

미국의 프라이버시와 개인정보보호

-개인정보보호에 대한 유럽연합과의 차이를 중심으로-

A Study on a Unique and Distinctive Culture (Law and Understanding) Regarding the Protections for Privacy in the U.S.

정 혜 련*
Jung, Hye-Ryun

목 차

- | | |
|----------------------------|---------------------------|
| I. 들어가며 | IV. 프라이버시 및 개인정보 보호에 대한 국 |
| II. 미국의 프라이버시와 개인정보 보호 | 제적인 논의 |
| III. 미국에서의 개인정보 보호: 법원과 규제 | V. 맺으며 |
| 기관 | |

미국에서의 사생활 공개에 관한 프라이버시의 보호, 곧 개인정보 보호는 “연방과 주의 여러 개별적인 법들이 서로 합쳐진 형태(patchwork)로 일정한 개인정보의 프라이버시를 보호한다. 미국은 공공 및 민간주체가 보유하는 개인정보를 보호하는 연방차원의 일반법은 존재하지 아니 한다. 민간주체가 개인정보를 수집하고 공개하는 것에 대하여 의회는 전반적으로 대처한 것이 아니라 개별적인 분야에 따라 대처해 왔기 때문에 미국의 법제는 원칙적으로 개인정보를 보호하는 것이 아니라 특별히 규율하는 분야의 개인정보만을 예외적으로 보호한다. 따라서 대부분의 개인정보는 이러한 개별적인 분야에 포함되지 않으므로 대부분의 개인정보가 법률에 의하여 보호받지 않는다. 따라서 개인정보를 보호하는 미국의 법제는 개별적인 분야마다 상업적인 이익과 프라이버시에 대한 이익과의 조화와 균형을 중시한다.

이에 반하여 유럽연합은 소비자와 프라이버시에 보다 더 치중하는 접근방법과 일반법

투고일 : 2016. 8. 31. / 심사외퇴일 : 2016. 9. 20. / 게재확정일 : 2016. 10. 13.

* 홍익대학교 법과대학 겸임교수, 법학박사(SJD)

Adjunct Professor, College of Law, Hongik University

에 의하여 규율하고 있다고 할 수 있다. 즉 유럽은 프라이버시를 기본권으로 파악하고 있다. 달리 말하면, 기본권이라고 하여 다른 권리에 우월하다는 것은 아니지만 경제적인 권리가 프라이버시보다 우월하지는 않은 것으로 파악하고 있다.

이처럼 미국은 개인정보 보호를 위한 일반법이 존재하지 않으며, 의료, 금융, 신용평가 등 개인정보가 사용되는 특정 산업이나 특정 분야에서 초점을 맞춘 법률에 의하여 개별적으로 협소하게 규율되고 있을 뿐이다. 이에 반하여, 유럽연합은 공공 및 민간을 모두 규율하는 일반법에 의하여 광범위하게 규율한다. 또한 EU는 프라이버시를 기본권으로 바라보고 있으나 미국은 표현의 자유와 같은 다른 이익과 균형을 이루어야 하는 것으로 바라보고 있다. 또한 유럽연합의 개인정보법제는 법적 근거가 없는 경우에는 개인정보의 처리를 금지하지만, 미국의 개인정보법제는 피해를 야기하거나 법에 의하여 제한되지 않는 한 일반적으로 개인정보를 처리하도록 허용하고 있다.

이처럼 미국의 프라이버시와 개인정보 보호에 관한 현황을 살펴보는 것은 중요한 의미가 될 수 있다. 왜냐하면 과거에서부터 미국은 프라이버시에 대한 개념과 정의를 다양하게 하고 있기 때문이다. 이 글에서 살펴본 바와 같이, 유럽에서의 프라이버시에 대한 정의는 미국과는 다르다. 따라서 이 글에서는 미국의 프라이버시와 개인정보 보호에 관한 현황을 소개하고, 유럽과 그 외의 국가들의 프라이버시와 개인정보보호에 관한 논의와 현황을 미국과 비교하여 살핀다.

[주제어] 프라이버시, 개인정보, 연방거래위원회, 사생활 결정권, 개인정보 결정권, 기본권, 프라이버시 권리

I. 들어가며

디지털 시대의 등장으로 더욱 빠르게 발전하는 인터넷 환경¹⁾에서 인터넷 이용자의

1) 1990년 가정으로 인터넷이 보급되고, 1995년 eBay와 Amazon이 사업을 시작하면서 온라인 고객이라는 기존의 오프라인 고객과는 대비되는 집단이 등장했다. 더불어, Netflix와 Zappos는 더 광범위한 온라인 고객층을 만들어 냈다. 1998년 Yahoo와 Lycos에 이어서 Google이 새로운 검색엔진을 통해 사람들에게 단순한 정보검색을 넘는 다양한 콘텐츠를 제공하기 시작하면서, Google은 동시에 인터넷 상의 개인행동에 대한 방대한 데이터를 수집하게 되었다. 2003년 당시 SNS(Social Networking Service)로서 My space가 선전하기 시작하였으며, 2004년에는 Chris Sharpley의 소셜미디어(social media)라는 표현으로 대변되는 Facebook이 등장하여 인기를 얻기 시작한다. 이러한 사이트들은 더욱 더 방대한 개인에 대한 디지털 데이터를 축적하기 시작했다. 더욱이, 언제 어디서나 인터넷 접속이 가능한 스마트폰(Smart phone)의 등장으로 인하여 데이터의 집적속도를 가속화 하였다. 현재는 사용자의 위치가 그 장치의 위치로 대변될 뿐만 아니라, 심지어 그 사용자에게 경고 없이도 위치정보가 그대로 노출되고 있는 상황이다. 이 외에도 Skype와 MSN 메신저 그리고 SMS (Short Message Service) 역시 소셜미디어와 같이 그 사용량이 점점 늘어나는 추세이다. Cameron Chapman, "The History of the Internet in a Nutshell", *Six Revisions*, November 15, 2009, <<http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/>>. 미국에서 VOD와 DVD 우편 대여 서비스를 제공하는 회사로 잘 알려진 Netflix는 2500만

프라이버시 침해가 빈번히 발생하고 있다. 이에 대응하여 2012년 오바마 행정부는 인터넷 이용자 프라이버시 보호를 위하여 새로운 프라이버시 프레임워크를 발표하기도 했다.²⁾ 이 프레임 워크에 의해 만들어질 법안들은 소비자뿐만 아니라 기업에게도 중요한 의미를 가지게 될 것이다. 오바마 행정부의 프레임워크 발표 후, 온라인 광고업계는 방문자의 추적 중지 요청 버튼 (Do Not Track)³⁾을 만들어 이용자에게 자신의 정보수집에 대하여 인지 및 통제를 할 수 있도록 하겠다고 발표하였다.⁴⁾ 이와 같이 이용자의 프라이버시에 대한 새로운 인식과 보호를 위한 시도를 통해 새로운 법적 장치가 갖춰질 것이며, 이로써 개인정보가 노출될 수 있는 위험은 줄어들 것이다.

하지만 미국에서는 수년간 정책과 입법의 변화과정에서 기존의 프라이버시 보호 방식에 문제점⁵⁾이 드러나기 시작하였으므로, 여전히 이에 대한 구체적인 해결책이 제시되어

명 이상의 대규모 회원을 보유하고 있으며, 미국 인터넷 트래픽의 30% 이상을 점유하고 있다. <<http://www.netflix.com/>>, 온라인 신발 판매 1위 업체인 재퍼스닷컴(Zappos.com Inc.)은 2009년에는 10억 달러를 넘는 매출을 기록했다. 300만 켤레에 달하는 신발을 재고로 보유하고 모든 구매자들에게 익일 무료 배송을 제공한다. 엔지니어링에서 지속적인 온라인 고객 환경 개선과 창고 로봇 시스템 조율에 이르기까지, 재퍼스의 모든 부문에 IT가 활용된다. <http://www.zappos.com/>; Pew Research Center, "Pew Internet and American Life Project, Internet Trend Data", <<http://www.pewinternet.org/Static-Pages/Trend-Data/Online-Activities-Total.aspx>>; BBC, "Google 'in breach' of UK data privacy agreement", July 27, 2012, <<http://www.bbc.co.uk/news/technology-19014206>>. SNS(Social networking Service)란 일반적으로 온라인상에서 불특정 타인과 관계를 맺을 수 있는 서비스를 칭한다. 이용자들은 SNS를 통해 인맥을 새롭게 쌓거나, 기존 인맥과의 관계를 강화시킨다. 국내의 대표적인 SNS로는 '싸이월드'를 들 수 있다. Terence Craig & Mary Ludloff, *Privacy and Big Data*, 2011, p. 3; Adam Singer, "49 Amazing Social Media, Web 2.0, and Internet Stats", *The Future Buzz*, January 12, 2009, <<http://thefuturebuzz.com/2009/01/12/social-media-web-20-interst-numbers-stats/>>; Opera Software Press Release, "Who's Watching You", January 28, 2011, <<http://www.opera.com/press/release/2011/01/28/>>; Wikipedia, "SMS (Short Message Service)", <<http://en.wikipedia.org/wiki/SMS>>.

- 2) Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, Feb. 2012, <<http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>>.
- 3) "Digital Advertising Alliance (DAAD) Comments on Microsoft Decision to Embed Do Not Track in IE 10 Set 'on' by Default", Business Wire, May 31, 2012, <<http://www.businesswire.com/news/home/20120531006914/en/Digital-Advertising-Alliance-DAA-Comments-Microsoft-Decision>>.
- 4) 기업들의 프라이버시 보호를 위한 노력의 일환으로 자체적으로 온라인 프라이버시 정책을 만들어서 이 기준에 충족하도록 하고 있다. 예를 들어서, TRUSTe <http://learn.truste.com/content/search_amer_privacy_brand_learnmoreq211?campaign=7018000000tc5k&campaign_theme=privacy&campaign_tactic=keyword_amer_privacy_google_brand_exact_learnmore&leadsource_detail=keyword_amer_privacy_google_brand_exact_learnmore&le>, Verisign <<http://www.verisign.com/>>, BBBOnline(<<http://www.bbb.org/us/bbb-online-business/>>).
- 5) 오바마 정부의 프레임워크에서, 정보제공자가 아닌 다른 자로부터의 취득한 정보에 대한 제한이 없다는 점과 제공된 정보를 이용할 때에 그 목적에 적합한지를 판단하는 범위가 확대되어 있다는 점이 문제로 지적되고 있다. David Goldman, "Obama's big idea: Digital health records", CNNMoney, January 12, 2009, <<http://cs.gmu.edu/~mlocasto/research/securehealth/content/CNN-digital-health-records.pdf>>.

야 할 것이다. 먼저 개인의 프라이버시 보호와 기업의 빅 데이터⁶⁾ 활용 사이에서 균형 내지 형평성을 찾아야 한다는 점이다. 다시 말해서, 개인의 정보보호 측면만이 강조되어 빅 데이터의 활용을 통한 산업의 발전뿐만 아니라 기업과 이용자를 위한 새로운 기술의 개발이 제약을 받아서는 안될 것이다. 궁극적으로 개인의 자유와 혁신을 통한 사회적 발전은 모든 법적 장치 사이에서 균형을 잃지 않아야 한다. 다만 개인정보에 대한 통제권은 그것을 다루는 기업과 같은 제3자가 아닌 그 정보제공자 자신에게 있어야 한다는 근본적인 원칙은 어떤 경우에도 변함이 없어야 한다.

위와 같은 문제점들에 대하여 미국의 프라이버시와 개인정보 보호에 관한 현황을 살펴보는 것은 중요한 의미가 될 수 있다. 왜냐하면 과거에서부터 미국은 프라이버시에 대한 개념과 정의를 다양하게 하고 있기 때문이다. 또한 유럽에서의 프라이버시에 대한 정의는 미국과는 다르다. 따라서 이 글에서는 미국의 프라이버시와 개인정보 보호에 관한 현황을 소개하고, 유럽과 그 외의 국가들의 프라이버시와 개인정보보호에 관한 논의 및 현황을 살핀다.

