 있다. 미국에서 개인정보 보호는 공공부문과 민간부문으로 나누어지며, 법은 공공부문에만 적용하고 민간부문에 대해서는 원칙적으로 윤리적 통제만 가능하도록 하고 있다. 미국의 개인정보 보호는 1966년의 정보자유법(Freedom of Information Act)에서 골격을 잡았다. 즉 원칙적으로 연방정부가 보유하고 있는 정보를 공개하기는 하지만 프라이버시법에 의한 정부 규제가 이루어지고 민간부문에서는 원칙적으로 정보의 자유로운 유통을 보장하면서 개별 분야에서의 개인정보 보호를 목적으로 영역별로 보호 법제를 가지고 있는 점이 특징이다.[19)]

현재 연방 차원의 개인정보보호는 1966년에 제정된 정보자유법(Freedom of Information Act), 1970년의 공정신용조사법(Fair Credit Reporting

18) 최경진 외 5인, 『빅데이터 환경에서 개인정보호 강화를 위한 법·제도적 대책방안 연구』, 개인정보 보호위원회 용역보고서, 2012년 12월. 43면

19) 김상겸 외 5인, 앞의 책, 25면

Act), 1974년의 프라이버시법(Privacy Act), 1978년의 금융프라이버시권법(Right to Financial Privacy Act), 1980년의 프라이버시 보호법(Privacy Protection Act of 1980), 1986년의 전자통신프라이버시법(Electronic Communication Privacy Act), 1988년의 컴퓨터 사용의 상호 비교 및 프라이버시 보호법, 1994년의 전기통신프라이버시법, 1996년의 통신법(Communication Act)이 제정되었고, 1995년 6월에 '프라이버시와 개인정보 제공 및 이용의 원칙'이 작성되었다. 이 원칙은 국가정보 통신기반 구축을 위한 정보통신기반 전담팀에서 정보정책위원회를 구성하고 3개 팀 중의 하나인 프라이버시팀이 작성한 원칙으로서, 계약자유에 따라 제공자의 고지와 소비자의 동의라는 2개의 필수조건을 고려하면서 업계의 자율적인 규제를 우선시 하고 있다.[20]

1998년 11월에 상무부가 제시한 개인정보보호를 위한 세이프하버 원칙(Safe Harbor Principles), 2000년 4월의 아동 온라인 프라이버시 보호법(Child Online Privacy Protection Act), 2002년의 전자정부법에서 도입한 프라이버시 영향평가제도 등을 통해 구현되고 있다. 그리고 인터넷상의 개인정보 보호를 위해 "소비자 온라인 프라이버시 공개법(Consumer Online Privacy and Disclosure Act)"과 "소비자 인터넷 프라이버시 증진법(Consumer Internet Privacy Enhancement Act)" 등의 법안이 의회에 제출되었다. 빅데이터 정보환경에 개인정보를 보호하기 위한 최근의 법률로는 미국 의회 제113회기인 2013년부터 2014년 사이에 제출된 '전자 통신 프라이버시법 개정안'(Electronic Communications Privacy Act Amendments Act of 2013) 등이 있다.[21]

또한 법적 규제 이외의 자율적 규제로, 기업들은 1999년 11월 온라인 프로파일링에 관한 워크샵에서 '네트워크 광고 이니셔티브'(Network Advertising Initiative)의 창설을 공표하였고, 그 후 "NAI 원칙(The NAI

20) 김상겸 외 5인, 위의 책, 26면
21) 최경진 외 5인, 앞의 책, 44면

Principles)"이 제안되었다.[22] 구글, 아마존 등 온라인 사업자들도 약관과 내부규칙을 가지고 개인정보를 보호하고 있으며 '정보통신망광고협회'(Network Advertising Initiative)는 소속 회원사를 위한 자율규제규칙을 제정하여 운영해오고 있다.[23]

개별법의 경우, 미국 개인정보 보호법제의 특징인 영역별 방식에 따라 개인정보 보호를 위해 다수의 개별법률들이 제정되고 있다. 이러한 개별법은 장점과 함께 단점을 가지는데, 장점은 보호가 특히 필요한 개인정보 취급영역에 한정해 법적 규제를 가하는 점이며, 단점은 개별영역별로 법률을 제정함으로써 관련 업계 혹은 이익단체의 영향을 받을 우려가 높다는 점이다.[24]

## 제 1 절 연방프라이버시법

### Ⅰ. 연방프라이버시법의 입법화

프라이버시는 미국에서 전통적으로 보통법상의 불법행위에 의하여 보호되어 왔다. 프라이버시가 판례에 의하여 헌법상의 권리로서 인정되면서부터 프라이버시 사건은 미국 개정헌법 제4조의 부당한 압수·수색 금지조항이나 개정헌법 제1조의 결사의 자유 조항을 근거로 하여 해결해 왔다. 그렇지만 미국이 1960년대부터 고도정보화사회로 접어들게 되면서 행정업무가 복잡다기화 되고 행정기관이 보유한 개인정보 양의 비약적인 증가가 있었다. 이렇게 증가되어진 정보량을 처리하기 위해 컴퓨터기술을 가급적 많이 활용할 필요성이 제기되었다. 이에 미국 예산관리처(Office of Management and Budget; OMB)는 연방정부의 각 부서에 분산되어 있던 개인기록의 전산화 및 집중화를 위

22) Id.
23) 정필운, 앞의 글, 17면
24) 김상겸 외 5인, 앞의 책, 26면

하고, 연방정부의 기록보존시스템과 정보 수집 과정을 개혁하기 위해 국립정보센터(National Data Center)를 세우기로 계획을 수립했다. 이런 구상이 알려지자 국민 여론은 국민 개개인의 프라이버시 침해의 위험성 때문에 거부반응이 많이 일었다. 그리고 1968년에 하원 정치활동 위원회가 충분한 대응책 마련한 후 국립정보센터 설치를 권고함으로써 정부의 이러한 계획은 일단 중단되었다.[25)]

한편 행정기관뿐만 아니라 민간조사기관에 의한 개인의 프라이버시 침해도 빈발하였다. 그러자 1970년에 공정신용조사법(Fair Credit Reporting Act)이 제정되었다(Pub. L. No. 91-508, 84 Stat. 1136). 이 법은 소비자 신용조사업자에 대해 보험, 인사, 소비자 신용 등의 정보와 비밀 보호, 관련성과 정확성 등에 대하여 합리적 조치를 취할 것을 의무화하였다. 다른 한편에서는 공공기관에 의한 프라이버시 침해 방지를 위한 법률의 입법화도 계속해서 시도되었다. 특히 보건교육복지부 장관이 1973년에 공표한 자문위원회 보고서에는 다음의 다섯가지 원칙이 제시되었다. 목적 외 이용 금지의 원칙, 개인 접근의 원칙, 기록시스템의 공시 원칙, 충분한 안전조치를 취할 원칙, 개인구제의 원칙이 그것이다. 이것은 이후 프라이버시법의 골간을 형성하게 된다. 미국 연방의회는 1974년 하반기에 접어들면서 그동안의 논의사항을 토대로 만든 프라이버시 법안들을 심의하게 된다. 이들 프라이버시 법안 가운데 규제가 완화된 하원안 H.R. 166373과 권리보호에 있어 엄격한 상원안 S.3418이 각각 하원과 상원에서 압도적인 찬성을 얻어 연방의회를 통과하게 된다. 그렇지만 이 두 법안의 내용에는 많은 차이가 있었기에 양원협의회의 심의를 당연히 거쳐야 했었으나, 회기 만료 전에 입법을 끝마치려는 상·하원의 의지가 워낙 강해서 결국 '프라

25) 성낙인 외 9인,『개인정보보호법제에 관한 입법평가』입법평가보고서 08-13 (한국법제연구원, 2008년) 463-464면.

이버시법'(Privacy Act)이 1974년 12월 31일에 공포되기에 이르렀다 (Pub. L. No. 93-579, 88 Stat. 1896).[26]

행정기관 문서에 국민들의 접근 보장을 위해 1966년에 제정된 미국 연방법률이 정보공개법(Freedom of Information Act, 5 U.S.C. § 552)이라면, 국민 개개인에게 민감할 수 있는 개인 문서가 대중에게 공개되는 것을 방지하려는 연방법률이 1974년의 프라이버시법(Privacy Act, Pub. L. No. 93-579. 5 U.S.C. § 552a)이었다. 그 명칭으로 봤을 때 프라이버시법은 프라이버시 일반에 대한 보호 법률인 것 같은 인상을 주지만, "개인에 관해 보유된 기록(Records maintained on individuals)"이라는 표제가 붙어있는 데에서 알 수 있듯이, 프라이버시법은 행정기관 보유의 개인 정보에 대한 보호를 입법목적으로 하는 개인정보 보호에 국한된 연방법률이다. 프라이버시법은 연방 행정기관에 의한 개인 정보 공개에 제한을 두고 있다. 또한 이러한 개인 정보를 연방 행정기관이 공개할 경우에 본인에게 그 개인정보에 대한 접근권을 보장하게 하고 있다. 그리고 개인 정보의 수집에 제한을 두어 개인정보는 가능한 한 본인으로부터 수집할 것, 필요최소한으로 정보를 보유할 것 등을 의무화 하고 있다. 정보의 보유에 대해서도 정확성 및 비밀유지를 의무화하고 있다. 프라이버시법은 1988년의 '컴퓨터매칭과 프라이버시보호법'(Computer Matching and Privacy Protection Act, Pub. L. No. 100-503)에 의해 컴퓨터연결프로그램에 이용하기 위한 개인 정보 제공을 제한하는 내용들이 추가되게 되었다.[27]

## Ⅱ. 연방프라이버시법의 적용 범위와 내용

행정기관이 관리하는 기록시스템에 포함된 모든 기록, 즉 행정기관이 개인에 관하여 보유하는 기록이 연방프라이버시법에 의해 보호되

26) 성낙인 외 9인, 위의 책, 465면
27) 성낙인 외 9인, 위의 책, 465-466면

는 대상이다. '개인에 대하여 보유된 기록'(Records maintained on individuals)의 의미에 관해서는 정의규정이 있다. 이에 따르면 '개인'(individual)은 미국 시민이나 영주권을 취득한 외국인을 의미하고(§ 552a(a)(2)), '보유'(maintain)는 보관, 수집, 이용과 유포를 의미하며(§ 552a(a)(3)), '기록'(record)은 행정기관이 보유하고 있는 개인에 관한 정보의 모든 항목 혹은 그것이 수집되거나 정리된 것을 의미한다. 이것에는 취업경력, 전과기록, 의료병력, 금융거래, 학력 등이 포함되지만 이것들에 한정되는 것은 아니고, 개인의 성명, 식별번호나 기호 혹은 사진, 지문 등과 같이 신원을 확인할 수 있는 특기사항이 포함된다(§ 552a(a)(4)). 그리고 '기록시스템'(system of records)은 행정기관이 보유한 기록이 정리된 것으로서 개인정보가 성명, 기호, 식별번호 등 개인에게 배정된 신원확인을 위한 특이사항에 의해 검색되는 것을 의미한다(§ 552a(a)(5)). 이 때 이 특이사항은 수작업에 의한 것이든 자동처리된 것이든 구분하지 않는다.[28]

