成均館大學校 比較法硏究所
成均館法學 第17卷 第3號 2005年 12月
SungKyunKwan Law Review
The Institute for Comparative Legal Studies
Vol. 17 No. 3 December. 2005

미국의 프라이버시 법제에 관한 연구

조 규 범*

Ⅰ. 서설

미국은 19세기 말부터 판결과 학자들에 의하여 프라이버시의 개념이 발전되기 시작하였으며, 1965년 Griswold v. Connecticut 사건[1] 이전까지 프라이버시 침해를 보통법상의 불법행위로 보아 손해배상의 책임을 인정해 온 법적인 전통을 가지고 있다. 이 사건 이후부터 프라이버시를 헌법적인 권리로 인정하면서 법적인 논의를 거듭하고 있지만, 대륙법계 국가인 프랑스, 독일 등 다른 유럽국가들과는 달리 포괄적이고 체계적인 개인정보 관련 법체계를 가지고 있지는 않다. 그러나 이처럼 기본법이 부재한 상황에서도 사회적 변화나 기술발달에 맞춰 공공·통신·온라인 등 각 영역별로 개인정보와 관련한 개별법적인 접근을 취하여 대응하고 있다.

특히 미국은 개인정보보호를 위한 접근방식에서 경제적·기술적 관점을 중시하는 경향이 있다. 이는 민간부문에 두드러지게 나타나는 현상으로써, 사적 자치의 원칙을

* 대한민국국회 입법정보연구관, 법학박사.

1) Griswold v. Connecticut, 381 U.S. 479, 484 (1965)에서는 권리장전(Bill of Rights)의 경계영역(penumbra)에서 프라이버시권을 구한다.

중시하여 정부의 간섭을 최소화한 자유로운 시장경제의 질서를 유지하기 위한 목적에서 비롯된 것이다.

프라이버시 보호를 위한 규제방식은 법집행기관에 의한 방식과 산업계에 의한 자율규제(self-regulation) 방식으로 구분할 수 있다. 자율규제란 정부의 전통적인 세 가지 요소인 입법, 집행, 평가에 기반을 두고 있지만, 이들 기능들은 정부에 의한 것이라기 보다는 민간부문에 의하여 수행되는 규제방식이다.[2] 미국은 민간부문에서 특별히 규제할 필요성이 인정되는 경우에만 법률을 제정할 뿐, 원칙적으로 업계가 자율적으로 개인정보보호를 위한 제도를 마련하도록 유도하는 것은 정부의 몫으로 남겨두고 있다. 이러한 자율규제적 접근방식은 개인정보를 인권으로 보아 국가가 적극 관여하여 보호하여야 한다고 보는 유럽의 입장과는 다른 태도이다. 자율규제방식은 소비자 선호에 따라 업체의 행동이 결정되는 시장접근법과도 차이가 있다. 순수한 시장접근법에서는 소비자들이 강력한 프라이버시 보호를 실현하고 있는 회사와 거래하기를 원할 것이라 가정하기 때문이다.

최근 정보화시대에 부수한 기술의 발전에 따라 CCTV 감시, 개인정보 프로파일링, 아이디 도용, 온라인 프라이버시, RFID 프라이버시, 유전자복제 등 생명공학과 관련한 프라이버시,[3] 생체정보와 관련한 프라이버시 문제[4] 등과 같은 새로운 이슈들이 제기되고 있다. 이에 미국의 관련 이슈에 대한 개별법적인 접근과 영역별 개인정보 관련 법률현황 및 주요 판례에 대한 연구는 최근 유사사례에 대처하여야 하는 한국에게도 중요한 의미를 부여할 것이라 판단된다.