II. 미국의 프라이버시와 개인정보 보호

1. 프라이버시 보호의 헌법상 근거

미국의 연방헌법은 프라이버시에 대한 권리를 명시적으로 규정하고 있지 않으며 연방 대법원도 ‘일반적인’ 프라이버시권을 선언한 적이 없으나, 연방대법원은 프라이버시권이 헌법상 묵시적으로 보장된다고 인정하고 있다. 연방대법원이 사생활결정에 관한 프라이버시의 보호를 헌법상의 권리로 처음 인정한 것은 1965년의 *Griswold v. Connecticut* 사건⁷⁾에 의한 것이었다. 이 사건에서 연방대법원은 결혼한 남녀의 피임약(기구) 사용을 금지시키는 코네티컷주의 법이 프라이버시에 대한 권리를 위반한 것이라고 하면서, 프

6) 빅 데이터는 기존 데이터 베이스만으로는 처리가 불가능한 정도의 대용량 정보의 집합의 의미를 넘어, 이 정보의 수집, 분석, 발굴까지 포함하는 개념이다. 즉, 빅 데이터는 네트워크에 접속하여 활동하는 개인이 매 순간 노출할 수 밖에 없는 다양한 비정형 데이터들을 수집, 분석, 발굴하여 새로운 정보로 가공하는 모든 일련의 작업을 말한다. Berkman Center for Internet and Society, Harvard University, “A History of Digital Data Creation”, <http://cyber.law.harvard.edu/digitaldiscovery/timeline_files/frame.htm>.

7) 381 U.S. 479, 1965.

라이버시에 대한 권리는 연방 헌법상의 여러 기본권 규정에 의하여 묵시적으로 인정된다고 판시하였다.⁸⁾ 이후 *Roe v. Wade* 사건⁹⁾에서 연방대법원은 프라이버시권이나 프라이버시의 일정영역(zones of privacy)을 보장해주는 것이 헌법의 수정조항(표현의 자유에 관한 제1 수정헌법, 제4 및 제5 수정헌법 등)에 포함되어 있고, 여성이 낙태하는 것에 대하여 프라이버시권을 가진다고 한 *Whalen v. Roe* 사건¹⁰⁾에서는 사생활 공개를 회피하고 중요한 사항을 독자적으로 결정하는 것에 대한 2가지 유형의 프라이버시 이익이 있다고 하였다.

연방대법원이 프라이버시에 대한 권리를 헌법상 묵시적으로 존재하는 것으로 인정하였더라도 사생활결정에 관한 프라이버시와 개인정보 자기결정에 관한 프라이버시에 대하여 인정하는 헌법상의 지위는 다르다. 연방대법원이 사생활결정에 관한 프라이버시를 인정한 것으로는 피임과 낙태를 결정하는 것에 관한 *Griswold v. Connecticut* 사건과 *Roe v. Wade* 사건을 들 수 있다. 연방대법원이 비록 헌법상 명문으로 규정되어 있지 않더라도 여러 기본권 규정에 보호된다고 한 프라이버시가 바로 의사결정에 관한 프라이버시이다. 따라서 사생활결정에 관한 프라이버시의 헌법상의 지위는 명확하게 인정된 것이다.

그러나 개인정보 자기결정에 관한 프라이버시의 헌법상 지위는 매우 약하다. 현재까지 개인정보 자기결정에 관한 연방대법원 판례는 3개이다. *Whalen* 사건은 개인정보가 공개되지 않는 것에 대하여 개인이 이익을 가진다는 것을 처음으로 인정한 사건이자 개인정보 자기결정 프라이버시에 관한 사건이다. 연방대법원은 일정한 의약품에 대한 처방전을 주 정부에 제공하도록 요구하는 뉴욕주법의 위헌성을 부인하면서도, 프라이버시에 대한 헌법상의 권리는 사적 문제에 대한 개인의 의사자치 뿐만 아니라 매우 개인적인 정보를 공개하는 것을 방지하는 것에 이익도 존중한다고 판시하였다. *Whalen* 사건에 의하여 개인정보자기결정권이 연방대법원에 의하여 인정된 것처럼 보이지만, “일정한 상황 하에서 개인정보의 원치 않는 공개를 방지할 법적·규범적 의무가 헌법에 그 근거가 있다고 주장할 수 있다는 것을 인정”한다고만 함으로써 개인정보자기결정권의 의미나 범위 등을 명확하게 논의하지 않았다. 이러한 논조는 *Nixon v. Administrator of General*

8) 헌법상의 기본권 규정은 표현의 자유와 같이 기본권을 명시적으로 보호하기도 하지만, 특정의 기본권을 명시하지 않고 마치 ‘(일식이나 월식 때 비치는) 옅은 빛(penumbra)’의 형태로도 보호하는데, 여기에 속하는 것 중의 하나가 바로 정부에 의한 간섭으로부터 보호받는 프라이버시에 대한 권리라는 것이다. *Id.* at 483, 484.

9) 410 U.S. 113, 1973.

10) *Whalen v. Roe*, 429 U.S. 589, 1977.

Services 사건¹¹⁾에도 이어졌는데, 연방대법원은 프라이버시를 구성하는 요소 중의 하나는 개인적인 문제를 공개하는 것을 방지하는 것에 대하여 개인이 가지는 이익이라고 하면서, 다만 프라이버시에 대한 권리는 정부가 가지는 이익과 균형이 이루어져야 한다고 판시하였다. 그러나 연방대법원은 “최소한 정부의 이익이 관련되는 경우, 대통령을 비롯한 공인은 공직상 자신이 한 행위와 관계되지 않는 개인적인 삶의 문제에 대하여 프라이버시권으로 헌법상 완전히 보호받지 않는 것이 아니라는 것에 대하여 동의할 수 있다”고 하여 개인정보 자기결정권이 헌법상 인정된다고 가정하는 방식으로 판시하였다. 이후 30여년이 지난 2010년 연방대법원은 *NASA v. Nelson* 사건¹²⁾에서 약물 사용 여부, 약물사용으로 인한 치료 및 상담여부, 정직성이나 신뢰성 기타 부정적인 정보를 가지고 있는지 여부의 질문에 대한 개인정보 자기결정 프라이버시에 대한 헌법상 권리가 침해되지 않았다고 판시하면서도 개인정보 자기결정 프라이버시에 대한 헌법상의 권리의 존재 여부에 대한 판단은 훗날로 미루었다.¹³⁾

1970년대에 개인정보 공개 프라이버시에 관한 *Whalen* 및 *Nixon* 사건 이후 개인정보를 공개하지 않는 것에 대하여 헌법상의 프라이버시권이 존재하는지 여부는 모호하다.¹⁴⁾ 미국 연방대법원이 개인정보 자기결정 프라이버시에 대한 헌법상의 ‘일반적인’, ‘광범위한’ 권리가 존재한다고 인정하지 않은 것은 분명하다.¹⁵⁾ 그렇다고 연방대법원이 이러한 권리가 존재하지 않는다고 하지 않았으며 그 존재를 인정한 것도 분명하다. 2010년도의 *NASA* 사건이 이러한 불명확한 상태를 해결한 것도 아니다. 그러나 과반수이상의 연방항소법원이나 많은 숫자의 주법원들은 개인정보 자기결정 프라이버시권에 대하여 헌법상의 권리가 존재한다고 가정하여 헌법상의 지위를 부여하는 것으로 알려지고 있다.¹⁶⁾ 이러한 상태는 연방대법원이 개인정보 자기결정에 관한 프라이버시에 대한 헌법상의 권리 인정에 대한 명확한 입장을 밝힐 때까지 계속될 것이다.

미국에서 개인정보 자기결정 프라이버시권의 헌법상 지위를 논의하는 실익은 미국에서 개인정보의 보호범위나 법체제와 관련이 있다. 곧 개인정보 자기결정 프라이버시의

11) *Nixon v. Admin. of Gen. Servs.*, 433 U.S. 425, 1977.

12) *Nelson, et al. v. NASA, et al.*, 530 F.3d 865 (9th Cir. June 20, 2008).

13) *Id.* 756-757, 763-764.

14) *Am. Fed’n of Gov’t Employees, AFL-CIO v. Dep’t of Hous. & Urban Dev.*, 118 F.3d 786 (D.C. Cir. 1997).

15) *NASA v. Nelson* 사건에서 *Scalia* 대법관은 동의의견을 통하여 개인정보 자기결정 프라이버시에 대한 헌법상의 권리가 존재하지 않는다고까지 하였다. *Id.* at 764.

16) *Mary J. Fan, Constitutionalizing Informational Privacy by Assumption*, 14 U. Pa. J. Const. L. 953, 974-975, 2012.

보호는 한국이나 유럽연합에서의 개인정보의 보호에 해당하는 것이고, 따라서 미국에서 헌법상 일반적인 권리의 지위를 가지지 않는다는 것은 결국 미국에서 개인정보는 헌법상의 지위라기보다는 법률의 지위에 의해서만 보호된다는 것을 의미한다. 실제로 미국에서의 개인정보 자기결정에 대한 프라이버시의 보호, 곧 개인정보의 보호는 연방 및 주 법률, 불법행위, 지적재산권 등에 의하여 보호되는데, 다만 개인정보 전반을 규율하는 일반법에 의해서가 아니라 지엽적인, 부분적인 분야에서만 보호된다.

2. 개인정보 보호의 의미

미국의 프라이버시에 대한 정의와 분류는 매우 다양하다. 이런 다양한 역사적 배경 때문에 프라이버시를 더욱 이해하기 어려운 것으로 하고 있다. 또한 미국에서는 주로 프라이버시라는 개념을 중심으로 논의되고 있으나 유럽연합에서는 개인데이터, 곧 개인정보라는 개념을 중심으로 논의되고 있다. 따라서 미국과 유럽연합에서의 이러한 개념이 어떠한 차이가 있는가도 매우 모호하다. 이를 이해하기 위해서는 먼저 미국 연방헌법상 프라이버시 보호의 지위와 프라이버시를 대체로 사생활 결정 및 공개에 관한 프라이버시로 구분하여 이해하는 것이 필요하다.

미국에서 프라이버시는 1890년 Warren과 Brandeis(1916-1939 연방대법관)가 작성한 ‘프라이버시에 대한 권리’라는 논문에서 논의한 것에서 시작된다. 이들은 코먼로상 각 개인이 자신의 생각, 정서 및 감정을 타인에게 어느 정도로 전달할 것인지에 대하여 선택한 권리를 가지며, ‘혼자 있을 권리(right to be let alone)’가 불법행위법에 의하여 보호되어야 한다고 주장하였다. 이들의 주장은 학자들에 의하여 지지를 받기 시작했으나, 법원이 이를 광범위하게 수용하게 된 것은 1960년 Prosser 교수(당시 UC Berkeley 로스쿨 학장)가 프라이버시에 관한 논문을 발표하면서부터였다.¹⁷⁾

미국에서 프라이버시에 대한 권리는 1890년 Warren과 Brandeis는 프라이버시에 대한 권리를 ‘혼자 있을 권리’로 정의하면서 다양하게 정의되어 왔고, Prosser교수에 의하여 4개의 불법행위 유형으로 구분되었다. 개인의 행동영역을 기준으로 하여서는 3가지 형

17) Prosser 교수는 ① 원고의 한가함이나 고독 또는 사생활 간섭, ② 원고에 관한 난처한 개인적 사실의 공개, ③ 원고에 대한 왜곡, ④ 피고의 이익을 위한 원고의 성명이나 원고와 동일시되는 사항의 이용 등 네 가지 형태의 프라이버시 침해가 코먼로로 인정되어야 한다고 주장하였다. 프라이버시 침해에 대한 Prosser 교수의 네 가지 불법행위는 ‘불법행위 Restatement (Second)’에 규정되었고(§§652A-E), 이후 법원에 의하여 광범위하게 수용되었다.