연방프라이버시법의 적용범위를 일정한 기록시스템으로 한정한 것은 검색된 자료들을 모두 보호의 대상으로 삼는다면 행정기관의 부담이 과도할 수 있을 뿐만 아니라 국민의 알권리를 보장하려는 정보공개법의 취지를 고려하지 않을 수 없었기 때문이다. 연방프라이버시법의 적용을 받는 '행정기관'(agency)에는 모든 행정관청, 군사관청, 정부법인, 정부관리법인, 대통령직속 사무국을 포함한 기타 연방정부의 행정기관 및 모든 독립규제위원회를 의미한다는 정보공개법의 '행정기관'에 관한 규정(§ 552(f)(1))을 준용하고 있다(§ 552a(a)(1)). 이들 행정기관들 가운데 일부 행정기관의 장은 특정 기록에 대한 연방프라이버시법의 적용 면제를 내용으로 하는 규칙을 제정하여 공포할 수 있다. 이 경우 행정기관은 그 규칙에서 면제사유를 설명해야 하며(§ 552a(j)),

28) 성낙인 외 9인, 위의 책, 466면

연방프라이버시법의 적용이 면제되는 기록의 예로는 범죄예방이나 수사 혹은 형벌의 집행을 담당하는 기관이 보유하는 기록, 중앙정보국(Central Intelligence Agency; CIA)이 보유하는 기록이 있다(§ 552a(j)(1), (2)).[29]

그 이외에 연방 프라이버시법의 주된 내용은 다음과 같다. 연방 프라이버시법에서는 목적구속성과 정보의 직접수집 등을 규정하고(§§552a(e)(1)-(3)), 기록의 정확성・완전성 유지, 기록시스템의 고시 등(§§552a(e)(5)-(10)), 자기정보의 열람과 정정(§§552a(d)), 컴퓨터결합(computer matching)을 위한 정보제공의 제한(§§552a(o)-(q)), 개인정보의 공개 제한(§§552a(b)-(c)), 형사처벌과 손해배상(§552a(g)), 예산관리처(§552a(v))에 의한 감독 등을 규정하고 있다.[30]

## 제 2 절 그 외 공공부문에서의 개인정보보호 법률

그 외에도 정부와 행정기관에 의한 개인 정보의 취득에 제한을 가하는 연방 법률들이 여러 건 제정되었다. 예를 들어, 금융기관이 보유하는 개인정보의 보호를 위해 금융프라이버시권법(Right to Financial Privacy Act)이 1978년에 제정되었다. 금융프라이버시권법은 금융기관이 보유하는 개인정보에 대한 정부의 접근을 원칙적으로 금지하면서 예외적으로 정부가 개인정보에 대한 비밀 보장을 전제로 할 경우에만 그 개인정보에 대한 접근을 허용하고 있다12 U.S.C. §§ 3401-3422). 그리고 도청 등과 관련하여서는 연방통신법(Telecommunication Act)은 도청 등과 관련하여 송신자의 동의 없이 유선으로 통신을 감청하거나 통신의 존재나 내용 등을 타인에게 누설하는 것을 금지하고 있다. 또

29) 성낙인 외 9인, 위의 책, 466-467면
30) 성낙인 외 9인, 위의 책, 467-479면

한 1968년의 '범죄방지와 가두의 안전을 확보하기 위한 종합법률'에서는 유선통신과 무선통신에 관한 감청을 원칙적으로 금지하면서 예외적으로 영장을 발부받은 수사기관의 전화 감청은 허용하고 있다(U.S.C. Title18 Chapter 119). 1986년의 전자통신프라이버시법(Electronic Communications Privacy Act, ECPA)은 전자통신에도 이러한 보호를 확대했으며, 감청의 방법에 대해서도 '기타의 취득'으로 규정함으로써 널리 금지 범위를 확대시켰다. 1980년의 프라이버시보호법(Privacy Protection Act, PPA)은 보도기관 종사자에 대한 압수·수사를 원칙적으로 금지하함으로써 보도기관 종사자와 그 정보원의 프라이버시 보호를 꾀하고 있다(42 U.S.C. § 2000 aa). 또한 1988년의 비디오프라이버시보호법(Video Privacy Protection Act, VPPA)은 대여한 비디오의 정보에 대한 압수·수색을 위해 필요한 영장의 요건을 엄격하게 규정하였다(6 U.S.C. § 2710). 또한 전과정보와 관련해 연방수사국과 주당국이 정보를 공유하는 시스템을 허용하고, 수사 이외의 목적으로 전과정보를 이용하는 경우 그 이용방법 등에 대해 제한을 가하고 있다(42 U.S.C. § 14611). 그리고 정보의 개시·제공에 대해서도 프라이버시 보호를 꾀하고 있다. 즉, 1966년의 정보공개법(Freedom of Information Act, FOIA)은 공개가 프라이버시에 대한 명백한 부당 침해가 될 경우에는 정보공개 의무의 예외를 인정하고 있다. 또 법집행기관의 기록에 포함된 프라이버시에 관해서는 보다 넓게 비공개를 규정하고 있다(5 U.S.C. § 552). 또한 1978년의 성범죄피해자의프라이버시보호법(Privacy Protection for Rape Victims Act)은 성폭행사건에서 피해자의 과거 성관계 등을 합법적인 증거에서 제외함으로써 피해자의 프라이버시 보호에 만전을 기하고 있다.[31]

31) 성낙인 외 9인, 위의 책 468-469면

## 제 3 절 민간부분에서의 개인정보 보호 법률

민간부분의 개인정보 보호에 대해 포괄적 법률은 없고 다만 개별적 영역에서 그때그때 필요할 때 법률을 제정해왔다. 이러한 개별적 법률이 제정되지 못한 영역에서는 개인정보에 대한 규제가 사업자의 자율적 규제에 맡겨져 있는 것이다. 다음에서는 민간부분에서의 개인정보 보호법률들을 제정 시기순으로 살펴본다.[32]

### Ⅰ. 공정신용조사법

공정신용조사법(Fair Credit Reporting Act, FCRA)이 1970년에 제정되었는데 이 법률은 소비자의 신용 등에 관한 조사기관의 보고에서 보고가 허락되는 목적과 사항을 제한하면서 소비자의 접근권을 보장하고 있다(15 U.S.C. §§1681a-1681u). 공정신용조사법은 통상적으로 제3자에게 소비자에 관한 기록들을 제공할 목적으로 소비자의 신용에 관한 정보를 수집하거나 평가하는 일을 하는 신용조사기관에게 의무들을 과한다(15 U.S.C. §1681a(f)). 이런 개인기록에는 영업적 신용기록이나, 조사기관의 요구로 준비되는 보험기록에 관한 요청들이 포함되지 않는다. 공정신용조사법은 정보주체에게 정보를 제공할 의무를 과하면서 동시에 신용조사기관으로 하여금 이런 기관이 보유하고 있는 파일들 속에 들어있는 모든 정보의 내용, 소송과 무관한 조사기록들의 출처를 제외한 정보에 관한 기타 출처, 6개월내 소비자 기록을 얻은 사람 명단 등을 공개하게 하고 있다(15 U.S.C. §1681g). 그리고 정보주체에게 그 정보가 정확하지 않을 경우 정정을 요구할 수 있게 하고 있다(§1681i). 이러한 정정요구에 대해 신용조사기관은 재조사를 해서 문제된 정보의 현 상황을 기록하고 해당 정보가 더 이상 유효하지 않

32) 성낙인 외 9인, 위의 책, 469면

거나 부정확할 경우에 그 기관은 그 정보를 삭제해야 한다. 정보가 삭제되지 않으면 정보주체는 100단어를 넘지 않는 범위내에서 그에 관한 해명을 할 수 있고, 이런 정보주체의 해명은 미래의 보고서에 기록된다(§1681i(b), ©). 이런 신용기록 사용자들은 조사기관의 정보에 근거해 반대되는 결정을 내릴 경우 정보주체에게 통지를 하여야 한다. 관련자의 요구가 있으면 기록의 사용자는 신용기록들에 반대되는 결정들을 내릴 경우 그 근거를 관련자에게 공개하여야 한다(§1681m). 그리고 동법은 권한 없이 정보를 받는 사람에 대한 처벌규정을 두고 있다(§1681q, r). 만일 위 규정들에 위반할 때에는 민사책임을 부담하게 되며, 이 민사책임에 대해서는 연방거래위원회(FTC)가 집행의 권한을 갖고 있다. 그러나 공정신용조사법은 신용조사기관이 정보를 부가적으로 사용하거나 공개하는 것에 대해서는 적절히 대응할 수 없는 약점을 지닌다. 신용조사회사가 신용기록의 "신용 헤더(credit header)" 부분을[33] 여러 경제주체들에게 파는 것을 허락하고 있다. 이 부분은 신용조사업계의 로비가 영향력을 발휘한 결과로 보여진다. 공정신용조사법의 문제점으로 개인과 신용조사회사간의 역학관계의 불균형을 해결해 내지 못했다는 점이 지적된다.[34]

## Ⅱ. 가족의 교육권과 프라이버시에 관한 법률

'가족의 교육권 및 프라이버시에 관한 법률'(Family Educational Rights and Privacy Act, FERPA)이 1974년에 제정되었다(Pub. L. No. 93-380, 88 Stat. 484). 이 법은 연방의 보조를 받는 모든 교육기관과 조직에게 교육 관련의 기록을 학생들의 보호자에게 열람할 수 있도록 한다. 또한 학생과 학부모의 동의 없이는교육 관련 기록을 공개하거나 제3자에게 제공하지 못하게 하고 있다(20 U.S.C. §1232g.). 그러나 이러한 제한

33) 성명, 주소, 전화번호, 사회보장번호, 고용정보, 생일 등
34) 성낙인 외 9인, 앞의 책, 470-472면

의 적용범위는 교육 분야에 국한되고, 그 중에서도 일부의 기록만을 대상으로 한다. 그러나 20 U.S.C. § 1232g(a)(4)(B)(ii)이 규정하는 교육 공무원에 의해 보유되는 기록 및 건강기록과 심리적 기록은 제외된다.(§ 1232g(a)(4)(B)(iv))[35]

## Ⅲ. 금융프라이버시권법

미국에서 금융기관이 보유하고 있는 개인정보에는 개인의 금융거래나 상거래에 관한 정보뿐만 아니라 고객정보를 위시해 각종 개인정보가 포함되어 있다. 이런 이유로 정보가 누설되거나 제3자에게 공개되는 경우에는 개인의 경제활동에 관한 세밀한 상황이 공개되게 됨으로써 금융기관이 보유하고 있는 정보의 취급에는 세심한 주의가 요구된다. 미국에서는 이런 이유로 금융기관의 고객정보가 법적 보호의 대상이 되는 개인정보로서 프라이버시의 권리에 기초해 보장된다.[36]

금융기록프라이버시법(Financial Records Privacy Act, FRPA)은 1978년에 제정되었으며, 법에 정한 내국세수입청이나 은행감독기관 등의 경우를 제외하고는 행정기관이 금융기록들을 수집하는 것을 금한다(12 U.S.C. §3402). 여기서 '금융기록들'이란 '금융기관과 소비자간의 관계를 담고 있는 금융기관에 의해 보관되는 기록정보'를 말한다. 다만 이런 기록에는 개인 소비자 관련 기록만 해당된다. 또한 '금융기관'이란 은행, 수신여신협회, 저축은행, 소비자금융기관, 신용카드발급업자, 신용조합를 포함한다(§3401(1)). '정부기관'은 국가기관, 공무원이나 국가기관의 고용인을 뜻한다(§3401(3)). 소비자는 이런 정보 공개에 동의할 수는 있다. 하지만 이런 정보가 이런 금융기관의 업무활동 조건으로서 공개되어서는 안 된다.(§3401(a), 3404(b)). 다만 이런 기록들이 정당한 법집행을 위해 수집된다고 믿을 만한 이유가 있거나 이

35) 성낙인 외 9인, 위의 책, 472면
36) 김상겸 외 5인, 앞의 책, 27면

런 기록의 복사가 금융기관에 봉사하거나 소비자를 위한 것일 경우에만 소환장이나 행정상 명령에 의해 이런 기록들을 공개할 수 있다(§3405). 그리고 연방형사절차 규칙에 의한 영장 발부를 위해 이런 기록들을 얻을 수 있다(§3406). 그래서 이런 기록들의 공개는 영장 기타의 합법적 요구를 넘어서 이루어져서는 안 된다. 또한 보험회사나 보험정보 수집기관들은 그들이 다루는 보험 거래를 위해 기록한 개인정보를 그 개인정보의 주체인 개인이 이용할 수 있도록 해야 한다. 이에 의해 해당 개인은 보험회사나 다른 보험정보 수집기관들이 갖고 있는 자신 관련 정보의 공개를 서면으로 요청할 수 있다. 정보주체인 개인이 요구하는 경우에 보험회사나 다른 보험정보 수집기관들은 보통 30일내에 이런 요구에 답해야 한다. 해당 개인이 개인정보를 요청할 때 신청자와 보험계약자는 보험회사나 다른 보험정보수집기관들의 기록에 대해 자신에 관한 정보를 수정, 삭제하도록 요구할 수 있고, 보험회사나 다른 보험정보 수집기관들은 30일내에 이런 개인의 요구에 답해야 한다. 또한 보험회사나 다른 보험정보수집기관들이 개인정보를 수정하거나 삭제한다면 그 개인에게 이에 관해 서면으로 통지해야 한다. 보험회사나 다른 보험정보 수집기관들이 이러한 개인의 요청들을 거절한다면 개인에게 거절이유, 거절에 관한 해당 개인의 진술권 있음, 심사를 요구할 개인의 권리에 대해 통지해야 한다. 이런 진술권은 개인이 동의하지 않는 정보에 대한 것으로서 보험회사나 다른 보험정보 수집기관들이 이것을 정리해야 한다. 회사나 기관이 일단 해당 개인으로부터 진술을 받으면, 그 개인의 기록들 속에 논란이 되는 개인정보에 대한 진술을 기록·정리하고 이런 자료를 나중에 살펴보고 접근할 수 있게 해야 한다. 논란이 되는 정보를 계속 공개할 때 보험회사나 다른 보험정보 수집기관은 논란이 되는 문제를 분명하게 확인하고, 이런 개인의 진술을 다른 공개 정보와 함께 제공해야 한다. 추가로 이들 기관이나 이들 회사들은 과거에 이들로부터 그 개

인에 대해 정보를 받은 기관이나 회사들에게 이런 새로운 진술을 해야만 한다. 일반적으로 보험회사나 다른 보험정보 수집기관들은 보험거래와 관련해 수집된 개인 정보를 공개할 수 없다. 그러나 이런 규정은 아주 많은 예외들을 가지고 있기 때문에 이런 예외가 허용되려면 정보의 수령자가 누가 될 수 있는지, 정보 공개가 이루어지는 목적이 무엇인지를 구체화 해야 한다. 또한 정보가 제공된 사실과 어떤 상황에서 정보가 제공되었는지에 대해 해당 개인에게 통지해야 한다. 또한 공개에 대한 다른 제한은 해당 개인에 의한 승인이다. 일반적으로 보험회사나 보험정보 수집기관은 개인이 공개를 승인한 정보만을 공개할 수 있다.[37)]

위에서 조문을 통해 본 바와 같이 금융프라이버시법은 정부기관에 의한 금융기록 접근을 원칙적으로 금지하고 예외적으로 고객의 동의, 수색영장, 행정기관의 소환영장, 사법기관의 소환영장, 공식적인 서면 청구에 의하지 않으면 정보는 공개되지 않는다. 그리고 금융기관의 개인정보 취급에 대해 금융기관의 보호정책을 명시할 의무를 부과하고 소비자 스스로가 개인정보의 이용에 대한 선택을 할 때 지침이 될 수 있는 정보를 제공하도록 했다. 또한 소비자가 관련회사 이회의 제3자와 정보공유를 선택할 수 있게 했다.[38)]

금융 분야의 프라이버시 보호와 관련해 금융 업체들은 고객 정보를 다케팅 목적으로 전송할 경우에 반드시 오프트아웃 옵션을 제공하도록 했다. 미국의 MPA는 이메일 선호, 우편 선호, 전화 선호 서비스에 대한 책임을 부담하고 있고 연방의 '두앗콜 리스트'(Do-Not-Call List)는 오프트아웃 방식으로 운영되고 만약 데이터 제공자가 오프트아웃의 옵션을 선택했을 경우 7일 이내에 그 요청대로 조치를 취해야 한다.[39)]

37) 성낙인 외 9인, 앞의 책, 473-474면
38) 김상겸 외 5인, 앞의 책, 27면
39) 김상겸 외 5인, 위의 책, 28-29면

## Ⅳ. 케이블통신정책법

1984년의 케이블통신정책법(Cable Communications Policy Act, CCPA, 47 U.S.C. § 551)은 개인식별정보에 대해 가입자에 대한 고지의무를 규정하고 있다(§ 551(a)(1)). 그리고 가입자가 동의하지 않으면 가입자의 시청 습관을 나타내는 정보들을 사업자가 수집하거나 공개하지 못한다(§ 551(c)(2)(C)(ii)). 또한 가입자에게 정보에 대한 접근권을 보장하고 정보 삭제도 요구할 수 있게 했으며 이에 위반하면 소송을 제기할 수 있게 했다(§ 551(f)(1)). 그러나 그러한 규정은 유선방송 운영자에게만 적용되고 개인 정보가 '정당한 영업활동'을 위해서는 공개될 수 있게 넓은 예외규정을 두고 있다(§ 551(f)(1)). 이런 점에도 불구하고 케이블통신정책법은 소비자들에게 자신의 유선방송 관련 기록에 대해 통제권을 주는 첫 번째 시도라고 볼 수 있다.[40]

이렇듯 미국에서는 개인의 시청 경향에 대한 정보를 보호하기 위해 케이블통신정책법이 제정되었고, 그 외에 보도기관의 개인정보 보호를 위한 1980년의 프라이버시보호법이 있다.[41]

## Ⅴ. 전자통신프라이버시법

1986년의 전자통신프라이버시법(Electronic Communications Privacy Act, ECPA, 18 U.S.C. §§ 2510-2522, 2701-2709, 2711)은 1986년에 제정되었으며, 1968년의 연방도청법(Federal Wiretap Act, 18 U.S.C. §§ 2510-20)의 적용범위를 이메일, 무선전화, 기타 컴퓨터 전송수단을 포함하는 새로운 정보, 목소리, 비디오 통신으로까지 확대했다. 전자통신프라이버시법은 정보서비스 제공자와 관리인에게 개인의 프라이버시를 보호

40) 성낙인 외 9인, 앞의 책, 475면
41) 김상겸 외 5인, 앞의 책, 28면

할 의무를 부여하고 있다. 또한 통신도청을 범죄로서 처벌하고 있고 전자 통신 도청은 영장에 의해서만 할 수 있도록 하고 있다(18 U.S.C. §2510). 그리고 전자통신서비스 사업자가 통신내용을 외부에 공개하는 것을 금하고 있고, 축적된 통신에 대한 부정한 액세스를 금지하고 있다(18 U.S.C. §2710). 이러한 통신 접근 금지규정은 1988년에 비디오프라이버시보호법(Video Privacy Protection Act)으로 개정되었다. 개정법률은 비디오테이프 임대 및 판매업자가 기록을 부당하게 공개하는 것을 금하고 위반하면 민사상의 책임을 부과하고 있다(18 U.S.C. §2710). 그러나 비디오프라이버시보호법에서는 개인정보의 수집과 이용에 대해 특별한 제한규정을 두지는 않고 있다. 또한 인터넷서비스 제공은 비디오프라이버시보호법의 적용이 면제된다. 따라서 가입자의 이메일을 조사하는 것은 허용된다.[42]

## Ⅵ. 비디오프라이버시법

비디오프라이버시법(Video Privacy Protection Act, VPPA, Pub. L. No. 100-618, 102 Stat. 3195)은 1988년에 제정되었다. 연방대법관 후보였던 Robert Bork의 비디오카세트 대여 기록을 한 신문기자가 입수한 것이 이 법을 만든 직접적인 계기가 되었다. 비디오프라이버시법은 비디오테이프 서비스제공자가 대여하거나 구입한 비디오카세트의 제목 같은 개인 정보를 개인의 서면 동의없이 고의로 공개하는 것을 금하고 있다(18 U.S.C. § 2710(b)). 그리고 이에 위반한 행위에 대해 소송을 할 수 있게 하고 있다(§§ 2710(b)(1), (c)(1)). 이 비디오프라이버시법은 비디오카세트테이프에만 적용되고, 레코드 가게, 서점, 잡지사, 카탈로그회사, 기타 소매점에 대해서는 유사한 제한이 없다(§ 2710(a)(4), (b)).[43]

42) 성낙인 외 9인, 앞의 책, 475-476면
43) 성낙인 외 9인, 위의 책, 476-477면

## Ⅶ. 전화소비자보호법

전화소비자보호법(Telephone Consumer Protection Act, TCPA, Pub. L. No. 102-243, 105 Stat. 2394)은 1991년에 제정되었다. 동법은 텔레마케팅에서 소비자의 프라이버시 보호를 위해 자동전화 시스템과 팩스를 이용하여 텔레마케팅을 하는 것에 제한규정을 두고 있고, 가입자의 프라이버시 보호를 위한 규제규정들도 두고 있다(47 U.S.C. §227). 전화소비자보호법은 개인이 거부의사를 밝혔음에도 불구하고 통신판매인이 계속 전화를 할 경우에 그 개인은 통신판매인에 대해 500달러 이하의 손해배상청구소송을 제기할 수 있게 하고 있다. 만약 통신판매인에게 고의가 있으면 그 손해의 3배에 상당하는 금액을 배상토록 하고 있다. 그러나 전화소비자보호법은 전화로 인한 피해를 구제하는 것을 목적으로 하므로 개인 자료의 수집, 사용, 판매는 규제하지 않는다(47 U.S.C. § 227(c)(5)).[44]

## Ⅷ. 운전자프라이버시보호법

운전자프라이버시보호법(Driver's Privacy Protection Act, DPPA, 18 U.S.C. §§ 2721-2725)은 1994년에 제정되었다. 운전자프라이버시보호법은 자동차 기록에 포함된 개인정보를 판매하는 여러 주의 관행에 제동을 거는 기능을 했다. 운전자프라이버시보호법은 자동차와 관련된 개인정보를 판매상들에게 제공하기 전에 꼭 운전자의 동의를 얻도록 했다(18 U.S.C. § 2721(b)(12)). 그러나 그것은 단지 자동차 기록에만 적용될 뿐이며, 나머지 정보에 대해서는 그들이 보유하고 있는 수많은 형태의 다른 기타 기록들 속에 담긴 정보를 공개하는데 있어서는 아무런 제한을 받지 않는다.[45]