태로 발전되어 왔다.¹⁸⁾

사생활결정에 관한 프라이버시는 개인이 혼인, 출산, 피임, 낙태, 가족관계, 자녀 양육 및 교육, 흡연 등 사적인 결정(intimate decision)에 대하여 국가나 타인으로부터 간섭받지 않고 결정하고 자신이 선택한 바에 따라 행동할 수 있는 능력을 의미한다. 따라서 이러한 프라이버시는 개인이 출산이나 양육과 같이 중요한 결정을 하는 것에 대하여 간섭받는 것으로부터의 자유를 의미하고 의사자치의 원칙(principles of autonomy)과 밀접하게 관련된다.¹⁹⁾

프라이버시를 결정 및 공개에 관한 프라이버시 양자로 구분한 것은 연방대법원의 Whalen v. Roe 사건에서 비롯된다.²⁰⁾

미국법상의 프라이버시 개념은 공간적, 사생활 결정 및 사생활 공개에 관한 프라이버시를 포함한다. 이에 반해, 유럽연합의 데이터지침이나 데이터규정에서 언급되고 있는 ‘개인데이터(personal data)’, 즉 개인정보의 개념보다 광범위하다. 유럽연합이 보호하는 개인데이터와 미국의 것은 동일하지 않지만 대체로 유사하다고 할 수 있는 것이 바로 미국법상의 사생활 공개에 관한 프라이버시이다. 사생활 공개에 관한 프라이버시는 ‘개인적인 사안(personal matters)’이나 ‘개인의 비밀적인 정보’를 ‘공개’하여 난처해지는 것으로부터 해당 개인을 보호하는 것이고, 이에 대한 명확한 정의가 내려져 있는 것도 아니므로, 개인데이터(개인정보)의 수집, 처리, 이용 등에 대하여 통제를 가하는 유럽연합의 개인데이터 보호와는 차이가 있는 것이라 할 수 있다.²¹⁾

사생활 공개에 관한 프라이버시는 정확하게 정의되지 않고 있지만 대체로 개인이 자기 자신에 대한 정보를 통제할 권리로 정의되는 것이 일반적이고, 이러한 개인정보가 유럽에서 논의되는 개인데이터와 관계되므로, 미국에서의 사생활 공개에 관한 프라이버

18) 개인의 행동영역을 기준으로 하여서는 ① 공간적 프라이버시(spatial privacy), ② 사생활 결정에 관한 프라이버시(decisional privacy), ③ 사생활 공개에 관한 프라이버시(informational privacy)의 3가지 형태로 발전되어 왔다. 이 중에서 ‘사생활 결정에 관한 프라이버시와 ② 사생활 공개에 관한 프라이버시 양자의 의미와 이들을 구별하는 것은 미국에서의 프라이버시와 유럽연합이나 한국에서 사용되는 데이터 내지 개인정보 보호를 이해하는 것과 개인정보 보호에 대한 미국과 유럽연합 및 한국법의 관계를 이해하는데 도움이 된다.

19) ‘사생활공개에 관한 프라이버시’는 개인에 대한 비밀적인 사안이 공개되지 않도록 할 능력으로서, 해당 개인을 난처하게 하거나 기타 손상시키는 방식으로 사적이거나 비밀스러운 정보를 부당하게 전파하는 것으로부터 해당 개인을 보호하는 것이다. 따라서 사생활공개에 관한 프라이버시는 개인정보의 처리(수집, 저장, 이용, 공개 등)에 대하여 통제할 권리를 의미한다.

20) 연방대법원은 프라이버시를 보호하는 사건들은 최소한 ① 중요한 결정을 독자적으로 하는 것에 대한 이익과 ② 개인적인 사안(personal matters)을 공개하지 않는 것에 대한 이익이라는 두 가지 이익을 보호하는 것과 관련된다고 하여, ① 사생활결정에 관한 프라이버시와 ② 사생활공개에 관한 프라이버시로 구별하였다.

21) 또한 Whalen 사건에서는 프라이버시를 보호하는 이익 중의 하나로서 ‘개인적인 사안을 공개하지 않는 것에 대한 이익’을 언급하였을 뿐이지 법원이 사생활공개에 관한 프라이버시를 정의한 것도 아니었다.

시는 유럽에서의 개인데이터의 보호와 유사하거나 이에 해당하는 것이라 할 수 있다. 개인이 자신에 관한 정보를 통제할 권리라는 사생활공개에 관한 프라이버시(information privacy)는 고전적인 프라이버시권의 한 유형으로서 개인의 생활을 공개하는 불법행위 그 이상으로 프라이버시 보호를 확대하는 것이다.

개인정보에 대한 통제를 의미하는 사생활 공개에 관한 프라이버시는 미국의 프라이버시법에서 중요한 획을 그었던 콜롬비아 대학의 Westin 교수가 정의한 프라이버시의 개념과 일맥상통하는 것이라 할 수 있다. Westin 교수는 프라이버시를 ‘개인, 단체 또는 기관이 자신들에 관한 정보가 언제, 어떻게, 어느 정도로 타인에게 전달되는가를 결정할 권리’라고 하여 ‘통제’를 프라이버시의 핵심적인 요소로 정의하였다. 1965년 Griswold v. Connecticut 사건과 1973년 Roe v. Wade 사건에 의하여 피임과 낙태에 대한 프라이버시, 곧 사생활 결정에 관한 프라이버시가 인정되었는데, 법으로 규율되지 않았던 정부나 민간주체에 의한 개인정보 사용을 법령화하는데 선구적인 역할을 하였다. 컴퓨터나 인터넷이 광범위하게 사용되지 않았던 시대에 Westin 교수는 이미 개인정보의 이동(flow)을 간파하여 그 필요성을 역설한 것인데, Westin 교수가 정의한 프라이버시는 사생활 공개에 관한 프라이버시라 할 수 있고 이것은 유럽에서 개인데이터(개인정보)를 보호하는 것에 해당하는 것이라 할 수 있다.

3. 프라이버시, 개인정보, 개인데이터 및 개인정보자기결정권

프라이버시를 사생활결정과 공개에 관한 프라이버시로 구분하는 것은 1990년 중반 이후 사생활공개에 관한 프라이버시를 새로운 학문의 영역으로 확립하고자 한 여러 학자들의 새로운 논의에서 비롯된다고도 할 수 있다.²²⁾ 이들 학자들은 일정한 기본적인 결정을 할 수 있는 권리인 사생활결정에 관한 프라이버시(decisional privacy)와 개인에 관한 정보를 통제할 수 있는 권리인 사생활공개에 관한 프라이버시(information privacy, informational privacy)로 구분한다. 또한 이들은 기술적인 배경과 측면에서 프라이버시 문제에 접근하고 이를 규율하는데 관심을 가지며, 사생활공개에 관한 프라이버시는 개인이 자신에 관한 정보를 통제할 권리로 정의한다.²³⁾ 이들 학자들이 주창하는 사생활공개에 관한 프라이버시는 Whalen vs. Roe 사건이 구분한 것 중의 하나인 개인적인 사안을

22) Neil M. Richards, “The Information Privacy Law Project”, 94 GEO. L. J. 1087, 1089, 2006.

23) Id.

공개하지 않는 이익에 대한 프라이버시와는 분명한 차이점이 있으며, 사생활공개에 관한 프라이버시를 보호하는 것이 유럽연합이나 한국에서 개인정보를 보호하는 것과 매우 유사하다. 따라서 이러한 프라이버시는 *Whalen vs. Roe* 사건이 구분한 개인적인 사안을 공개하지 않는 프라이버시와 구별될 뿐만 아니라 이보다 광범위한 개념의 것으로서, 개인정보 통제에 관한 프라이버시가 보다 적합한 용어라고 할 수 있다. 또한 바로 이러한 프라이버시를 보호하는 것이 한국이나 유럽연합에서 개인정보를 보호하는 것에 해당하는 것이라 할 수 있는데, 유럽연합에서는 1995년의 지침이나 2012년 제안된 규정 등을 통하여 모두 개인데이터(personal data)라는 개념을 이용하고 있다. 유럽에서의 데이터 보호는, 혼자 있을 권리를 보호하는 것이라기보다는, 개인에게 자신의 인격과 관련된 모든 데이터를 처분할 수 있는 권리를 보장하는 프라이버시 보호의 한 형태이다.²⁴⁾ 따라서 미국에서 프라이버시의 하나로서 구분되는 사생활공개에 관한 프라이버시권은 ‘개인정보 자기결정 프라이버시권’이고, 이를 보호하는 것은 개인정보 내지 개인데이터를 보호하는 것이며, 이에 대한 한국에서의 헌법상의 권리는 ‘개인정보자기결정권’이라 할 수 있다. 요컨대 미국에서의 개인정보 자기결정 프라이버시의 보호는 한국이나 유럽에서의 개인정보나 개인데이터를 보호하는 것에 해당한다. 따라서 이하에서는 이들 용어를 혼용하여 사용하기로 한다.

4. 미국과 유럽연합의 개인정보 보호의 전개

프라이버시에 관한 법이 가장 발달한 국가는 미국이다. 1890년 Warren과 Brandeis가 논문에서 프라이버시를 처음으로 논의한 이후는 말할 것도 없고, 1970년대 초반 개인정보 보호 논의를 주도한 것은 미국이다. 개인정보 보호가 시작되려는 시점인 1970년대 초반인 1973년에 미국의 보건·교육·후생부(HEW)는 1973년 ‘공정한 정보관행 규칙(Code of Fair Information Practices)’을 정하는 입법을 권고하면서 자동화된 개인데이터 시스템의 요건으로서 5개 원칙을 담은 야심적인 보고서(이하 ‘HEW 보고서’)²⁵⁾를 발표하였다. HEW 보고서의 ‘공정한 정보관행원칙(Fair Information Practices Principles, FIPPs)’²⁶⁾

24) Alessandra Suuberg, at 275.

25) U.S. Department of Health, Education & Welfare, “Secretary’s Advisory Committee on Automated Personal Data System, Foreword to Records, Computers and the Rights of Citizens”, 1973.

26) FIPPs에 대한 더 자세한 내용은, Robert Gellmann, “Fair Information Practices: A Basic History”, April 25, 2012, <<http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>>.

은 구속력이 있는 것이 아니었으나 이후 미국과 전세계적으로 정보 프라이버시에 있어서 중요한 역할을 하였다. FIPPs는 HEW의 보고서에 한정된 것이 아니라 이후 미국에서 많은 형태의 FIPPs가 나오게 되었으며, ‘1974년 프라이버시 보호법(Privacy Act of 1974)’의 제정에 영향을 미쳤고, 이후에도 정보 프라이버시 보호에 대한 미국의 주된 접근방법이 되었다.²⁷⁾ 전세계적으로도 개인데이터 처리에 관한 공통된 원칙을 담고 있는 FIP는 각 국가의 데이터보호법에 영향을 미쳤으며, OECD 가이드라인의 기초가 되었다.

그러나 1970년대에 들어오면서 유럽국가들이 개인정보를 보호하기 위하여 공공 및 민간에 모두 적용되는 일반법을 입법하고 감독과 법집행을 위한 정부기관을 설립하게 되면서, 개인정보 보호분야에 있어서 미국은 주도권을 잃게 된다. 1973년 스웨덴이 개인정보보호법을 제정한 이후 여러 국가들이 개인정보 보호에 관한 일반법을 입법함으로써 개별적인 분야에 대해서만 입법한 미국과 비교되었다. 또한 유럽위원회는 1991년 자동 처리 개인정보 보호협약을 채택하였고, 1995년에는 데이터지침을 채택하였고, 유럽 외의 많은 국가들이 유럽과 같은 일반법 형태의 개인정보 보호법을 채택하였으며, 국제적으로는 OECD가 가이드라인을 내 놓았다. 따라서 개인정보 분야에서는 유럽이 오히려 주도하는 상황이 되었다.

5. 한국 헌법상의 개인정보자기결정권

헌법상의 지위가 불확실한 미국의 개인정보 자기결정 프라이버시권과 달리, 한국에서의 이러한 권리에 해당하는 개인정보자기결정권은 헌법상의 권리로 인정되고 있다.²⁸⁾

헌법재판소 2005. 5. 26. 자 99헌마513, 2004헌마190(병합) 결정

개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.

개인정보자기결정권의 보호대상 이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.