---

44) 성낙인 외 9인, 위의 책, 477면
45) 성낙인 외 9인, 위의 책, 478면

## Ⅸ. 텔레커뮤니케이션보호법

1996년의 텔레커뮤니케이션보호법은 통신법을 상당 부분 개정하여 1996년에 제정되었다. 텔레커뮤니케이션보호법은 텔레커뮤니케이션 업자에게 소비자 정보 보호의무를 부과하고 있다. 따라서 사업자는 일정한 정보에 대해 비밀유지의 의무를 부담하며 개시청구권이 이용자에게는 보장되고 가입자 리스트를 제공하는 등의 제한규정을 두고 있다(47 U.S.C. §222).[46]

## Ⅹ. 건강보험책임법

건강보험책임법(Health Insurance Portability and Accountability Act, HIPAA, Pub. L. No. 104-191, 110 Stat. 1936)은 1996년에 제정되었다. 의료분야에 관한 개인 정보 문제에 대해 규제조항들을 두고 있다. 건강보험책임법은 보건후생부가 의료기록과 관련된 프라이버시를 규제하기 위한 행정입법 제정의무를 부과하고 있다(110 Stat. at 2033-34). 이에 근거해 보건후생부는 보상, 치료, 또는 수술의 목적 이외의 모든 사용과 공개를 위해서는 위임이 필요하다는 명령을 공포했다(45 C.F.R. § 164.508(a)).[47]

## Ⅺ. 아동온라인프라이버시보호법

아동온라인프라이버시보호법(Children's Online Privacy Protection Act, COPPA, 15 U.S.C. §§ 6501-6506 (2000))은 1998년에 제정되었다. 이 법은 인터넷에서 아동의 개인정보들을 모으는 것을 규제함을 주된 내용으로 한다. 이 법은 인터넷상에서의 프라이버시를 직접 다루는 최

46) Id.
47) 성낙인 외 9인, 위의 책, 478-479면

초의 연방법률이라는 점에서 큰 가치를 지닌다. 아동온라인프라이버시보호법에 따르면, 아동에 대한 웹사이트는 웹상에 프라이버시 관련 정책에 대해 게시해야 한다(§ 6502(b)(1)(A)(i)). 서비스제공자는 아동의 개인정보를 수집, 사용 또는 공개하기 전에 '증명될 수 있는 부모의 동의'(verifiable parental consent)를 획득해야 한다(§ 6502(b)(1)(A)(ii)). 이 법은 이 법의 집행기관인 연방거래위원회가 부모의 동의를 얻는 구체적인 절차 및 방법에 대해 이를 규칙으로 정하게 하고, 이 규칙에 위반되면 이를 불법행위고 규정하고 있다(§ 6502(b)). 이런 아동온라인프라이버시보호법의 규정에 따라, 1999년 10월에 연방거래위원회는 아동온라인프라이버시보호규칙(Children's Online Privacy Protection Rule)을 공포했다. 이 아동온라인프라이버시보호규칙에 따르면 아동대상 서비스 사업자에게는 인터넷상에서 아동의 개인정보의 수집・사용에 대해 불공정 행위와 사기행위를 금하고 있다. 또한 프라이버시 정책에 대한 고지(notice)에 들어가야 할 내용과 부모의 동의(parental consent)를 얻는 방법에 대해 규정하고 있다. 전자에는 3자에 대한 제공시에 고지해야 할 내용으로 정보가 제공될 제3자의 신원, 기업정보, 개인정보의 비밀성, 완전성, 보안성을 유지할 것을 약속했는지 여부, 부모의 동의가 거부될 수 있는 지 등이 규정되어 있다(§312.4(b)(2)(iv)). 또한 후자에는 부모의 동의를 얻기 위한 방법으로 법정대리인에게 동의서를 제공하고 부모가 이에 서명하여 우편이나 팩스로 서비스 제공자에게 전달하는 방법, 특정의 온라인 거래와 관련해 부모가 신용카드를 사용하도록 하는 방법, '공개 키 기술'(public key technology)을 이용한 디지털 인증을 통해 동의를 받는 방법, 부모가 수신자 부담의 무료전화를 하게 하고 숙련된 응답직원을 통해 동의를 확인하는 방법, '부모가 앞에 말한 방법 중의 하나를 통해 얻은 개인식별번호나 패스워드가 딸린 이메일로 동의를 표시하는 방법 등이 규정되어 있다

(§ 312.5). 하지만 이 아동온라인프라이버시보호법의 적용범위는 매우 좁다. 이 법은 어떤 웹사이트나 아동을 겨냥한 온라인서비스의 운영자나 아동으로부터 개인정보를 수집한다는 실질적 인식을 가진 운영자에게만 적용되기 때문이다(§ 6502(b)(1)(A)). 게다가 이 법은 13세 이하의 아동으로부터 개인정보를 수집하는 웹사이트 운영자에게만 적용되므로 그 적용범위는 더 좁아진다(§ 6501(1)).[48]

## Ⅻ. 금융지주회사 관련법

금융지주회사 관련법(Pub. L. No. 106-102, 113 Stat. 1338)은 1999년에 제정되었다. 이 법은 합병되는 투자회사, 은행, 보험회사가 각 자회사들이 가지고 있는 '비공개 개인정보'(nonpublic personal information)를 공유할 수 있도록 하고 있다. 자회사들은 회사의 고객에게 그들이 비공개 개인정보를 공유하는지를 설명해야 하기는 하지만, 개인이 설명을 듣고 이런 비공개 개인정보의 공유를 막을 방법은 없다. 기껏해야 개인이 자신의 정보가 제3자에게 공개되지 못하도록 할 수 있을 뿐이다(15 U.S.C. § 6802(a), (b)). 최근 기업간의 결합이나 합병이 매우 활발히 이루어지고 있는 현실을 감안할 때, 정보 공유에 대한 규율로서는 아주 미흡한 법률이라 평가할 수 있다.[49]

## ⅩⅢ. 소비자 인터넷 프라이버시 증진법안

'소비자 인터넷 프라이버시 증진법안'(Bill of Consumer Internet Privacy Enhancement Act)은 2001년 1월 20일에 미국 연방하원의 '자원통상위원회'에 제출되었다. 이 법안은 기존의 인터넷상의 프라이버시 보호에 대해 보다 구체적으로 접근하고 있다. 프라이버시를 침해할

48) 성낙인 외 9인, 위의 책, 479-480면
49) 성낙인 외 9인, 위의 책, 480-481면

수 있는 기술적인 조치, 특히 그 중에서도 프로파일링에 쓰이는 쿠키나 트랙킹 소프트웨어에 의한 개인정보 수집에 대해서도 상세한 규정을 두고 있다. 이 법안은 개인식별정보의 수집과 관련하여, 고지나 마케팅 목적으로 이용하는 정보 또는 웹사이트에 의해 제공된 제품이나 서비스의 제공과 관련이 없는 경우 법에 비공개로 규정된 경우 수집된 개인식별정보를 제3자에게 게시하는 것을 이용자가 제한할 수 없다면, 웹사이트 관리자가 해당 웹사이트의 이용자로부터 온라인상의 개인식별정보를 수집하는 것이 위법라다고 규정하고 있다. 또한 이 법안은 '수집'의 의미에 대해 '수집 방법이 직접적이든 간접적이든, 능동적이든 수동적이든 상관없이 일정한 수단에 의해 서비스나 웹사이트의 제공자나 운영자가 인터넷 서비스, 온라인 서비스 또는 상업적 웹사이트의 이용자에 대해 그들의 개인식별정보를 모으는 것'이라고 정의하고 있다. 특히 쿠키의 이용을 포함해 서비스나 웹사이트의 이용자와 연결된 일정한 식별코드의 추적이나 이용이 있는 경우도 '수집'에 포함된다고 규정함으로써, 프로파일링을 위한 쿠키 등의 프로그램에 의한 개인정보 수집도 동법의 규제대상으로 삼고 있다.[50]

## XⅣ. 소비자 온라인 프라이버시 공개법안

'소비자 온라인 프라이버시 공개법안'(Consumer Online Privacy and Disclosure Act)은 2001년 1월 31일에 미국 하원 자원통상위원회에 그 법안이 제출되었다. '소비자 프라이버시 온라인 공개법안'은 온라인에서 개인정보의 프라이버시를 보호하기 위해 입법화되었고, 특히 프로파일링을 본격적으로 규제하고 있는 점이 특징이다. '소비자 프라이버시 온라인 공개법안'은 개인 정보의 수집, 공개, 이용과 관련된 불공정 사기행위에 대해 규제하며 인터넷 프로파일링의 금지를 규정하고

50) 최경진 외 5인, 앞의 책, 46-47면

있다. 따라서 웹사이트나 온라인 서비스 관리자는, 고지 시에 프로파일링 업무에 대해 개인에게 분명하게 공개하지 않고, 제3자가 영구쿠키를 설치하도록 하기 위해 개인에게 사전 동의 기회를 주지 않는다면, 개인의 인적 프로파일링을 개발하기 위해 제3자가 영구쿠키를 설치하는 것을 허용치 못하게 하고 있다.[51]

## XV. 기 타

미국에서는 의료 분야의 개인정보 보호를 목적으로 하는 법률은 제정되지 않았지만 의료분야의 개인정보에는 정보주체에 대해 일반적인 개인식별정보 이외에 진료기록이나 유전자에 관한 정보 등, 매우 중요한 정보가 포함되어 있는 경우가 많다. 이런 이유로 의료분야의 개이정보를 다루지 않으면 안 되는 상황이 되어 가고 있다. 이러한 배경 때문에 최근 들어 의료분야의 개인정보 보호에 미국이 적극적인 자세를 보여 1999년에 유전자 정보 보호를 포함한 '신기술 시대의 의료프라이버시 법안'(Medical Privacy in the Age of New Technologies Act of 1999)가 제출되는 등 의료정보에 대한 개인정보 보호활동이 활발히 이루어지고 있다. 이렇듯 미국에서 의료분야의 개인정보를 엄격하게 보호하려는 것은 의료에 대한 여러 가지 기록에의 접근 및 보호의 문제가 중요할 뿐만 아니라 유전자 정보 보호 등의 문제가 앞으로는 개인정보 보호의 핵심적인 과제가 될 것이기 때문이다.[52]

또한 미국에서는 민감하지 않은 데이터에 대한 정의는 내리고 있지 않지만 유럽에서와 마찬가지로 민감한 정보에 대해서는 정의를 내리고 있다. 미국에서 민감한 정보로 보는 것은 인종, 종교, 성적 취향, 정치, 건강 등이다. 이러한 민감한 정보에 해당하는 데이터를 수집, 활용하기를 원할 경우에는 데이터 제공자의 동의가 반드시 요구된다.

51) 최경진 외 5인, 위의 책, 47면
52) 김상겸 외 5인, 앞의 책, 27-28면

그리고 연방거래위원회는 데이터를 안전하게 처리하거나 유통하지 않는 데이터 베이스나 웹사이트 등의 매체에 대해 소비자보호법(Consumer Protection Law)를 적용시킨다. 연방거래위원회는 이미 오프라인과 온라인의 데이터 활용에 대해 위반 회사를 규제한 바 있고 웹사이트와 같은 매체에서 흐라이버시 보호의 방침이 없을 경우에는 '불공정 상거래 관행'(Unfair Commercial Practices)의 범위 내에서 이를 처리한다.[53]

## 제 4 절 세이프하버원칙과 자율규제론

### Ⅰ. 자율규제론

인터넷상의 프라이버시 보호, 그 중에서도 전자상거래와 프라이버시의 보호가 최근에 특히 문제가 되고 있다. 미국에서는 전자상거래와 프라이버시 보호에 대해 일반적으로 사업자의 자율규제로 이를 해결하려는 경향이 나타나고 있다. 1996년 6월에 연방거래위원회는 '새로운 하이테크 세계시장에서의 소비자 보호'(Consumer Protection in New Hi-tech Global Market)라는 제목으로 보고서를 제출하고 사이버 공간에서 프라이버시 침해의 위험성 문제를 제기하였으며, 1998년 6월에도 '온라인 프라이버시'(On-line Privacy)라는 보고서를, 1999년에 7월에는 '자율규제와 온라인의 프라이버시'라는 보고서를 각각 연방의회에 제출하였다. 그리고 2000년 6월 및 7월에는 '온라인의 프로파일링에 관하여'라는 제목의 보고서가 제출되었는데 이 보고서에서는 자율규제와 자율규제 지원 입법의 필요성이 크게 강조되었다. 이 '온라인의 프로파일링에 관하여'라는 보고서에서는 온라인에서 정보를 수집·이용하는 사업자는 그러한 행위를 소비자에게 고지할 것, 소비자에게 그러한 행위를 면할 수 있는 선택의 여지가 보장될 것, 수집된 정보에 대해 소비자에게 접근권과 진실 확인의 권리가 보장될 것, 사업자

53) 김상겸 외 5인, 위의 책, 29면

에게 정보의 비밀 보호와 정확성 확보를 위한 조치를 요구할 수 있을 것 등의 4원칙이 강조되고 있다. 그리고 또한 이의 집행을 위해 실효적 메카니즘의 필요성을 강조하고 있다. 미국에서는 프라이버시 준수 운영방안의 표준을 제시하고 일정 조건을 만족하는 업체에 “BBB 온라인 마크”나 “TRUSTe” 등의 인증마크를 주는 제도를 시행해 오고 있다. 정부와 비영리단체는 ‘프라이버시 정책’(Privacy Policy)을 작성해 홈페이지에 게시하여 그들 기관의 개인정보 취급방침에 대해 상세히 설명하고 있다.[54]

## Ⅱ. 세이프하버원칙

미국 상무부는 1998년 11월에 개인정보 보호를 위한 7가지 항목의 기준으로서 세이프하버원칙(Safe Harbor Principles)을 제시했다. 이것은 EU와의 무역을 위한 장벽을 제거하기 위해 EU가 제시하는 개인정보 보호기준을 준수하는지를 판가름하는 기준으로 제시된 것이었다. 그리고 이 원칙을 준수한 미국기업은 EU 기준에 적합한 개인정보 보호에 충실한 기업으로 추정되어 이후 아무런 제재 없이 EU와의 개인정보를 이전할 수 있도록 하기 위한 원칙이었다. 이 원칙은 미국산업계에 개인정보보호에 과한 원칙을 자율적으로 준수할 것을 권고하는 것이면서도 개인정보 보호와 관련해 빚어진 EU와의 통상마찰을 타개하기 위한 전략이기도 하였다. 동 원칙은 1998년 11월 4일의 초안 발표 이후 5차례의 개정을 거쳐 2000년 5월 31일에 EU회원국 만장일치로 그 내용에 대한 승인을 받았으며 같은 해 6월 9일에 최종안이 발표되었다. 세이프하버 원칙에서는 수집하는 개인정보의 유형, 해당 정보의 수집방법, 당해정보의 수집목적, 조직체의 유형, 당해 조직체가 정보주체에게 당해 정보의 이용과 공개를 제한할 수 있는 선택권과 조치

54) 성낙인 외 9인, 앞의 책, 481-482면

를 제공하고 있음을 알려주도록 규정하고 있다. 세이프하버원칙을 구체적으로 살펴보면 다음과 같다.[55]

1. 고지 (Notice)

고지는 최초의 정보 수집 시나 혹은 그 이후에 가능한 한 빨리 이루어져야 한다. 그러나 사전에 통지해야 하는 경우도 있는데, 최초 수집 목적 이외의 용도로 사용하는 경우나 최초로 제3자에게 정보를 공개하는 경우가 그것이다.[56]

2. 선택 (Choice)

개인정보의 제3자에 대한 공개나 최초 수집목적 이외 사용의 경우에는 정보 주체에게 그에 대한 선택의 기회가 제공되어야 한다. 일반적으로는 '오프트 아웃'(opt-out)방식을 취할 수 있지만 민감한 정보이면 '오프트 인'(opt-in) 방식을 택해야 한다.[57]

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

제3자에게 정보를 게시한다면 통지와 선택에 관한 원칙을 지켜야 한다. 기업은 대리인으로 활동하는 제3자에게 정보를 전송할 경우에 그 제3자가 세이프하버 원칙에 가입했거나 EU 지침이나 기타 적절한 방법을 따르거나, 최소한 그 제3자와 세이프하버 원칙의 조항들이 요구하는 만큼의 프라이버시 보호를 한다는 서면협정을 체결해야 한다. 그리고 제3자가 이런 요건을 충족한다면, 기업은 제3자가 제한사항 등에 위반하여 정보 처리를 하고 있음을 알았거나 알 수 있었을 경우, 제3자의 처리를 예방하기 위한 적절한 조치가 취해지지 않은 경

55) 최경진 외 5인, 앞의 책, 44-45면
56) 최경진 외 5인, 위의 책, 45면
57) Id.

우를 제외하고는, 제3자가 일정한 제한사항 등에 위반하여 정보를 처리하는 것에 대해 기업이 책임을 지지는 않는다.[58]

4. 안전 (Security)

기업은 개인정보 관련 기록을 생성, 유지, 이용 혹는 보급하는 경우에 손실과 오용, 비인가 접근, 공개, 변경이나 파기로부터 개인정보의 주체를 보호하기 위해 합리적 예방조치를 취해야 한다.[59]

5. 데이터 무결성 (Data integration)

세이프하버 원칙에 부합하도록 개인정보와 사용목적 사이에 연관성이 존재해야 한다. 원래의 수집 목적 또는 개개인이 이후 동의한 목적과 양립할 수 없는 방법으로 기업은 정보 처리를 할 수 없다. 그러한 목적에 의해 필요하면 기업은 정보의 애초 목적에 맞는 사용, 완전성, 정확성, 최신성을 보장하는 합리적인 조치를 취해야 한다.[60]

6. 접근 (Access)

개개인은 자신의 개인 정보에 접근하여 다른 사람의 프라이버시가 손상되지 않고 그 비용이 개인의 프라이버시에 비해 크지 않은 범위 내에서 이를 수정하거나 삭제할 수 있어야 한다.[61]

7. 강제 (Enforcement)

프라이버시 보호가 효과적으로 이루어지려면 원칙 준수를 확실히 강제하고 원칙을 준수하지 않아서 영향 받는 개인을 위한 청구권, 원칙

58) Id.
59) Id.
60) 최경진 외 5인, 위의 책, 46면
61) Id.

을 준수하지 않은 기업에 이루어지는 제재 등을 확보할 수 있는 시스템을 갖추어야 한다. 최소한 이런 시스템은 첫째, '원칙 및 관계 법령 혹은 민간이 설정해 산정한 손해액"에 따라 분쟁이 조사되고 처리되며 쉽게 이용할 수 있고 독립적이며 경제적으로 쿤 부담이 되지 않은 구제 수단과, 둘째, 프라이버시 처리 관련 관행에 대한 산업계 주장 등이 진실하고, 그러한 관행이 현재에도 이행 중임을 확인할 수 있는 계속적인 절차, 셋째, 원칙 준수를 약속한 기업이 원칙을 준수하지 않음으로써 발생된 문제를 해결하기 위한 의무, 그리고 그러한 기관에 대한 제재를 포함해야 한다. 기업의 원칙 준수를 보장하기 위하여 제재조치는 엄격해야 한다. 그리고 자체 검증 보고서를 해마다 제출하지 않으면 세이프하버 원칙의 적용을 받는 보호 대상으로부터 제외된다.[62]

## 제 5 절 전자정부법상 프라이버시 영향평가제도

### Ⅰ. 서 설

2002년 12월 공포된 '전자정부법'(E-Government Act of 2002, Public Law No: 107-347) 제28조를 통해 미국은 국민 중심의 전자정부를 구현해내는 과정에서 개인정보와 프라이버시가 충분하게 보호되도록 '프라이버시 영향평가'(Privacy Impact Assessment)를 실시하도록 이를 명문화하였다. 프라이버시 영향평가제도는 각종 전자정부 사업을 추진하면서 그 전자정부 사업이 프라이버시에 어떤 영향을 미치는지를 사전에 조사하여 전자정부 사업 추진과정에서 일어날 수 있는 국가기관의 개인 프라이버시 침해를 최소화하려는 데에 그 목적이 있다.[63]

62) Id.
63) 성낙인 외 9인, 앞의 책, 484-484면

## Ⅱ. 전반적인 내용

프라이버시 영향평가는 첫째, 신원 확인이 가능한 정보를 수집, 관리, 유지, 배포하기 위해 정보기술을 개발 혹은 조달하는 경우, 둘째, 정보기술을 사용해 수집, 관리, 유지, 배포될 정보를 새로이 수집하는 경우, 셋째, 연방 정부기관, 연방 정부기관의 대행기관 또는 그 직원을 제외한 10인 이상의 자에 대해 신원 확인 문제가 제기되거나 신원에 대한 보고의무가 부과되는 때에 특정 개인에 대해 물리적 접촉 혹은 온라인 접속을 허용하는 신원 확인이 가능한 모든 정보를 새로 수집하는 등의 업무를 수행하기 이전에 실시해야 한다(§208(b)(1)(A)). 예산관리처장은 지침을 통하여 평가되는 정보시스템의 규모라든지, 그 시스템에서 개인 식별을 가능하게 하는 정보의 민감성, 그 정보의 무단 공개로 인하여 초래되는 위험성에 대해 프라이버시 영향평가가 이루어질 수 있도록 해야 한다(§208(b)(2)(B)(i)). 또한 영향평가에서는 수집하려는 정보, 그 정보를 수집하는 이유, 그 정보를 수집하는 용도, 그 정보를 공유할 기관, 수집하는 정보의 내용과 정보 공유방식과 관련해 정보주체의 동의를 얻기 위한 고지 절차, 정보보호의 방안, 프라이버시보호법에 의한 기록 체계의 생성여부에 대한 사항을 다루어야 한다(§208(b)(2)(B)(ii)).[64]

## Ⅲ. 평가의 기관 및 절차와 평가결과의 공개

전자정부 관련 사업을 수행하는 개별 기관들은 필요한 범위 안에서 프라이버시 영향평가를 수행해야 한다.(§208(b)(1)(B)(i)) 또한 기관장의 결정에 의해 정보화 책임관이나 이에 준하는 공무원은 프라이버시 영향평가를 검토하여야 한다(§208(b)(1)(B)(ii)). 그러나 공개의 경우에도