새로운 독자적 기본권으로서의 개인정보자기결정권을 헌법적으로 승인할 필요성이 대두된 것은 다음과 같은 사회적 상황의 변동을 그 배경으로 한다고 할 수 있다.

인류사회는 20세기 후반에 접어들면서 컴퓨터와 통신기술의 비약적인 발전에 힘입어 중전의 산업사회에서 정보사회

27) Marcinkowski, at 1178.

28) 헌법재판소 2005. 5. 26. 자 99헌마513, 2004헌마190(병합) 결정.

로 진입하게 되었고, 이에 따른 정보환경의 급격한 변화로 인하여 개인정보의 수집·처리와 관련한 사생활보호라는 새로운 차원의 헌법문제가 초미의 관심사로 제기되었다.

... 이와 같은 사회적 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치라고 할 수 있다.

개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한 두개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다.

6. 미국과 유럽의 개인정보 보호의 특성 비교

미국에서의 사생활 공개에 관한 프라이버시의 보호, 곧 개인정보 보호는 다음과 같이 요약할 수 있다. 곧 “연방과 주의 여러 개별적인 법들이 서로 합쳐진 형태(patchwork)로 일정한 개인정보의 프라이버시를 보호한다. 공공 및 민간주체가 보유하는 개인정보를 보호하는 연방차원의 일반법은 존재하지 아니 한다. 민간주체가 개인정보를 수집하고 공개하는 것에 대하여 의회는 전반적으로 대처한 것이 아니라 개별적인 분야에 따라 대처해 왔다. 연방 법규범이 개인정보를 보호하는 분야는 소비자 신용도 제공, 전기통신, 연방정부 기관의 기록, 교육기록, 은행기록, 케이블가입자 정보, 비디오대여 기록, 자동차 기록, 보건정보, 정보통신 가입자 정보, 온라인상의 어린이 정보, 고객의 금융정보 등²⁹⁾ 이다.”³⁰⁾ 개인정보를 보호하는 미국의 이러한 법제는 원칙적으로 개인정보를 보호하는 것이 아니라 특별히 규율하는 분야의 개인정보만을 예외적으로 보호한다는 것을 의미하고, 따라서 대부분의 개인정보는 이러한 개별적인 분야에 포함되지 않으므로 대부분의 개인정보가 법률에 의하여 보호받지 않는다는 것을 의미한다.³¹⁾

29) Fair Credit Reporting Act of 1970 (FCRA) (42 U.S.C. §1681); Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. §§2510-2522, 2701-2711, 3121-3126); Privacy Act of 1974 (5 U.S.C. §552a); Family Educational Rights and Privacy Act of 1974 (FERPA) (45 U.S.C. §1232g); Right to Financial Privacy Act of 1978 (12 U.S.C. §3401); Cable Communications Policy Act of 1984 (47 U.S.C. §551); Video Privacy Protection Act of 1988 (18 U.S.C. §2710); Driver's Privacy Protection Act of 1994 (18 U.S.C. §2721); Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §1320d); Communications Act of 1934 (47 U.S.C. §222); Gramm-Leach-Bliley Act of 1999 (GLBA) (15 U.S.C. §§6801-6809).

30) Gina Stevens, Congressional Research Service, R41756, Privacy Protections for Personal Information Online 7, 2011.

31) Devin W. Ness, Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It, 31 CARDOZO ARTS & ENT. 925, 944, 2013.

개인정보를 보호하는 미국의 법제가 개별적인 분야마다 상업적인 이익과 프라이버시에 대한 이익을 적절하게 균형시킨 것이라고 한다면, 유럽연합은 소비자와 프라이버시에 보다 더 치중하는 접근방법과 일반법에 의하여 규율하고 있다고 할 수 있다. 곧 유럽은 프라이버시를 기본권으로 파악하고 있으며, 기본권이라고 하여 다른 권리에 우월하다는 것은 아니지만 경제적인 권리가 프라이버시보다 우월하지는 않은 것으로 파악하고 있다.³²⁾

III. 미국에서의 개인정보 보호: 법원과 규제기관

1. Consumer Privacy Bill of Rights (소비자 권리장전)

백악관의 ‘소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights)’은 전세계적으로 인정된 공정정보관행원칙(FIPPs)³³⁾을 적용시킨 것으로서 다음의 7가지를 규정하고 있다.

- (1) 개인의 통제. 소비자는 기업이 자신으로부터 어떠한 개인정보를 수집하고 이를 어떻게 사용하는지에 대하여 통제할 권리를 가진다.
- (2) 투명성. 소비자는 프라이버시 및 보안 관행에 대하여 용이하게 이해하고 접근할 수 있는 권리를 가진다.
- (3) 개인정보 제공상황의 존중. 소비자는 기업이, 소비자 자신이 개인정보를 제공하는 상황에 일치하여, 이를 수집, 이용 및 공개할 것으로 기대할 권리를 가진다.
- (4) 보안. 소비자는 개인정보를 안전하게 책임성 있게 처리하도록 할 권리를 가진다.
- (5) 접근 및 정확성. 소비자는, 개인정보의 민감성과 개인정보가 정확하지 않은 경우 소비자에게 발생할 불리한 결과의 위험성에 적절한 방식으로, 이용 가능한 형태로 개인정보에 접근하고 개인정보를 정정할 권리를 가진다.
- (6) 수집의 제한. 소비자는 기업이 수집하고 보관하는 개인정보가 합리적으로 제한이 가하여질 권리를 가진다.

기업은 개인정보 제공상황 존중의 원칙에 의하여 정해진 목적을 달성하기 위하여

32) Ness, at 945.

33) supra note 26.

필요한 만큼의 개인정보만을 수집하여야 한다. 기업은 개인정보를 더 이상 필요로 하지 않는 경우, 달리 처리하거나 개인과 식별되지 않도록 할 법적 의무가 없는 한, 개인정보를 안전하게 처리하고 개인과 식별되지 않도록 하여야 한다.

- (7) 책임성. 소비자는, 기업이 ‘소비자 프라이버시 권리장전’을 준수하는 것을 보장하기 위하여, 기업이 개인정보를 적절한 조치에 의하여 처리하도록 할 권리를 가진다.

백악관의 소비자 프라이버시 권리장전은 법률적 효과가 있는 것이 아니고 이해당사자들이 이를 행위규범으로서 실행하고 의회와 함께 입법하기 위한 것이다.

2. 연방거래위원회(FTC)

FTC가 소비자의 개인정보를 보호하기 시작한 것은 1970년대에 Fair Credit Reporting Act(FCRA)를 집행하는 것에서 비롯되는데, 이후 FTC는 법의 집행, 정책목표 제시, 소비자 및 기업 교육을 통하여 소비자의 개인정보를 보호해 오고 있다. FTC가 공정정보관행을 권고한 것은 정책목표를 제시한 것에 해당한다. FTC는 1998년 및 2000년 온라인상의 프라이버시에 대한 의회보고서를 통하여 공정정보관행(FIP)을 권고하였다. 1998년 보고서에서는 ① 통지/인식, ② 선택/동의, ③ 접근/참여, ④ 무결성/보안과 ⑤ 온라인상의 프라이버시를 보호하기 위한 정부나 자율규제 프로그램의 중요한 요소로서 준수하지 않는 것에 대한 제재를 가하는 신뢰할 수 있는 프로그램을 사용하도록 하는 집행/구제를 권고하였고, 2000년 보고서에는 ① 통지, ② 선택, ③ 접근, ④ 보안 네 가지를 권고하였다.

2.1 통지/인식(notice/awareness)

소비자가 자신에 대한 정보가 공개될 것인지 여부, 공개된다면 어느 정도로 공개될 것인지에 대하여 제대로 결정하기 위해서는, 개인정보가 수집되기 전에 기업의 정보관행이 소비자에게 통지되어야 한다. 또한 이러한 통지가 이루어져야 선택/동의 등의 원칙과 개인정보에 대한 소비자의 권리도 의미가 있게 된다. 통지는 명확하고 눈에 띄는 형태로 이루어져야 하며, 통지대상은 수집하는 정보, 수집방법, 이용방법, 선택·접근·보안 제공방법, 제3자에 대한 공개여부, 개인정보를 수집하는 사이트를 통하여 제3자가

수집하는지 여부 등이다.

2.2 선택/동의(choice/consent)

소비자가 수집된 개인정보가 어떻게 사용될 것인지, 특히 예컨대 거래를 위하여 사용하는 것 외에 내부적으로 우편발송대상에 포함시키거나 외부의 제3자에게 제공하는 등 개인정보를 2차적으로 사용하는 것에 대하여 선택할 수 있어야 한다. 선택방식은 opt-in과 opt-out이 있다.

2.3 접근/참여(access/participation)

개인이 자신에 대한 데이터에 접근(기업의 파일에 존재하는 데이터를 보는 것)하고 데이터의 정확성과 완전성에 이의를 제기할 수 있어야 한다. 이러한 원칙이 의미 있도록 하기 위해서는 데이터에 대한 적절한 시간 내의 저렴한 접근, 부정확하거나 불완전한 데이터에 이의를 제기하기 위한 간편한 수단, 데이터 수집자가 정보의 정확성을 확인할 방법, 정정하고 이의제기한 내용이 데이터 파일에 추가되어 모든 데이터 수령자에게 전달되도록 하는 수단 등이 포함되어야 한다.

2.4 무결성/보안(integrity/security)

데이터는 정확하여야 하며 데이터에 대한 보안이 이루어져야 한다. 데이터의 무결성을 보장하기 위해서는 수집자가 믿을만한 출처의 데이터만을 사용하거나 여러 출처가 있는 경우에는 교차로 체크하거나, 소비자가 데이터에 접근하도록 하거나, 시의적절하지 않은 데이터를 삭제하거나 익명의 형태로 전환하는 등 합리적인 조치를 취하여야 한다. 데이터에 대한 보안은 데이터의 멸실, 데이터에 대한 불법 접근, 데이터의 파손·이용·공개로부터 데이터를 보호하기 위한 관리적·기술적 조치를 포함한다. 관리적 조치는 데이터에 대한 접근을 제한하고 데이터에 접근할 수 있는 내부 직원이 데이터를 불법적인 목적으로 사용하지 않도록 하기 위한 내부 조직 내에서의 조치를 포함한다. 불법적인 접근을 방지하기 위한 기술적 보안조치는 송신되거나 저장된 데이터의 암호화, 비밀번호를 이용한 접근 제한, 모뎀으로는 접근할 수 없는 보안이 보장되는 서버나 컴퓨

터에 저장하는 것 등을 포함한다.

FTC의 공정정보관행은 FTC가 자체적으로 인정하는 바와 같이 불완전·불충분하며, 통지 및 선택을 강조함으로써 접근, 수집제한, 목적 명시, 데이터의 질적 적정성 및 무결성 보장과 같은 다른 공정정보관행을 충분히 고려하지 않은 것으로 비판받고 있다.³⁴⁾

3. 개인정보 보호 모델

개인정보를 보호하는 주된 방법은 ‘통지 및 선택 모델’과 ‘피해에 바탕을 둔 모델’ 두 가지로 나눌 수 있다. 전자는 소비자가 제대로 선택을 할 수 있도록 소비자에게 정보 수집과 이용관행을 설명하는 통지를 하도록 장려하는 것이다. 후자는 소비자를 신체적 안전이나 경제적 손실 등의 피해로부터 보호하는 것에 초점을 맞추는 것이다. 통지 및 선택 모델은 소비자들이 보통 읽지 않으며 읽더라도 이해할 수 없는 개인정보 정책방침을 만들도록 하는 단점이 있으며, 피해에 바탕을 둔 모델은 명예손상이나 감시당하는 고통 등 프라이버시와 관련된 보다 광범위한 문제점을 제기하지 않는 단점이 있는 것으로 비판받고 있다.