64) 성낙인 외 9인, 위의 책, 484면

보안상 이유나 혹은 프라이버시 영향평가에 포함된 민감정보나 개인정보를 보호하기 위해 공개에 관한 사항을 변경하거나 공개 자체를 배제할 수 있게 했다(§208(b)(1)(C)). 전자정부 기금 출연이 필요한 시스템의 경우에는 그 기관이 이에 대한 프라이버시 영향평가서 한 부를 예산관리처장에게 제출해야 한다(§208(b)(1)(D)). 이와 같은 대상에 관해 평가대상이 되는 정보시스템의 규모, 그 시스템에서 신원 확인을 할 수 있게 하는 정보의 민감성, 그 정보의 무단공개가 야기하는 위험에 대해 평가하게 되며, 평가 결과는 가능한 범위 내에서 이를 공개하도록 하고 있다(§208(b)(1)(B)(iii)).[65]

## Ⅳ. 예산관리처장의 임무

예산관리처장은 기관의 프라이버시 영향평가를 수행하기 위한 정책과 지침을 개발하며, 프라이버시 영향평가의 시행을 범정부적 차원에서 감독한다. 그리고 적절하다고 판단되는 범위 안에서 각 기관에 대해 기존 정보시스템이나 신원 확인이 가능한 정보의 계속적인 수집에 대한 프라이버시 영향평가를 수행한다(§208(b)(3)(C)).[66]

## Ⅴ. 프라이버시 영향평가제도에 대한 평가

미국은 최근에 위에서 살펴본 바와 같이 프라이버시 보호를 강화하기 위한 방편으로 2002년의 전자정부법에서 정부기관이 전자정부 사업을 추진하기 전에 그 전자정부사업이 개인정보 및 프라이버시에 미치는 영향을 분석하고 평가하여 대책을 마련할 것을 의무화하는 프라이버시 영향평가제도를 명문화하였는데, 이것은 미국이 개인 프라이버시 규제에 대한 필요성과 중요성을 인식하고 그에 맞게 빠르게 대응하고 있음을 보여준다.[67]

65) 성낙인 외 9인, 위의 책, 485면
66) Id.
67) 김상겸 외 5인, 앞의 책, 26면

## 제 6 절 입법체계에 대한 평가

미국의 개인정보 보호에 대한 입법은 점진적으로 그리고 사후적으로 이루어지고 있다고 평가할 수 있다. 또한 그 규율방식도 공공부문과 민간부문이 분리된 채로 분야별로 개별법이 제정되는 개별법주의의 경향을 띠고 있다. 이런 이유로 개인정보 보호에 대한 법률은 많지만 질적으로 충분한 보호는 확보되지 않고 있다는 지적이 많다. 또한 적용범위가 협소하여 이로 인한 법적 공백은 여러 군데에서 발견되고 있다. 예를 들어 연방법률은 연방기관의 업무 기록, 비디오 대여기록, 케이블 텔레비전 기록 그리고 주의 자동차 기록을 규제하지만, 주정부와 지방 자치단체의 공무원들이 보관하고 있는 대부분의 기록들은 물론이고 도서관, 슈퍼마켓, 백화점, 자선단체, 우편 주문목록, 서점 주인이 보유하는 다수의 기타 기록들을 확보하고 규제하지는 못한다. 또한 여러 법률들에서는 매우 제한된 범위의 개인정보에 대해 제한적인 형태의 통제권한만을 부여하고 있고, 이러한 규정들마저도 실효성 담보를 위한 장치들을 확보하지 못한 경우도 적지 않다. 그리고 만약 개인정보의 유통이 복잡한 경로를 거쳐 이루어진다면 그러한 경우에 법집행의 효율성을 확보하는 데 어려움이 있는 것도 사실이다. 또한 무엇보다도 개인정보가 언제 어디에서 어떻게 수집, 축적, 유통되는지를 알아내는 것부터가 쉽지 않은 일이다. 가령 그 정보가 부당하게 취급되고 있다는 사실을 인지한다 하더라도 관련 법을 위반한 자가 누구인가를 정확히 밝혀내는 것은  곤란한 경우가 적지 않다.[68]

이 외에도 국외 이전 개인정보의 강화가 문제될 수 있다. 미국에서 국외로 이전하는 개인정보에 대해 별도의 보호장치를 마련해 두지 않고 있다. 그러나 유럽연합은 자국민의 개인정보를 보호하기 위해 개

68) 성낙인 외 9인, 앞의 책, 486면

인정보를 제3국이나 국제기구로 이전하고자 한느 경우에 개인정보처리자나 프로세서가 2012년 'EU규제'(EU Regulation)에 따라 처리하는 것을 조건으로만 허용된다. 따라서 개인정보를 국외로 이전하고자 하는 경우에는 원칙적으로 EU 집행위원회나 개인정보 보호기구의 사전심사와 승인을 받아야 한다. 그런데 미국은 EU와는 달리 국외 이전 개인정보에 별도의 보호장치가 없다는 점이 문제점으로 제기될 수 있다.[69]

또한 미국은 인터넷 접속 정보의 처리제한과 관련해 인터넷접속정보, 인터넷프로토콜 주소, 로그 기록, 사물의 위치정보 등이 개인정보에 해당하는지 여부를 여전히 개인정보의 해석에 맡기고 있어 문제다. 즉 다른 정보와 쉽게 결합해서 특정 개인을 식별할 수 있는 조건에 있는지 여부에 따라 개별적으로 판단하고 있는 것이다. 이에 반해 EU는 이를 입법적으로 해결하고 있는데, 2009년 개정 EU ePrivacy Directive는 이른바 크키 정보의 수집과 이용을 제한하는 규정을 두고 있다.[70]

고유식별정보의 처리 제한과 관련해 미국은 공공서비스나 상거래 혹은 온라인 활동에 있어서 우리나라에서와 달리 실명과 고유식별정보를 요구하고 있지 않다. 주민등록번호가 없고 납세의무, 사회복지, 운전면허 등을 목적으로 고유식별번호가 부여되지만 분야별로 부여되어 있어서 오남용 가능성이나 데이터베이스의 프라이머리 키 값으로 사용하기에는 영속성이 부족하다. 이러한 사정에도 불구하고 미국에서는 사회보장번호(Social Security Number: SSN)가 광범위하게 사용되고 있다. 정부기관이나 기업들이 의료기록, 건강보험 계좌, 근로자 카드, 은행 계좌, 신용 계좌, 대학 학생증, 복지시설에서 사회보장 업무와는 상관없이 사회보장번호가 수집되고 있다. 이 때문에 미국에서도 사회보장번호의 분실, 도용, 상업적 매매가 큰 사회문제로 대두되고

69) 김상겸 외 5인, 앞의 책, 46면
70) 김상겸 외 5인, 위의 책, 62면

있다. 아직까지 사회보장번호의 매매를 금지하거나 수집과 이용을 제한하는 연방법률은 제정되지 않았으나 최근 몇 년 사이만 하더라도 사회보장번호의 상업적 매매를 금지하는 법안이 여러 개 발의되었다. 이 법안들 때문에 합법적으로 활동하고 있는 대다수 브로커들이 자율적으로 사회보장번호의 매매 관행을 축소하고 있고, 미국의 일부 주의 주법은 기업이 사회보장번호를 요구하는 것을 제한하거나 사용방법을 규제한다.[71]

71) 김상겸 외 5인, 위의 책, 99면

# 제 5 장 빅데이터의 활용과 개인정보 보호의 조화를 위한 미국의 노력

## 제 1 절 미국의 개인정보 감독기구와 빅데이터

미국에는 독립적인 개인정보 보호기관이 없다. 다만 공공부문에서는 예산관리처(Office of Management and Budget; OMB)가, 민간부문에서는 연방거래위원회(Federal Trade Commission; FTC)가 간접적인 의미에서 개인정보 보호 및 감독기관으로서의 역할을 수행한다. 예산관리처는 과거 우리나라의 기획예산처와 비슷한 기능을 수행하는데, 프라이버시 보호와 관련해서는 예산 관리의 측면에서 제한적인 기능만을 수행하고 있다. 연방 프라이버시법에 의하면, 예산관리처장은 연방 프라이버시법 규정의 시행에 의견 표명을 하고 지침 제정을 하며, 기관의 정보 사용을 규제하는 권한을 가진다(§552a(v)(1)). 또한 기관들에 의한 연방 프라이버시법의 적용을 지원하고 감독할 권한을 가진다(§552a(v)(2)). 그러나 연방 프라이버시법의 집행에 대해서는 각 정부기관의 장이 책임을 지는 것으로 되어 있고, 예산관리처가 그 이행에 관한 감독을 부분적으로만 수행한다. 또한 연방거래위원회는 소비자 보호를 위해 소비자의 프라이버시를 보호하는 기능을 함께 수행한다. 특히 소비자의 신용정보, 아동의 온라인 프라이버시, 공정거래의 관행에 대한 개인정보 보호 관련 법규를 집행하고 그 준수 여부를 감독할 권한을 가진다. 그러므로 전반적으로 볼 때, 미국에서는 프라이버시 보호에 대한 포괄적 권한을 가지는 감독기관은 존재하지 않는다고 말할 수 있다.[72]

2012년 2월에 오바마 대통령은 '네트워크 세계에서의 소비자정보프라이버시: 글로벌 디지털경제에서의 프라이버시 보호 및 혁신 촉진을

72) 김일환, 『개인정보보호법제의 정비방안에 관한 연구』, 한국법제연구원, 1997년, 191면 참조.

위한 기본구상’을 발표하였다. 그리고 그 때 ‘소비자 프라이버시 권리장전’(A Consumer Privacy Bill of Rights)을 제안했다. 이것은 개인정보와 관련된 개인의 권리와 그에 따라 기업에게 부과되는 기업의 의무를 설정하고자 하는 것이었다. 이 때 미국 내외에서 인정되는 공정한 정보실행원칙이 개인의 권리의 기초가 된다. 이러한 권리장전은 개인정보의 상업적 이용에 적용되며 이 때 개인정보란 ‘특정 개인과 관련 있는 모든 정보’를 뜻한다. 이에 따르면 소비자에게 보장되는 권리들 중에서 ‘최소수집의 원칙’(focused collection)에 따라 기업은 개인정보를 폐기치 말아야 할 의무를 지지않는 이상 개인정보가 더 이상 불필요한 경우 그 개인정보를 확실히 폐기하거나 비식별 처리해야 한다고 선언하였다. 또한 백악관은 소비자프라이버시 강화를 위해 의회에 법률 제정을 촉구했다. 이와 관련된 법안으로는 2011년 2월 11일에 캘리포니아 주하원의 의원인 스파이어(Jackie Speier)가 발의한 ‘온라인추적금지법안’(Do Not Track Me Online Act of 2011, H.R. 654)과 동년 4월 12일에 캘리포니아 주상원의 의원들이 발의한 ‘온라인 프라이버시 권 보호 법안’(Commercial Privacy Bill of Rights Act of 2011, S.799)을 들 수 있다. 전자에 의하면, 소비자는 광고대상을 특정한 타겟 광고를 위해 사용되는 온라인 추적으로부터 옵트아웃을 할 수 있게 되어 있다.[73] 다음에서는 이에 대해 보다 자세한 사항을 살펴보기로 한다.

## 제 2 절 연방거래위원회의 개인정보 보호를 위한 보고서

### Ⅰ. 서 설

미국 연방거래위원회는 인터넷 상에서 방대한 양의 개인정보를 자신도 모르게 노출 당하고 있는 인터넷 사용자들의 프라이버시 보호를

73) 최경진 외 9인, 위의 책, 49면

위해 2012년 3월 26일에 ‘급소간 변화의 시대에 맞춘 소비자 개인정보 보호’(Protecting Consumer Privacy in an Era of Rapid Change)라는 제하의 보고서를 발간했다. 연방거래위원회는 이 보고서에서 사업자가 이용자의 개인정보 보호를 위해 적용해야 하는 구체적인 프레임워크와 개인정보 정책을 위한 권고안을 제시한다.[74]

## Ⅱ. 내 용

### 1. 추적금지(Do-Not-Track) 옵션 제공의 강제

이 보고서는 ‘추적금지’(Do-Not-Track) 옵션의 제공을 강제하고 있다. 이 때 ‘추적’(Tracking)이란 인터넷 이용자의 행동 및 구독습관 기록을 공간, 가상공간, 시간 등과 연결시킬 수 있는 정보를 습득하는 행위를 의미한다. 이를 통하여 소비자의 개인정보를 임의로 가공해서 사업자간에는 일종의 상품가치를 가질 수 있기 때문에 개인정보의 중요성이 커지고 있다. 이러한 추적금지 옵션 강제 조항은 인터넷 이용자와 사업자간의 발·수진 정보의 대응방법에 대해 미국 정부가 정책적으로 대응하기 위한 조항이라고 할 수 있다. 또한 추적금지 옵션 강제조항은 사용자들이 직업 개인정보 추적의 수준을 제한할 수 있도록 ‘브라우저 벤더들’(Browser Venders)에게 추적금지 옵션을 제공하도록 강제한다. 이 때 추적금지 옵션은 이용자가 개인정보 수집을 거부할 선택권을 갖게 하는 시스템이다. 이용자가 이 시스템 하에서 자신의 개인정보 추적 수준을 제한할 수 있는데 이에 대해 구글이나 페이스북 등의 주요 기업들은 추적금지 버튼을 도입할 예정에 있다. 기술적인 면에서 봤을 때, 이용자가 컴퓨터 웹을 통해 정보를 송수신할 때, 컴퓨터 요청문에 ‘헤더’(header)라 불리우는 작은 정보를 가지게 되는데 이 헤더에는 사용자가 이용하고 있는 웹브라우저, 사용자 컴

74) 김상겸 외 5인, 앞의 책, 35면

퓨터의 언어 설정, 그 외에 기술적 세부정보들을 포함하고 있다. 추적 금지는 이 헤더에 컴퓨터 언어로 'Do-Not-Track'라는 의사표시 내용을 포함되게 하여, 이용자가 원하면 원클릭 버튼을 통해 이용자 본인의 이용내역이 추적되지 않도록 명령문을 실행하게 된다.[75]

2. 기업의 '설계단계 프라이버시'(Privacy by Design) 도입 촉구

'설계단계 프라이버시'(Privacy by Design)는 개인정보 보호를 위해 설계단계에서부터 이용자의 프라이버시를 고려해야 한다는 의미이다 개인정보 보호를 위한 설계단계에서부터 기업이 서비스와 상품의 성격 및 개인정보 주기를 반영한 취급방침을 마련하고, 마련된 개인정보 취급방침을 통하여 개인정보의 기술적 보호, 목적에 합당한 보유기간 설정, 최소한 정보 수집, 정보의 정확성 유지, 개인정보 파기 방침 등을 보장하도록 하고 있다.

3. 데이터 브로커 규제

정보 수집에 있어서의 투명성 강화를 위해 '중앙집권적으로 관리할 수 있는 웹사이트'(Centralized Website)를 만들어 데이터 브로커들을 공개하고 그들로 하여금 사용자의 개인정보를 수집하는 방법 등에 관해 밝힐 것을 요구했다. 그리고 사용자가 데이터 브로커가 수집한 정보에 접근할 수 있도록 해 줄 것을 의회에 요청했다.[76]

4. 자율규제 시행을 위한 코드(Self-Regulatory Code)

이 보고서는 기업과 개인정보 보호를 주장하는 시민단체가 자율규제 시행을 위한 기준을 마련할 것을 요구하고 실제로 기준이 마련되면 연방거래위원회가 이것이 집행될 수 있도록 조력할 것을 촉구했다.[77]

75) 김상겸 외 5인, 위의 책, 36-37면
76) 김상겸 외 5인, 위의 책, 38면
77) Id.

### 5. 이용자의 선택권 강화

개인정보를 수집하거나 수집 목적 이외로 이용하거나 특정 목적을 위해 이용자의 민감정보를 수집할 때에는 이용자의 동의를 구해야 하며 기업은 이용자에게 강요가 아니라 선택권의 보장을 제공해야 한다. 그리고 행태정보를 수집하는 사업자는 추적금지(Do-Not-Track) 기술과 같이 이용자가 정보수집 여부를 선택할 수 있는 시스템을 제공해야 한다.[78)]

### 6. 개인정보 취급방침의 투명성 증진

기업이 이용자에게 개인정보 취급방침을 알릴 때 명화하고 간결하며 표준화되어 있어야 한다고 권고하고 있다. 특히 표준화에 대해 연방거래위원회는 각 산업분야별로 수집하는 정보와 정보의 다양성은 인정하지만, 정보주체인 이용자의 명확한 이해를 돕기 위해 미국 상무성 주도하에 개인정보 관련 용어 및 취급방침의 표준화에 대해 논의를 진행하기로 했다. 그리고 개인정보의 성격에 따라 차별적인 접근권을 보장하도록 했다. 특히 연방거래위원회 보고서는 이를 세 가지 경우로 나누어 설명하고 있다. 첫째, 상품 및 서비스를 제공하는 업체의 경우에는 이용자의 개인정보에 대하여 업체가 수집해 보관하고 있는 개인정보의 목록을 공개하도록 하고 있다. 둘째, 은행, 보험, 고용 등 업무적 이용의 경우에는 이용자에게 자기정보에의 접근권과 정정요구권을 보장하도록 하고 있다. 셋째, 최근에 시장이 급격하게 커지고 있는 검색엔진이나 SNS의 경우에는 사업자가 이용자에게 수집 정보의 종류와 수집 경로를 공개하도록 권고하고 있다.[79)]

78) 김상겸 외 5인, 위의 책, 37-38면
79) 김상겸 외 5인, 위의 책, 39면

## 제 3 절 오바마 정부의 소비자 프라이버시 권리장전

### Ⅰ. 배경과 프레임워크의 네 가지 요소

미국의 오바마 정부는 2012년의 새로운 온라인 프라이버시에 대한 프레임워크를 발표하였다. 그리고 그 배경으로 미국의 소비자들은 그들의 개인정보가 안전하다는 확신을 줄 수 있는 명확한 룰을 더 이상 기다릴 수 없는 실정이고, 인터넷이 발전함에 따라 소비자의 개인정보 관리에 대한 신뢰는 디지털 경제의 지속적인 성장에 필요적인 점을 들었다. 그러면서 2012년 2월 23일 미국의 오바마 행정부가 2010년 발표된 상무성 소속 인터넷정책 TF팀의 그린페이퍼에 기초하여 세계 디지털 경제의 성정과 변화를 도모하면서도 동시에 소비자의 프라이버시 보호를 개선시킬 수 있는 청사진으로 '온라인 프라이버시 프레임워크'(Consumer Data Privacy in a Networked Wolrd: A Framework for Protecting Privacy and Promoting Innovation in the Golbal Digital Economy)를 발표하였다. 이 '온라인 프라이버시 프레임워크'의 핵심내용은 디지털시대에서의 신뢰유지가 온라인상의 경제활동을 보호하는 것이며, 소비자들의 신뢰 제고를 위해 기술적이고 관리적인 차원에서 개인 사생활의 보호가 아주 중요하다는 점을 밝힌 것이다. 이러한 오보마 정부의 소비자 권리장전 프레임워크에는 네 가지 중요한 요소가 포함되어 있다. 첫째, 소비자를 위한 온라인 프라이버시 권리장전의 제정, 둘째, 인터넷업체 그룹, 소비자 스룹 등의 다양한 이해관계인의 합의를 통한 온라인 프라이버시 권리장전에 부합하는 실효적인 법규의 제정, 셋째, 미국 거래위원회 법집행의 강화, 넷째, 정보 장벽을 낮추기 위한 세계 여러 나라와의 프라이버시 기준의 상호 운용성 고려가 그것이다.[80]

80) 김상겸 외 5인, 위의 책, 30-31면

## Ⅱ. 소비자 프라이버시 권리장전의 일곱가지 원칙

소비자 프라이버시 권리장전은 다음과 같은 소비자의 일곱 가지 권리를 보호하는 것을 핵심으로 하고 있다.

### 1. 자기정보통제권(Individual Control)

소비자는 자기 자신에 대한 정보권의 주체자이다. 따라서 개인정보 수집기관의 수집정보의 유형과 이용방법 등에 관한 통제권을 가진다. 이에 대해 기업은 소비자가 쉽게 이용하고 접근가능한 서비스를 제공하지만, 개인정보 수집과 이용에 대해 소비자가 직접 선택할 수 있게 지원해야 한다. 기업은 최근에는 사생활 보호를 강화하는 '추적금지'(Do-Not-Track) 기술을 통해 소비자가 자신의 개인정보를 통제할 수 있게 지원하고 있다.[81]

### 2. 투명성(Transparency)

소비자는 개인정보 보호와 보안 실무에 대한 정보를 알 권리를 가진다. 가장 적절한 시기와 장소에서 소비자들은 사생활 침해 위험과 관련된 의미있는 정보를 제공받아 개인별로 이를 통제할 수 있어야 하기 때문이다. 이에 대해 기업은 소비자가 수집하는 정보, 정보 수집의 필요성, 정보 이용방법, 정보 삭제 등에 대한 설명의무를 부담한다. 또한 사생활 보호 관련 서비스의 소비자 접근을 높이기 위해 일기 쉽고 효과적인 방법을 제공해야 한다. 또한 최근에는 스마트기기의 발전으로 휴대전화를 사용하는 경우가 많으므로 이런 특성을 고려해 휴대전화 이용자를 위한 효과적인 정보 구독방법을 제시해야 한다.[82]

81) 김상겸 외 5인, 위의 책, 31-32면
82) 김상겸 외 5인, 위의 책, 32면

### 3. 맥락의 존중(Respect for Context)

소비자는 일관된 맥락에서 기업의 개인정보 수집, 이용, 공개가 이루어지도록 기대할 권리를 가진다. 기업은 소비자에게 미리 공지한 것과 같은 방식으로 정보를 활용하며 개인정보 공개를 최소화해야 하는 의무를 부담한다. 기업이 개인정보를 목적 이외로 이용하거나 공개할 경우에는 투명성 침해로 간주하여 사건 발생 즉시 기업을 고발할 수 있다. 따라서 기업은 소비자의 나이와 교양수준 등에 따라 적절한 방침을 적용하여야 한다.[83]

### 4. 보안성(Security)

소비자는 자신의 개이정보에 대해 안전하고 신뢰할 수 있는 수준의 보안이 이루어지도록 요청할 수 있는 권리를 가진아. 이에 대해 기업은 개인정보에 대한 무단접근, 이용, 파괴, 수정, 공개 등을 방지할 보안대책을 수립해야 한다.[84]

### 5. 접근성 및 정확성(Access and Accuracy)

소비자는 데이터의 민감도와 위험도를 감안하여 적절한 방법과 이용가능한 형태로 개인정보에 접근하고 이를 수정할 수 있는 권리를 가진다. 또한 기업은 합리적인 방법을 통해 개인정보를 보유하고 관리할 의무를 진다. 소비자가 자신에 대한 개인정보를 수정, 삭제할 것을 요구할 때, 기업은 소비자가 사전에 수집한 소비자의 개인정보에 접근할 수 있도록 해야 하며 소비자가 자신의 개인정보에 대해 접근, 수정, 삭제를 요구할 때 가장 적절한 방법으로 개인정보를 다루어야 한다.[85]

---

83) 김상겸 외 5인, 위의 책, 33면
84) Id.
85) 김상겸 외 5인, 위의 책, 34면

### 6. 책임성(Accountability)

소비자는 기업이 소비자 개인정보 인권선언을 준수하고 소비자의 개인정보를 적절한 방법으로 처리하도록 할 권리를 가진다. 이에 대해 기업에게는 소비자와 정부가 그러한 권리를 시행할 수 있도록 할 의무가 발생한다. 기업은 직원에게 그러한 책임이 있음을 잘 알려야 하고 이에 따른 개인정보 취급이 이루어지도록 교육하고 평가해야 한다. 또한 개인정보 침해사고가 발생하며 '책임성'의 개념에 따라 계약상의 의무를 다하지 못한 데 따른 법적 처벌이 뒤따른다.[86]

### 7. 최소수집의 원칙(Focused Collection)

소비자는 기업의 개인벙보 수집과 보유에 대해 합리적인 제한을 가할 수 있다. 이에 대해 기업은 소비자정보보호법에 따라 기업 목적의 달성을 위한 최소한의 개인정보를 수집해야 하고 목적을 달성한 개인정보는 안전하게 삭제해야 한다.