IV. 프라이버시 및 개인정보 보호에 대한 국제적인 논의

1. UN 인권선언

국제법적 측면에서 프라이버시가 처음으로 인정된 것은 1948년 UN의 ‘인권선언(Universal Declaration of Human Rights)’이었다. UN의 인권선언은 “어느 누구도 자신의 프라이버시, 가족, 가정 또는 서신에 임의적인 간섭을 받지 아니하며, 자신의 명예나 명성에 대하여 침해받아서서는 아니 된다. 누구든지 이러한 간섭이나 침해에 대하여 법의 보호를 받을 권리를 가진다”고 선언하여(제12조),³⁵⁾ 프라이버시의 중요성을 공식적으로 인정하고 타인, 특히 국가가 개인의 사적 영역에 침입하는 것으로부터 개인을 보호하고

34) Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers 20”, 2010; Robert Gellman, “Fair Information Practices: A Basic History 11”, 2013.

35) 1966년의 ‘시민·정치적 권리에 관한 국제협약(International Covenant on Civil and Political Rights)’도 이와 동일하게 규정하고 있다. §17.

자 하였다. 이에 의하여 UN은 프라이버시권을 분명히 밝혔을 뿐만 아니라 국가들이 프라이버시를 법적 권리로 인정할 것을 촉구하였다.

이후 UN은 1980년부터 컴퓨터화된 개인파일에 초점을 맞추어 개인정보를 보호하기 위한 작업을 하기 시작하였다. 마침내 1990년에 나온 ‘컴퓨터화된 개인데이터 파일 규제에 대한 가이드라인’은 공정정보관행의 원칙(적법성·공정성, 정확성, 목적 특정성, 접근, 비차별, 보안, §§1-7), 국내 개인정보기관의 설립(§8), 상응하거나 상호적인 법체제 국가 간의 데이터 이동의 허용(§9) 등을 규정하였다. UN의 가이드라인은 OECD 가이드라인이나 유럽연합의 자동 처리 개인정보 보호협약(협약 108)만큼 평가를 받지 못하고 있다. OECD 가이드라인 등은 이미 1980년대 초에 나온 이후 개인정보 보호분야에서 어느 정도의 지위를 잡은 이후인 1990년에 나온 것이 그 원인이라 할 수 있다. 그러나 UN의 가이드라인은 개인정보 보호에 관한 진정한 국제적인 문서라는 점에서 의미가 크다.³⁶⁾

2. HEW 보고서 및 공정 정보관행 규칙

프라이버시권에 대한 규율은 국가나 지역마다 매우 다르며 각 국가들은 각자의 독특한 문화나 목적을 달성하기 위하여 프라이버시법을 발전시켜왔다. 국제적인 측면에서 프라이버시에 중요한 영향을 미친 두 가지로는 1973년 미국 보건·교육·후생부(이하 HEW)의 보고서와 1980년 채택된 OECD 가이드라인이다. Warren과 Brandeis가 프라이버시에 관한 논문을 발표하였던 19세기 말은 사진기가 광범위하게 사용되어 프라이버시 논의를 촉발시켰다고 한다면 20세기 후반은 디지털기술, 컴퓨터 및 인터넷에 의하여 정보가 수집되어 합쳐지고 저장됨으로써 프라이버시가 침해될 가능성이 더 높아졌다. 미국의 보건·교육·후생부(HEW)는 1973년 ‘공정한 정보관행 규칙(Code of Fair Information Practices)’을 정하는 입법을 권고하면서 자동화된 개인데이터 시스템의 요건으로서 5개 원칙을 담은 야심적인 보고서(이하 ‘HEW 보고서’)³⁷⁾를 발표하였다.

36) Paul De Hert, Vagelis Papakonstantinou, “Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency”, *A Journal of Law and Policy for the Information Society* Vol.9 Issue2, Moritz College of Law, 2013, at 282.

37) U.S. Department of Health, Education & Welfare, “Secretary’s Advisory Committee on Automated Personal Data System, Foreword to Records, Computers and the Rights of Citizens”, 1973.

- ① 그 존재가 비밀인 개인데이터를 기록하는 시스템이 있어서는 아니 된다.
- ② 어떠한 개인에 관한 정보가 기록되어 있고 어떻게 사용되는지를 그 개인이 알 수 있는 방법이 있어야 한다.
- ③ 어떠한 목적을 위하여 획득된 개인에 관한 정보가 동의 없이 다른 목적을 위하여 이용되거나 이용제공되는 것을 그 개인이 방지할 수 있는 방법이 있어야 한다.
- ④ 식별가능한 개인에 관한 정보 기록을 그 개인이 정정하거나 수정하는 방법이 있어야 한다.
- ⑤ 식별가능한 개인데이터 기록을 작성, 유지, 사용 또는 배포하는 기관은 그 데이터가 사용되고자 하였던 것에 대하여 신뢰할 수 있도록 확인하고 데이터가 악용되는 것을 방지할 합리적인 예방조치를 마련하여야 한다.

이러한 다섯 가지 원칙을 보다 현대적인 의미로 표현하면 ① 투명성, ② 이용제한, ③ 접근 및 정정, ④ 데이터 적정성 및 ⑤ 보안의 원칙이 된다. 개인데이터 보호가 시작되려는 시점인 1970년대 초반에 나온 HEW 보고서의 ‘공정한 정보관행원칙(Fair Information Practices Principles, FIPPs)³⁸⁾은 구속력이 있는 것이 아니었으나 이후 미국과 전세계적으로 정보 프라이버시에 있어서 중요한 역할을 하였다. FIPPs는 HEW의 보고서에 한정된 것이 아니라 이후 미국에서 많은 형태의 FIPPs가 나오게 되었으며, ‘1974년 프라이버시 보호법(Privacy Act of 1974)’의 제정에 영향을 미쳤고, 이후에도 정보 프라이버시 보호에 대한 미국의 주된 접근방법이 되었다.³⁹⁾ 전세계적으로도 개인데이터 처리에 관한 공통된 원칙을 담고 있는 FIPPs는 각 국가의 데이터보호법에 영향을 미쳤으며, OECD 가이드라인의 기초가 되었다.

3. OECD 가이드라인

3.1 정보의 중요성

개인정보를 보호하기 위한 첫 국제적인 논의는 사실상 1980년의 ‘OECD 가이드라인’이라 할 수 있다. 개인정보의 보호는 1970년대에 개인정보를 집중적으로 처리하는 것이 점차 증가하고 거대한 데이터 뱅크가 설립되기 시작함으로써 개인정보 보호의 중요성이 인식된 것에 기원한다. 그런데 기본권적 시각에서 논의되는 프라이버시 보호와 달리 개인정보의 보호는 경제적인 측면에서 논의가 시작되었고 OECD 가이드라인은 이를 잘 반영하고 있다. 곧 OECD 가이드라인도 프라이버시, 개인의 자유 및 전세계적으로 정보의 자유로운 흐름의 기본가치를 증진하고 보호하는 것에 대한 이익 등을 인정하면서도, 회원국 간에 정보의 자유로운 흐름을 증진시키고 경제·사회적 관계를 발전시키는

38) Supra note 26.

39) Marcinkowski, at 1178.

데 부당한 장애가 발생하는 것을 방지하기 위하여 가이드라인을 권고한다고 밝히고 있다. 개인정보 보호는 단순히 해당 정보 주체를 보호하는 것뿐만 아니라 “정보는 경제적인 가치를 가지고 있으며 일정한 데이터를 저장하고 처리할 수 있는 능력은 국가에게 정치적·기술적 우위를 제공”하며 이것은 “궁극적으로 초국가적인 데이터 흐름을 통하여 국가주권이 상실되는 것”⁴⁰⁾에 이를 수 있을 정도로 중요한 의미를 가지고 있다. OECD는 경제성장을 촉진하고 세계무역에 기여하는 것을 목적으로 한다. 따라서 이러한 목적을 위해서는 정보의 자유로운 흐름이 필요한데 각 국가가 개인정보를 보호하기 위한 조치는 이러한 성장에 장애물이 될 수 있다. 따라서 OECD는 각 국가의 국내입법이 정보의 자유로운 흐름에 장애가 되지 않도록 하고자 하였고, 그 결과로 탄생한 것이 1980년의 OECD 가이드라인이다.⁴¹⁾

3.2 가이드라인의 원칙

OECD 가이드라인은 데이터보호에 관한 HEW 보고서의 다섯 개 원칙을 확대하였다. OECD 가이드라인⁴²⁾은 프라이버시, 개인의 자유, 및 정보의 자유로운 국제적인 이동을 촉진하고 보호하기 위한 것으로서, 이를 위한 최소한의 기준인 8가지의 원칙을 담고 있다.

- ① 수집제한의 원칙 (collection limitation principle)
개인정보⁴³⁾ 수집은 제한되어야 하며, 개인정보는 적법하고 공정한 수단에 의하여 획득되어야 하고, 적절한 경우에는 개인정보 주체의 인지도 동의에 의하여 획득되어야 한다.
- ② 데이터의 질적 적정성의 원칙 (data quality principle)
개인정보는 그 이용될 목적과 부합하여야 하며, 이러한 목적을 위하여 필요한 한도에서 정확하고, 완전하고 최신의 것으로 유지되어야 한다.
- ③ 목적 명확성의 원칙
(a) 개인정보가 수집되는 목적은 최소한 데이터를 수집할 때에 명시되어야 하고, (b) ① 수집된 개인정보는 이러한 목적을 위하여 사용하는 것에 제한되어야 하며, ㉠ 이러한 목적과 부합하는 다른 목적이나 목적이 변경되는 경우에는 변경되는 각 경우에 명시된 목적을 위하여 사용하는 것에 제한되어야 한다.
- ④ 이용제한의 원칙
개인정보는, (a) 개인정보 주체의 동의에 의하거나 (b) 법률에 의한 경우를 제외하고는, 목적 명확성의 원칙에 따라 명시된 목적 이외의 목적을 위하여 공개, 이용제공, 기타 이용되어서는 아니 된다.
- ⑤ 안전성 보장성의 원칙
개인정보는 합리적인 보안조치에 의하여 데이터의 분실되거나 불법으로 접근·훼손·이용·수정·공개되는 것과 같은 위험으로부터 보호되어야 한다.

40) John M. Eger, “Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?”, *Law and Policy in International Business Issue4*, Georgetown University Law Center, 1978, pp.1065-1066.

41) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

42) 가이드라인은 총칙, 국내적용의 기본원칙, 이행책임, 국제적용의 기본원칙, 국내이행, 국제협력 및 상호작용 등 5개의 장으로 구성되어 있다.

- ⑥ 공개의 원칙
개인정보에 관한 진행과정(developments), 관행 및 정책방향을 전반적으로 공개하는 정책이 마련되어야 한다. 데이터 통제자의 신원이나 주소, 개인정보의 존재나 성격, 개인정보를 이용하는 주된 목적 등을 정하는 수단이 제공될 수 있어야 한다.
- ⑦ 개인참여의 원칙
개인은 다음의 권리를 가져야 한다.
(a) 데이터 통제자 또는 기타의 자로부터 개인정보를 보유하고 있는지 여부를 확인받을 권리
(b) 개인정보를 ㉠ 합리적인 시간 내에, ㉡ (데이터가) 과도한 경우 (비용을 요구한다면) 비용을 지급하고, ㉢ 합리적인 방식으로, ㉣ 개인이 인식할 수 있는 형식으로, 통지받을 권리
(c) 위 (a) 및 (b)에 따른 요청이 거부된 것에 대한 근거를 제공받고 이의를 제기할 권리
(d) 개인정보에 대한 이의를 제기하고, 이의제기가 받아들여진 경우 데이터를 삭제, 정정, 보완하거나 수정할 권리
- ⑧ 책임의 원칙
데이터 통제자는 위에서 제시된 원칙을 유효하게 하는 조치를 이행할 책임이 있다.

OECD 가이드라인은 1980년 채택 이후 프라이버시 보호에 관한 새로운 접근방법이나 개인정보 이용이 변한 것에 대처하기 위하여 2013년 개정되었다.⁴⁴⁾ 개정된 내용으로는 (a) 데이터 통제자로 하여금 이행책임의 내용으로서 프라이버시 관리프로그램(privacy management program)을 마련토록 하고[§15(a)], 데이터침해에 대하여 통지하도록 하며 [§15(c)], (b) 국내이행의 일환으로서 프라이버시 집행기관 및 국가 프라이버시 전략을 마련하도록 하고 있다.

- APEC Privacy Framework (Nov. 2004)
- ① 남용으로 인한 피해의 방지
② 통지
③ 수집제한
④ 이용제한
⑤ 선택
⑥ 개인정보의 무결성
⑦ 안전성 조치
⑧ 접근 및 정정

참고표: APEC Privacy Framework⁴⁵⁾

43) 가이드라인은 ‘개인데이터(personal data)’라는 용어를 사용하면서 이를 ‘식별되었거나 식별가능한 데이터 주체에 관한 모든 정보’라고 정의하고 있는데[§1(b)], 바로 개인정보에 해당하는 것이다.

44) OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.

45) <[http://inicio.ifai.org.mx/Estudios/APECPrivacyFramework\(Oct-2004\).pdf](http://inicio.ifai.org.mx/Estudios/APECPrivacyFramework(Oct-2004).pdf)>

4. 유럽연합의 개인정보 보호

4.1 유럽인권협약

유럽에서의 개인정보 보호는 1950년 유럽위원회(Council of Europe)가 인권과 기본적 자유를 보장하기 위하여 채택한 유럽인권협약⁴⁶⁾으로 거슬러 올라간다. 이 협약은 “누구든지 자신과 가족의 생활, 가정, 서신을 존중할 권리를 가지고 있다”고 하여 프라이버시를 보호하고($\S 8$ I) 국가가 이에 간섭하는 것을 금지하고 있다($\S 8$ II).⁴⁷⁾ 이 규정에 의하여 개인정보의 보호는 유럽인권법원(1959년 설립)의 판단을 통하여 이루어지는데, 유럽인권법원은 협약을 위반한 것에 대하여 개인이나 단체 등이 제기하거나 국가 간에 제기된 소송을 심리하고 판단한다. 이에 의하여 유럽위원회의 체약국(2013년 현재 47개)이 협약을 준수하는 것이 감시될 뿐만 아니라 개인정보의 보호가 이루어지게 된다.

개인정보는 협약 제8조에 의하여 보호되는 범주에 속하는데, 유럽인권법원은 그동안 협약 제8조에 규정되어 있는 ‘개인의 생활(private life)’을 광범위하게 해석하여 국가가 피용자의 이메일과 전화통화를 감시하거나, 도청하거나, 동의를 받지 않고 개인정보를 수집하거나 개인정보에 접근하지 못하도록 할 수 있는 권리 등을 인정하였다.⁴⁸⁾

4.2 기본권 차원의 개인정보 보호

유럽에서의 개인정보 보호는 기본권(fundamental right)의 지위를 얻고 있다. 유럽에서 개인정보 보호를 규정한 조약은 유럽인권협약, EU 기본권헌장, EU 기능조약이다.⁴⁹⁾ 개인정보 보호에 대하여 기본권의 지위를 부여한 가장 기본적인 조약은 EU 기본권헌장

46) Convention for the Protection of Human Rights and Fundamental Freedoms (채택 1950, 발효 1953).

47) 곧 정부당국이 이러한 권리에 간섭하는 것을 금지시키고, 다만 국가안전보장 또는 공공의 안전이나 국가의 경제적 번영, 무질서나 범죄의 예방, 건강이나 윤리의 보호, 타인의 권리나 자유를 보호하기 위하여 민주사회에서 필요한 경우 법에 따라 간섭하는 것을 예외로 규정하고 있다($\S 8$ II).

48) Marc Rotenberg & David Jacobs, “Updating the Law of Information Privacy: The New Framework of the European Union”, *Harvard Journal of Law & Public Policy* Vol.36 Issue2, Harvard Law School, 2013, pp.612-613.

49) EU 기본권헌장(EUCFR, Charter of Fundamental Rights of the EU) 제8조는 누구든지 개인데이터를 보호받을 권리가 있다는 것과 특정목적에 위한 공정한 처리, 당사자의 동의나 적법한 근거에 의한 처리, 데이터에 대한 접근권 및 정정권 부여를 규정하고 있다. EU 기능조약(TFEU, Treaty on the Functioning of the EU) 제16조는 누구든지 개인데이터를 보호받을 권리가 있으며, 유럽의회와 위원회가 개인데이터 처리에 대하여 보호받기 위한 규칙을 규정할 것을 규정하고 있다.

인데, 유럽연합조약(Treaty on European Union)은 기본권헌장에 규정된 권리에 대하여 조약과 동일한 지위를 부여하고 있으며(§6.1), 1995년의 데이터지침과 2012년 제안된 개인정보 규칙은 그 목적으로서 개인데이터와 관련된 기본권 보호를 천명하고 있다(§1). 1995년의 데이터지침이 개인정보의 흐름과 관련된 경제적 중요성을 인식한 것에서 탄생되었다는 것을 부정할 수 없지만, 개인정보의 보호는 이제 기본권의 지위로 있는 것으로 인정되어 있다. 개인정보의 보호가 유럽에서 기본권의 지위에 있다는 것은 개인정보를 보호하는 것이 공동시장의 문제, 곧 경제적인 문제와 분리되고 인권 보호적 측면을 가진 프라이버시와도 분리될 정도로⁵⁰⁾ 독자적 지위를 획득하였다는 것을 의미한다.

4.3 유럽 국가들의 개인정보 보호

1960년대 중반 금융, 보안, 의료지원 등을 위하여 독일의 헤센주 정부 등이 데이터를 수집하기 시작하였는데, 거의 모든 헤센주 주민의 건강이나 수입과 같은 민감 데이터가 저장되고 수집목적과 다른 목적을 위하여 사용될 수 있음으로써 시민에 대한 영구적인 감시가 이루어질 위험이 있게 되었고, 이에 따라 독일의 헤센주는 1970년 세계에서 처음으로 데이터보호법을 제정하였다. 이후 유럽국가들간의 지리적으로 서로 근접해 있으며 문화·정치·통신·무역에 대한 공통된 관심사로 인하여 유럽국가에서 많은 개인정보 보호입법이 이루어졌다. 또한 정보기술의 등장과 감시사회에 대한 논의도 여러 국가에서 개인정보 보호입법을 촉발시키게 되었다. 이들 유럽 국가들의 개인정보 보호입법은 공정정보관행의 원칙을 포함하거나, 접근이나 정정 등 개인정보 주체에게 일정한 권리를 부여하거나, 개인정보 처리에 대한 통제 메커니즘을 마련하거나 데이터의 국경 간 이동 등에 대한 내용을 담고 있다.⁵¹⁾

스웨덴은 데이터보호법을 1973년 처음으로 제정하였다. 이후 독일(1976), 덴마크(1978), 노르웨이(1978), 프랑스(1978), 영국(1984), 핀란드(1988), 네덜란드(1988) 등의 국가들이 데이터보호법을 제정하였다. 1970년대 이후 1980년대까지 입법된 유럽 국가들이 데이터보호법을 조화시킬 필요성이 생겼고 이에 따라 나온 것이 1995년 데이터지침이다.

50) Tanzou, at 25-26.

51) Paul De Hert, Vagelis Papakonstantinou, op. cit., at 283.

4.4 자동처리 개인정보 보호협약

유럽인권협약은 유럽에서 프라이버시를 보호하는데 상당한 역할을 하였으나 기술발전과 기업환경의 변화로 인하여 유럽인권협약상의 프라이버시 개념이 도전을 받게 되었다. 유럽위원회는 이미 1960년대 말부터 개인정보에 대하여 작업을 해왔고 1970년대 중반까지 개인정보에 대한 결의안을 내놓고 있었다. 그러나 유럽위원회는 정보기술의 발전으로 인한 개인정보의 문제점을 해결하기 위하여 1981년 ‘자동 처리 개인정보 보호 협약’을 채택하였다.⁵²⁾ 곧 ‘협약 108(Convention 108)’이라고도 불리는 이 협약은 자동 처리되는 개인데이터가 국경간에 이동하는 것이 증가하는 것을 고려하여 모두의 권리와 기본적 자유의 보장을 확대하고, 개인이 국경과 관계없이 프라이버시에 대한 자유를 누릴 수 있도록 하며, 프라이버시에 대한 기본권적 가치와 정보의 자유로운 이동을 조화시키기 위한 것(협약 서문)이었다.

이 협약은 ‘개인정보(personal data)’를 식별되었거나 식별가능한 개인에 관한 모든 정보라고 정의하고, ‘자동 처리(automatic processing)’를 자동화된 수단에 의하여 전체 또는 일부분 수행되는 경우에 개인정보의 저장, 개인정보에 대한 논리적·수리적 연산 수행, 변경, 삭제, 검색 또는 배포를 포함한다고 정의하여(§2) 유럽인권협약과 마찬가지로 매우 광범위하게 규정하고 있다. 이 협약은 공정정보관행의 원칙을 포함시켰으며, 데이터의 질적 적정성과 관련하여 개인정보가 공정하고 적법하게 획득 및 처리되어야 하고, 명시되고 적법한 목적을 위하여 저장되어야 하며, 저장된 목적과 관련하여 적절, 관련성이 있고 과도하지 않아야 하며, 정확하고 최신의 것으로 유지되어야 하며, 저장된 목적을 위하여 필요한 기간을 초과하지 않는 동안 개인정보 주체를 확인할 수 있는 형태로 보존되도록 하고 있다(§5). 또한 인종, 정치적 견해, 신앙 등 기타 신념, 건강이나 성생활, 형사범죄 등 민감정보는 법이 적법한 안전장치를 마련하지 않는 한 자동적인 처리를 금지하고 있다(§6). 이 협약은 개인정보의 국경 간 이동에 관한 기준을 처음 마련함으로써(§12) 국내법에 의하여 개인정보를 보호하기 위한 입법이 확산되도록 하는 역할을 하였다.

자동 처리되는 개인정보를 보호하기 위한 이 협약은 유럽인권협약과 달리 정부와

52) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. 2001년 유럽위원회는 독립적인 데이터보호기관을 설립하고 비회원국에 대한 데이터 이동에 제한을 가하는 ‘추가 의정서’를 채택하였다. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Nov. 8, 2001, C.E.T.S. No. 181.

민간주체 모두에게 적용되었으나, 개인정보의 ‘자동화된’ 처리(automatic processing) ‘에 대해서만 적용되어 수동적으로 처리되는 데이터는 적용되지 않으며, 법이 충돌하는 경우에 어느 국가의 법이 적용되는가에 대하여 모호하고, 비회원국에 대한 개인정보의 이동제한은 국제무역을 방해할 수 있고, 집행을 위한 메커니즘이 존재하지 않는 문제점을 안고 있었으며,⁵³⁾ 무엇보다도 국가간에 많은 차이점이 발생하도록 하였다.⁵⁴⁾ 따라서 개인정보 보호에 관하여 국가 간에 차이가 나거나 충돌되는 법을 일치하도록 하기 위한 일반적인 규범을 필요로 하게 되었다.

4.5 데이터지침

1993년 유럽연합(European Union)이 출범된 이후 유럽에서는 프라이버시 보호에 관한 입법이 쏟아져 나오게 되었다. 그 중에서 가장 중요한 것은 1995년의 ‘데이터지침’⁵⁵⁾으로서, 데이터지침은 개인정보를 보호하는 것에 관한 유럽연합 차원의 첫 입법이다. OECD 가이드라인과 마찬가지로 데이터지침도 개인정보와 관련된 경제적 측면에서 탄생한 것이라 할 수 있는데, 이것은 데이터지침의 목적에서도 나타나고 있다. 데이터지침은 회원국으로 하여금 첫째, 자연인의 기본권 및 자유를 보호하고 특히 개인데이터의 처리에 관한 프라이버시권을 보호하고, 둘째, 이러한 보호와 관련된 근거에 의하여 회원국 간에 개인데이터의 자유로운 흐름이 제한되거나 방해하지 않도록 하는 것을 목적으로 하고 있다(§1). 유럽공동시장이 형성되고 작동하기 위해서는 회원국 간에 개인 데이터가 자유로이 이동할 수 있어야 할 뿐만 아니라 개인이 기본권이 보장되어야 한다(Recital 3).