86) 김상겸 외 5인, 위의 책, 35면

# 제 6 장 결 론

이상에서, 미국에서의 빅데이터 '활용'과 정책 및 법제를 지식행동화 데이터, 빅데이터 연구와 개발 이니셔티브, 개방형의 표준화된 정부정보 채택 행정명령, 정부 데이터 개방 실행계획을 중심으로 살펴보고, 미국에서의 빅데이터 '규제'와 정책 및 법제에 대해서는 온라인 프라이버시 프레임워크, 소비자 프라이버시 권고, 빅데이터와 프라이버시 워킹 그룹 권고, 과학기술자문위원회 권고를 중심으로 살펴보았다. 그리고 빅데이터 활용에 일종의 한계를 드리우는 개인정보 보호 관련 법제에 대해서도, 연방프라이버시법을 위시한 공공부문에서의 개인정보 보호 입법과 사적 부문에서의 개인정보 보호입법으로 나누어 살펴보았다. 그리고 나서는 최근 미국에서 이루어지고 있는 빅데이터 기술의 활용과 개인정보 보호의 조화를 도모하기 위한 노력들을 연방거래위원회의 개인정보 보호를 위한 보고서와 오바마 정부의 소비자 프라이버시 권리장전을 중심으로 살펴보았다. 아무쪼록 미국의 경험과 그 경험을 통해 만들어진 정책과 법제에 대한 이러한 연구가 우리나라가 앞으로 빅데이터 활용 정책과 법제를 만듦에 있어 적지 않은 시사점을 줄 수 있을 것을 기대한다.

법과 현실 사이의 괴리, 그리고 법과 기술 사이의 괴리가 커지면 커질수록 그 피해는 국민들에게 돌아간다. 그러므로 환경의 변화에 대처하면서도 빅데이터의 활용을 최대한 보장하고 프라이버시권 등 국민의 권리도 보호할 수 있는 균형 잡힌 빅데이터 관련 정책과 법제의 정비가 절실히 요망된다고 할 것이다.

# 참 고 문 헌

## 1. 국내문헌

강경근, “정보보호의 헌법규범적 접근과 전망”,『공법학연구』 제6권 제2호, 한국비교공법학회, 2005

계희열,『헌법학(상) (신정2판)』, 박영사, 2005

고영삼,『전자감시사회와 프라이버시』, 도서출판 한울, 1998

권건보,『개인정보보호와 자기정보통제권』, 경인문화사, 2005

권영성,『헌법학원론(개정판, 2005년판)』, 법문사, 2005

권형준, “자기정보통제권에 관한 고찰”,『헌법학연구』제10집 제2호, 한국헌법학회, 2004. 6

김갑중,『디지털시대의 정보 프라이버시』, 학영사, 2003

김동희,『행정법 I』, 박영사, 2001

김민정・김성숙,『디지털 경제와 소비자』, 태일사, 2005

김범환,『(인문사회분야 학생을 위한) 정보통신경제론 디지털 경제론』, 청목출판사, 2001

김상겸,『개인정보보호법 정비방안 연구』, 한국인터넷법학회, 2012. 12.

김연수,『개인정보보호 고도 지식정보 사회의 개인정보와 Cyberlaw』, 사이버출판사, 2001

김일환, “개인정보 공동이용의 통제와 감독에 관한 비교법적 고찰 - 미국과 독일의 법제를 중심으로”,『헌법학연구』제13권 제2호, 한국헌법학회, 2007. 6

김종호,『국가정보보호법의 필요성과 기본방향』, 경희대학교 출판국, 2004

김철수,『헌법학개론 (제18전정신판)』, 박영사, 2006

박윤흔,『행정법강의(상)』, 박영사, 2001

백윤철・이창범・장교식,『개인정보보호법』, 한국학술정보, 2008

성낙인,『헌법학(제7판)』, 법문사, 2007

성낙인,『언론정보법』, 나남출판, 1998

_____, “행정상 개인정보보호”,『공법연구』제22집 제3호, 한국공법학회, 1994

이관기,『알권리와 프라이버시 - 전통적 대립과 정보사회의 갈등』, 한국교육문화원, 1993

이민영,『개인정보법제론』, 진한M&B, 2005

이인호, “한국 정보법의 발전동향 정보공개법과 개인정보보호법을 중심으로”,『공법연구』제35집 제4호, 한국공법학회, 2007. 6

임홍빈,『기술문명과 철학』, 문예출판사, 1995

전석호,『정보사회론: 커뮤니케이션 혁명과 뉴미디어(개정4판)』, 나남, 2004

정종섭,『헌법학원론(제2판)』, 박영사, 2007

정필운, “미국의 빅데이터 정책 및 법제”,『빅데이터 법제 제1차 워크숍 자료집』, 한국법제연구원, 2014

최 영,『뉴미디어시대의 네트워크 커뮤니케이션』, 커뮤니케이션북스, 1998

한상희, “정보화와 헌법”,『법학논문집』 제26집 제2호, 중앙대학교 법학연구소, 2002. 11

홍준형, 『행정법총론』, 한울, 1997

홍준형, 『법정책의 이론과 실제』, 법문사, 2008

허 영, 『한국헌법론』, 박영사, 2001

## 2. 외국문헌

Anthony. Giddens, *Social Theory and Modern Sociology,* Cambridge, UK: Polity Press, 1987

Barbara S. Wellsberry, "Bridging the Difference: The Safe Harbor and Information Privacy in the United States and the European Union," *Privacy and Information Law Report*(1 NO. 6 Privacy Info. L. Rep. 13), 2001

Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective,* Ashgate, 2003

Colin J. Bennett, *Regulating Privacy : Data Protection and Public Policy in Europe and the United States,* Ithaca : Cornell University Press, 1992

Colin Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?," *Technology And Privacy: The New Landscape* 99, Phillip E. Agre & Marc Rotenberg eds., 1997

Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," 53 *Stanford Law Review* 1393, 2001

Daneil J. Solove & Paul M. Schwartz, *Information Privay Law*, 4th ed., Wolters Kluwer Law &Business, 2011

David Banisar/Simon Davies, “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments”, 18 *J. Marshall J. Computer & Info. L.* 1, 1999

David Harvey, *The Condition of Postmodernity - an Enquiry into the Origins of Cultural Change,* Cambridge, Mass: Blackwell, 1989

David H. Flaherty, *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press, 1989

David W. Leebron, “The Right to Privacy's Place in the Intellectual History of Tort Law”, 41 *Case W. Res. L. Rev*. 769, 1991

Douwe Korff, *Data Protection Law in the European Union*, DMA, 2005

Erik Brynjolfsson and Brian Kahin, *Understanding the Digital Economy Data, Tools, and Research,* Cambridge, Mass.: MIT Press, 2000

M. Ethan Katsh, *The Electronic Media and the Transformation of Law,* New York: Oxford University Press, 1989

Executive Office of the President &President’s Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective,* May 2014

Fred H. Cate, *Privacy in the Information Age*, Brookings Institution Press, 1997

Henry H. Perrit Jr., *Law and the Information Superhighway*, Wiley Law Publications, 1996

Herbert J. Spiro, “Privacy in Comparative Perspectives”, in: *Privacy Nomos* XIII, J. Roland Pennock & John W. Chapman eds., 1971

James Michael, *Privacy and Human Rights,* Hampshire: Dartmouth, 1994

Janlori Goldman, Zoe Hudson, and Richard M. Smith, California Health Care Foundation, *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*, Jan. 2000

Joel R. Reidenberg, “A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace”, 52 *Stan. L. Rev*. 1315, 1342, May, 2000

Joel R. Reidenberg, “Restoring Americans' Privacy in Electronic Commerce”, 14 *Berkeley Tech. L. J*. 771, 1999

Joel R. Reidenberg, “Privacy Protection and the Interdependence of Law, Technology and Self-Regulation”, *23rd International Conference on Data Protection Commissioners*

John Locke, *The Second Treatise of Government*(1690), Thomas P. Peardon ed., Liberal Arts Press, 1952

Joseph I. Rosenbaum, “Privacy on the Internet: Whose Information is it Anyway?”, 38 *Jurimetrics* 565, 1998

J.W.K. Burnside, “The Fundamentals of Computer Technology,” Gordon Hughes(ed.), *Essays on Computer Law,* Melbourne, Australia: Longman Professional, 1990

Lynn Margherio, *The Emerging Digital Economy*, Washington, D.C.: U.S. Department of Commerce, 1998

Nigel Waters, “Re-thinking Information Privacy - A Third Way in Data Protection?”, *21st International Conference on Privacy and Personal Data Protection,* 1999. 9. 13

Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection*, Michie Law Publishers, 1996

Peter Knight and James Fitzsimons, *The legal environment of computing,* Sydney Reading, Mass: Addison Wesley Pub. Co., 1990

Peter Carey, *Blackstone's Guide to Data Protection Act* 1998, Blackstone Press, Ltd, 1998

Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Data Protection Directive* , 1998

Philip Agre, "Introduction", in: *Technology and Privacy: The New Landscape,* Philip E. Agre & Marc Rotenberg eds., 1997

R. Gellman, "Conflict and Overlap in Privacy Regulation: National, International, and Private", in: B. Kahin & C. Nesson (eds.), *Borders in Cyberspace,* MIT Press, 1997

R. Clayton · H. Tomlinson, *The Law of Human Rights,* Oxford University Press, 2000

Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", 4 *Harv. L. Rev*. 193, 1890

Swift, Ronald, "The new economic opportunity for business-creating increased profitability through CRM," *CRM Project*, 2, 2001

Thomas C. Cooley, *Laws of Torts,* 1st ed. 1880

William L. Prosser, "Privacy", 48 *Cal. L. Rev*. 383, 1960

Yves Poullet, “Data Protection Between Property and Liberties: A Civil Law Approach”, in: *Amongst Friends in Computers and Law,* H.W.K. Kaspersen & A. Oskamp eds., 1990