데이터지침은 개인정보가 유럽연합의 국가간에 이동하는 것을 규율하고 개인정보의 저장, 송신 및 처리의 보안에 대한 기준을 설정한 법규범이다. 데이터지침은 개인정보의 자동적인 처리뿐만 아니라 수동적인 처리에도 적용된다(§3.1). 또한 적법한 개인정보 처리조건을 회원국이 보다 더 정확하게 규정하도록 재량을 부여하기 위한 것으로서(§5), 데이터지침은 개인에게 직접 적용되지 않고 회원국이 지침에 바탕을 두어 국내법으로 입법함으로써 개인에게 적용된다. 데이터지침은 첫째, 자연인의 기본권과 자유, 특히 개인정보 처리에 관한 프라이버시권을 보호하고, 둘째, 이러한 보호를 이유로 회원국

53) Wade, at 669-670.

54) Marc Rotenberg & David Jacobs, op. cit., at 616.

55) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31.

간에 개인정보가 자유로이 이동하는 것을 제한하거나 금지하지 않도록 하기 위한 것이다 (§1). 이를 위하여 데이터지침은 개인정보의 질적 적정성의 원칙(§6), 개인정보의 적법한 처리기준(§7), 민감한 정보의 원칙적 처리 금지(§8), 개인정보에 대한 개인정보주체의 접근권(§12), 개인정보 주체의 반대할 권리(§14), 개인정보의 처리의 비밀(§16), 개인정보에 대한 안전성 보장(§17) 등을 규정하고 있다.

데이터지침상의 개인정보에 대한 권리는 절대적이지 않으며 제한되거나 예외가 허용된다. 곧 데이터의 질적 적정성 원칙(§6.1) 등에 대하여 ① 국가안전보장, ② 방위, ③ 공공의 안전, ④ 범죄의 예방 등, ⑤ 중요 경제 또는 금융이익, ⑥ 위 ③, ④, ⑤의 공공의 권한행사와 행사와 관련된 감시, 조사 또는 규제기능, ⑦ 개인정보 주체나 타인의 권리와 자유의 보호를 보장하기 위하여 필요한 조치로서 제한될 수 있다(§13.1). 또한 접근권(§12)도 과학연구나 통계작성을 위하여 제한될 수 있다(§13.2).

1995년 채택되고 발효된 데이터지침은 회원국들이 1998년까지 이를 이행토록 하였다 (§32.1). 데이터지침은 유럽연합 내부와 외부에 대한 영향에 의하여 평가될 수 있다. 우선 유럽연합 내에서는 높은 수준의 개인정보를 보호하도록 하면서 전역에서 개인정보가 자유로이 이동할 수 있는 환경을 마련한 것으로 평가된다.⁵⁶⁾

V. 맺으며

앞서 살펴본 바와 같이, 미국에서의 사생활 공개에 관한 프라이버시의 보호, 곧 개인정보 보호는 다음과 같은 특징을 지닌다. “연방과 주의 여러 개별적인 법들이 서로 합쳐진 형태(patchwork)로 일정한 개인정보의 프라이버시를 보호한다. 공공 및 민간주체가 보유하는 개인정보를 보호하는 연방차원의 일반법은 존재하지 아니 한다. 민간주체가 개인정보를 수집하고 공개하는 것에 대하여 의회는 전반적으로 대처한 것이 아니라 개별적인 분야에 따라 대처해 왔다. 연방 법규범이 개인정보를 보호하는 분야는 소비자 신용도 제공, 전기통신, 연방정부 기관의 기록, 교육기록, 은행기록, 케이블가입자 정보, 비디오 대여 기록, 자동차 기록, 보건정보, 정보통신 가입자 정보, 온라인상의 어린이 정보, 고객의 금융정보 등⁵⁷⁾ 이다.”⁵⁸⁾ 개인정보를 보호하는 미국의 법제는 원칙적으로 개인정보를

56) Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC), at 3, COM (2003) 265 final, May 15, 2003.

보호하는 것이 아니라 특별히 규율하는 분야의 개인정보만을 예외적으로 보호한다는 것을 의미한다. 따라서 대부분의 개인정보는 이러한 개별적인 분야에 포함되지 않으므로 대부분의 개인정보가 법률에 의하여 보호받지 않는다.⁵⁹⁾

개인정보를 보호하는 미국의 법제는 개별적인 분야마다 상업적인 이익과 프라이버시에 대한 이익과의 조화와 균형을 중시한다. 이에 반하여 유럽연합은 소비자와 프라이버시에 보다 더 치중하는 접근방법과 일반법에 의하여 규율하고 있다고 할 수 있다. 즉 유럽은 프라이버시를 기본권으로 파악하고 있다. 달리 말하면, 기본권이라고 하여 다른 권리에 우월하다는 것은 아니지만 경제적인 권리가 프라이버시보다 우월하지는 않은 것으로 파악하고 있다.⁶⁰⁾

또한 미국과 유럽의 프라이버시와 개인정보보호는 다음과 같이 요약될 수 있다. 첫째, 개인정보 보호를 위한 일반법이 존재하지 않으며, 의료, 금융, 신용평가 등 개인정보가 사용되는 특정 산업이나 특정 분야에서 초점을 맞춘 법률에 의하여 개별적으로 협소하게 규율되고 있을 뿐이다. 이에 반하여, 유럽연합은 공공 및 민간을 모두 규율하는 일반법에 의하여 광범위하게 규율한다. 또한 EU는 프라이버시를 기본권으로 바라보고 있으나 미국은 표현의 자유와 같은 다른 이익과 균형되어야 하는 것으로 바라보고 있다. 또한 유럽연합의 개인정보법제는 법적 근거가 없는 경우에는 개인정보의 처리를 금지하지만, 미국의 개인정보법제는 피해를 야기하거나 법에 의하여 제한되지 않는 한 일반적으로 개인정보를 처리하도록 허용하고 있다. 둘째, 개인정보는 연방대법원에 의하여 사생활 공개에 관한 프라이버시만큼 보호받지 않고 있으며, 개인정보의 보호는 연방 및 주 법률, 코몬로상의 불법행위, 대리관계에 관한 규범, 자율규제의 원리 등에 근거하고 있다.

유럽연합은 개인정보 보호분야의 법을 형성시키는데 있어서 국제적으로 주요한 역할

57) Fair Credit Reporting Act of 1970 (FCRA) (42 U.S.C. §1681); Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. §§2510-2522, 2701-2711, 3121-3126); Privacy Act of 1974 (5 U.S.C. §552a); Family Educational Rights and Privacy Act of 1974 (FERPA) (45 U.S.C. §1232g); Right to Financial Privacy Act of 1978 (12 U.S.C. §3401); Cable Communications Policy Act of 1984 (47 U.S.C. §551); Video Privacy Protection Act of 1988 (18 U.S.C. §2710); Driver's Privacy Protection Act of 1994 (18 U.S.C. §2721); Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §1320d); Communications Act of 1934 (47 U.S.C. §222); Gramm-Leach-Bliley Act of 1999 (GLBA) (15 U.S.C. §§6801 - 6809).

58) Gina Stevens, "Privacy Protections for Personal Information Online 7", *Congressional Research Service R41756*, 2011.

59) Devin W. Ness, "Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It", *CARDOZO ARTS & ENT Vol.31*, 2013, at 925, 944.

60) Ness, at 945.

을 해 왔다. 이것을 가능하게 한 주된 요인은 EU법이 회원국으로 하여금 개인정보를 해외에 이전하는 것을 봉쇄할 수 있도록 하였기 때문이다.⁶¹⁾ 미국과 달리 유럽은 개인정보를 일반법의 형식으로 규율하고 있으며 데이터보호, 곧 개인정보 보호라는 명칭으로 강력하게 규제하고 있다.⁶²⁾

과거와 비교하여 개인이 감당할 수 없을 정도로 거대하게 축적된 정보는 더 다양한 용도로 그리고 더 편리하게 사용될 수도 또는 정보주체가 미리 예측하지 못한 용도로 개인에게 상당히 불리하게 사용될 여지도 있다.⁶³⁾ 따라서 빅 데이터와 프라이버시 간 충돌은 이러한 모든 장단점을 고려하면서 해법이 제시되어야 할 것이다. 시장이 요구하는 빅 데이터의 적극적 활용과 타인의 부당한 간섭을 거부하고 개인의 평온과 사생활이 보호되는 프라이버시가 언제나 서로 상충되는 위치에 놓여 있는 것은 아니다. 프라이버시 보호에 대한 신뢰를 바탕으로 시장은 보다 자유롭게 새로운 빅 데이터 기술을 소비자를 위하여 개발하고 활용할 수도 있기 때문이다.⁶⁴⁾ 이미 IT분야에서 국제적인 우위를 점하고 있으며, 빅 데이터 시대를 맞이하고 있는 우리나라에서도 미국과 유럽의 개인정보 보호정책을 면밀히 검토하여 적극적으로 법제를 마련할 필요성이 있겠다.

61) Schwartz, at 5.

62) Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (EC); Council Directive 2002/58, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) (EC).

63) Robert Gellman, "Fair Information Practices: A Basic History", April 25, 2012, <<http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>>.

64) The Privacy Protection Study Commission, "Personal Privacy in an Information Society", July, 1977, <<http://aspe.hhs.gov/datacncl/1977privacy/toc.htm>>.

참고문헌

1. 단행본

- Alan F. Westin, *Privacy and Freedom*, Consortium Book Sales & Dist, 1967.
- Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTC's New Approach to Privacy*, The Atlantic, 2012.
- Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law, Fourth Edition*, Aspen Pub, 2011.
- Fred H. Cate et al., *Data Protection Principles for the 21st Century -Revising the 1980 OECD Guidelines*, Microsoft Corporaton, 2013.
- Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.
- Justin Brookman, *Corporate Accountability Is Important, But Consumers Still Need Meaningful Control*, iapp Privacy Perspectives, 2014.
- Terence Craig & Mary E. Ludloff, *Privacy and Big Data*, O'Reilly Media, 2011.

2. 학술지

- 이대희, “빅데이터와 개인정보 보호”, 정보법학, 정보법학회, 2015, 127-158쪽.
- 정혜련/김은경, “빅데이터와 보호에 대한 현안”, 해외방송통신분쟁 ISSUE REPORT 제36호, 방송통신위원회, 2013, 28-60쪽.
- A. Michael Froomkin, “The Death of Privacy?”, *Stanford Law Review Vol.52 No.5*, Stanford University School of Law, pp.1461-1543.
- Benjamin Shmueli & Ayelet Blecher-Prigat, “Privacy for Children”, *Columbia Human Rights Law Review Vol.42*, Columbia University, School of Law, 2011, pp.759-795.
- Bartosz M. Marcinkowski, “Privacy Paradox(ES): In Search of a Transatlantic Data Protection Standard”, *Ohio State Law Journal, Vol.74 No.6*, Ohio State University, College of Law, 2013, pp.1167-1194.
- Chris Jay Hoofnagle & Jennifer M. Urban, “Alan Westin's Privacy Homo Economicus”, *Wake*

- Forest Law Review Vol.49*, Wake Forest University School of Law, 2014, pp.261-317.
- Danah Boyd & Kate Crawford, “CRITICAL QUESTIONS FOR BIG DATA -Provocations for a cultural, technological, and scholarly phenomenon”, *Information, Communication&Society Vol.15, Issue5*, Routledge, 2012, pp.662-679.
- Daniel J. Solove, “Conceptualizing Privacy”, *CALIFORNIA LAW REVIEW Vol.90 No.4*, School of Law, University of California, Berkeley, 2002, pp.1087-1155.
- _____, “Introduction: Privacy Self-Management and the Consent Dilemma”, *Harvard Law Review: Vol.126 No.7*, Harvard Law Review, 2013, pp.1880-1903.
- David Navetta, “Legal Implication of Big Data: A Primer”, *Information Systems Security Association Journal No.14*, ISSA, 2013, pp.14-19.
- Dennis D. Hirsch, “Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law”, *Georgia Law Review Vol.47 Issue1*, University of Georgia, 2006, pp.1-64.
- Elise Young, “Educational Privacy in the Online Classroom: FERRA, MOOCs, and the Big Data Conundrum”, *Harvard Journal of Law & Technology Vol.28 No.2*, Harvard Law School, 2015, pp. 549-592.
- Fred H. Cate & Viktor Mayer-Schoeberger, “Notice and consent in a world of Big Data”, *International Data Privacy Law Vol.3 Issue2*, Oxford Journals, 2013, pp.67-73.
- Ira S. Rubinstein, “Big Data: The End of Privacy or a New Beginning?”, *International Data Privacy Law Vol.3 No.2*, Oxford Journals, 2013. pp.74-87
- _____, “Voter Privacy in the Age of Big, Data”, *Wisconsin Law Review*, University of Wisconsin Law School, 2014, pp.861-936.
- Ira S. Rubinstein & Nathaniel Good, “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents”, *Berkeley Technology Law Journal Vol.28 Issue2*, University of California, Berkeley School of Law, 2013. pp.1332-1414.
- Jed Rubinfeld, “The Right of Privacy”, *HARVARD LAW REVIEW Vol.102 No.4*, Harvard Law Review Association, 1989, pp.737-807.
- Jennifer Moore, “Traumatised Bodies: Towards Corporeality in New Zealand’s Privacy Tort Law Involving Accident Survivors”, *New Zealand Universities Law Review Vol.24 No.3*, 2011. pp.386-420.

- Jeremy Ginsberg, Matthew H. Mohebbi, Rajan S. Patel, Lynnette Brammer, Mark S. Smolinski & Larry Brilliant, “Detecting influenza epidemics using search engine query data”, *Nature Vol.457*, Nature Publishing Group, 2009, pp.1012-1015.
- Jerry Kang, “Information Privacy in Cyberspace Transactions”, *Stanford Law Review Vol.50 No.4*, Stanford University School of Law, 1998, pp.1193-1294.
- Joseph Jerome, “Big Data: Catalyst for A Privacy Conversation”, *Indiana Law Review Vol.48*, Elsevier, 2014, pp.213-242.
- Jules Polonetsky & Omer Tene, “Privacy and Big Data: Making Ends Meet”, *Stanford Law Review Online Vol.66*, Stanford Law School, 2013, pp.25-33.
- Kate Crawford & Jason Schultz, “Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms”, *Boston College Law Review Vol.55 Issue1*, Boston College Law School, 2013, pp.93-128.
- Michael D. Birnhack & Niva Elkin-Koren, “Does Law Matter Online? Empirical Evidence on Privacy Law Compliance”, *Michigan Telecommunications and Technology Law Review Vol.17 Issue2*, University of Michigan Law School, 2011, pp.337-384.
- Michael D. Birnhack, “A Quest for a Theory of Privacy: Context and Control”, *Jurimetrics Vol.51, No.4*, American Bar Association, 2011, pp.447-479.
- _____, “Reverse Engineering Information Privacy Law”, *Yale Journal of Law and Technology Vol.15 Issue1*, Yale Law School, 2012, pp.24-68.
- Neil M. Richards, “The Information Privacy Law Project”, *Georgetown Law Journal Vol.94*, Georgetown University Law Center, 2006, pp.1087-1140.
- Nicolas P. Terry, “Protecting Patient Privacy in the Age of Big Data”, *UMKC Law Review Vol.81 Issue2*, University of Missouri-Kansas City School of Law, 2012, pp.385-416.
- Omer Tene & Jules Polonetsky, “Big Data for All: Privacy and User Control in the Age of Analytics”, *Northwestern Journal of Technology and Intellectual Property Vol.11 Issue5*, Northwestern University School of Law, 2013, pp.240-274.
- Paul M. Schwartz, “Property, Privacy, and Personal Data”, *Harvard Law Review Vol.117 Issue7*, The Harvard Law Review Association, 2004. pp.2056-2128.
- Peter Leonard, “Consumer Data Analytics: Privacy Settings for ‘Big Data‘ Business”, *International Data Privacy Law Vol.4 Issue1*, Oxford Journals, 2014, pp.53-68.

Robert. N. Mayer, “The US Consumer Movement: A New Era Amid Old Challenges”, *Journal of Consumer Affairs Vol.46 Issue2*, Wiley-blackwell, 2012, pp.171-189.

3. 기타자료

한국정보화진흥원, “Big Data 글로벌 10대 선진 사례”, 2012.

Article 29 Data Protection Working Party and the Working Party on Police and Justice, “The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data”, 02356/09/EN, WP 168, Dec 1, 2009.

Charles Duhigg, “How Companies Learn Your Secrets”, The New York Times Magazine, Feb 16, 2012.

Commissioner Julie Brill, “Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions”, Address at the Woodrow Wilson School of Public and International Affairs, Princeton University, February 20, 2014.

Executive Office of the President, President’s Council of Advisors on Science and Technology, “Big Data and Privacy: A Technological Perspective iv”, May 2014.

FTC, “Privacy Online: A Report to Congress”, 1998.

FTC, Protecting Consumer Privacy in an Era of Rapid Change, “A Proposed Framework for Business and Policymakers”, Preliminary FTC Staff Report iv, Dec 2010.

International Working Group on Data Protection in Telecommunications (IWG), “Working Paper on Big Data and Privacy: Privacy principles under pressure in the age of Big Data analytics”, 2014.

McKinsey Global Institute, “Big data: The next frontier for innovation, competition, and productivity”, McKinsey & Company, 2011.

U.S. Department of Health, Education & Welfare, “Secretary's Advisory Committee on Automated Personal Data System, Foreword to Records, Computers and the Rights of Citizens”, 1973.

White House, “Big Data: Seizing Opportunities, Preserving Values”, May. 2014.

White House, “Consumer Data Privacy in a Networked World: A Framework for Protecting

Privacy and Promoting Innovation in the Global Digital Economy”, 2012.
World Economic Forum, “Unlocking the Economic Value of Personal Data: Balancing Growth and Protection”, 2012.

4. 웹 자료

Adam Singer, “49 Amazing Social Media, Web 2.0, and Internet Stats”, The Future Buzz, January 12, 2009, <from <http://thefuturebuzz.com/2009/01/12/social-media-web-2.0-interest-numbers-stats/>>.

Andrew B. Serwin, “Understanding Proposed Models for Privacy”, Privacy & Security Source, January 15, 2011, <from <http://www.privacysecuritysource.com/understanding-proposed-models-for-privacy/>>.

BBC, “Google ‘in breach’ of UK data privacy agreement”, July 27, 2012, <from <http://www.bbc.co.uk/news/technology-19014206>>.

Berkman Center for Internet and Society, Harvard University “A History of Digital Data Creation”, <http://cyber.law.harvard.edu/digitaldiscovery/timeline_files/frame.htm>.

Bill Schmarzo, “Big Data in Traditional Retail – Part I”, InFocus, August 6, 2012, <http://infocus.emc.com/william_schmarzo/big-data-in-traditional-retail-part-i/>.

Bruce Schneier, “Why ‘Anonymous’ Data Sometimes Isn’t”, WIRED, December 13, 2007. from http://www.wired.com/politics/security/commentary/securitymatters/2007/12/security_matters_1213.

Cameron Chapman, “The History of the Internet in a Nutshell”, Six Revisions, November 15, 2009, <<http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/>>.

David Goldman, “Obama’s big idea: Digital health records”, CNN Money, January 12, 2009, <<http://cs.gmu.edu/~mlocasto/research/securehealth/content/CNN-digital-health-records.pdf>>.

Business Wire, “Digital Advertising Alliance (DAAD) Comments on Microsoft Decision to Embed Do Not Track in IE 10 Set ‘on’ by Default”, May 31, 2012, <<http://www.businesswire.com/news/home/20120531006914/en/Digital-Advertising-Alliance-DAA-Comments-Microsoft-Decision>>.

- FCC, “What We Do”, <<http://www.fcc.gov/what-we-do>>.
- FTC, “FTC Staff Issues Privacy report, Offers Framework for Consumers, Businesses, and Policymakers”, December 1, 2010, <<http://www.ftc.gov/opa/2010/12/privacyreport.shtm>>
- FTC, “Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Business and Policymakers”, December. 2010, <<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>>.
- Irfan Khan, “Big data startups lure investment dollars”, IT world, August 16, 2012, <<http://www.itworld.com/it-managementstrategy/289534/big-data-startups-lure-investment-dollars>>.
- Jenn Webb, “The Truth about data: Once it’s out there, it’s hard to control”, O’Reilly Strata Making Data Work, April 4, 2011, <<http://strata.oreilly.com/2011/04/jeff-jonas-data-privacy-control.html>>.
- John J. Heitmann, “FCC Announces June 28, 2011. Location Based Services (LBS) Forum”, AD Law Access, May 25, 2011, <<http://www.adlawaccess.com/2011/05/articles/privacy-and-information-security/fcc-announces-june-28-2011-location-based-service-lbs-forum/>>.
- Nate Anderson, “Study: Reading online privacy policies could cost \$365 billion a year”, arstechnica, October 9, 2008, <<http://arstechnica.com/tech-policy/news/2008/10/study-reading-online-privacy-policies-could-cost-365-billion-a-year/>>.
- Nathan Wolfe & Lucky Gunasekara & Zachary Bogue, “Crunching Digital Data Can Help the World”, CNN, February 2, 2011, <<http://www.cnn.com/2011/OPINION/02/02/wolfe.gunasekara.bogue.data/>>.
- Office of Science and Technology Policy, “Obama Administration Unveils ‘Big Data’ Initiative: Announces \$200 Million in New R&D Investments”, March 29, 2012, <http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf>.
- Opera Software Press Release, “Who’s Watching You”, January 28, 2011, <<http://www.opera.com/press/release/2011/01/28/>>.
- Quentin Hardy, “Rethinking Privacy in an Era of Big Data”, NY Times, June 4, 2012, <<http://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data/>>.

Robert Gellmann, “Fair Information Practices: A Basic History”, April 25, 2012,
<<http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>>.

The Privacy Protection Study Commission, “Personal Privacy in an Information Society”,
July 1977, <<http://aspe.hhs.gov/datacncl/1977privacy/toc.htm>>.

The Secretary’s Advisory Committee on Automated Personal Data Systems, “Records,
Computers and the Rights of Citizens”, July, 1973,
<<http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>>.

The White House, “Big Data is a big deal”, March 29, 2019,
<<http://www.whitehouse.gov/blog/2012/03/29/big-data-big-deal>>.

The White House, “We Can’t Wait: Obama Administration Unveils Blueprint for a ‘Privacy
Bill of Rights’ to Protect Consumers Online”, February 23, 2012,
<<http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>>.

U.S. Department of Health & Human Services, “HHS Imposes a \$4.3 Million Civil Money
Penalty for HIPAA Privacy Rule Violations”,
<<http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html>>.

U.S. Department of Health & Human Services, “Understanding Health Information Privacy”,
<<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>>.

United States Department of Commerce, “Internet Policy Task Force Privacy Green Paper”,
<<http://www.commerce.gov/node/12471>>.

[Abstract]

A Study on a Unique and Distinctive Culture (Law and Understanding) Regarding the Protections for Privacy in the U.S.

Jung, Hye-Ryun*

The U.S. Administrative bodies including Federal Trade Commission have been striking a balance between the socially beneficial uses of big data and the harms to privacy than can result from the analysis of the big data. The Korean government and other countries' ones have been concentrated their efforts in order to achieve the balance between them. But there's some distinctions about the concept and the notion of 'Privacy' among the countries. Particularly, the meanings of the 'Privacy' in the U.S. have long history and they are various compared to other countries such as Europe and Korea.

Thus, this article deals with the concepts and definitions of the 'Privacy' in the United States. In order to provide the understanding of this, it first illustrates the Constitutional context under the U.S. laws and it also analyzes the courts decisions of the U.S.. Then it introduces the frameworks and regulating bodies to protect privacy. Specifically, it provides a fundamental principle and the laws to protect privacy in the U.S. and Europe. By recognizing these, it finally suggests the characteristics and the differences between the U.S. and the European countries regarding the privacy laws and policies.

[Key Words] privacy, big data, FTC, decisional privacy, informational privacy, fundamental principle, law and policies

* Adjunct Professor, College of Law, Hongik University