이 연구에서는 사회적 변화나 기술의 발전에 따라 각 부문별로 여러 가지의 프라이버시 보호 관련 법률을 마련하고 있는 미국의 입법론적 대응을 개괄적으로 고찰하고자 한다. 이를 위하여 제2장에서는 미국 프라이버시 법제의 특성을 살펴보기 위하여 그 개념 및 도출배경 등을 고찰한다. 제3장에서는 프라이버시 관련 미국헌법의 보

---

2) Albert J. Marcella, Jr. and Carol Stucki, Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues, John Wiley & Sons, Inc., 2003, p. 19.

3) 생명공학과 관련한 기본권적 문제를 헌법적으로 분석한 논문으로는 김형성, "생명공학의 헌법적 가능성과 한계", 공법연구 제32집 제1호, 2003 참조; 이 논문에서는 생명공학과 관련하여 가장 먼저 직면하게 되는 기본권적 가치는 인간의 존엄이며, 유전자의 조작이나 재조합이 정보의 자기결정권이나 프라이버시를 침해할 수 있음을 경고하고 있다. 같은 논문 273-274면 참조.

4) 생체인식기술의 발전에 따른 프라이버시 보호에 관한 고찰로는 김일환, "정보사회에서 생체정보의 보호에 관한 헌법적 고찰", 인권과 정의 통권 제344호, 2005 참조; 이 논문에서는 생체인식기술의 발전에 따른 개인정보침해문제들을 헌법이론적으로 분석하면서, 이를 기술적, 제도적, 법규범적 차원에서 검토하여 입법화하는 작업이 시급히 필요함을 주장한다.

호 및 연방법제의 입법현황과 함께, 제정법이나 판례법 외에도 개인정보보호를 위한 중요한 역할을 하는 '세이프 하버 원칙'(Safe Harbor Principles)을 살펴보기로 한다. 또한 제4장에서는 각 부문별로 개별적으로 접근하고 있는 개인정보보호 관련 연방법제의 구체적인 입법의 현황 및 내용들을 조사·분석한다. 마지막으로 제5장 결론에서는 미국 프라이버시 법제의 시사점을 살펴본 후 우리나라 개인정보보호법제의 정비방향을 제시하기로 한다.

II. 미국의 프라이버시 법제의 특성

1. 미국에서의 프라이버시의 개념

처음 미국에서 프라이버시권이 등장했을 때, 이는 혼자 있을 권리라는 소극적 권리로서 불법행위 법리로 해석하였다. 그러나 정보기술의 발달로 종래의 소극적 프라이버시권 개념에 대한 재검토가 논의되게 되었고, 적극적 의미로서 프라이버시권 개념이 등장하였다.[5] 이는 개인이 사회에서 살아가기 위해서는 사회에 의한 간섭을 받지 않는 비밀의 영역이 불가결한 것이고 그러한 의미에서 개인에게는 자기에 관한 개인정보를 자기가 통제할 수 있는 권리가 인정되어야 한다는 것이다. 따라서 이에는 남에게 알리고 싶지 않은 일정한 사적인 개인정보에 대하여 개인정보의 수집, 개인정보의 이용·제공, 개인정보의 유지·관리의 각각의 수준에서 정보주체에 의한 통제의 권리가 보장되어야 함과 동시에 그 권리들의 실효성을 확보하기 위해 개인정보의 열람청구권, 정정청구권 등을 인정하여야 함을 의미한다.[6]

미국의 프라이버시는 복합적인 개념으로서 한마디로 정의하기가 어렵다.[7] Warren과 Brandise는 프라이버시권을 '홀로 있을 권리'(the right to be let alone)로 이해하고, 민주주의체제에서 가장 중요한 자유로서 헌법에 반영되어야 한다고 주장하였다.[8]

---

5) 졸고, "미국에서의 인터넷 프라이버시 보호와 프라이버시 에스크로 시스템에 관한 연구", 헌법학연구 제8집 제4호, 2002, 361-368면 참조.

6) 황인호, "개인정보보호제도에서의 규제에 관한 연구", 공법연구 제30권 제4호, 229-233면 참조.

7) 프라이버시의 이슈에 관하여는 수많은 관점이 있다. Edward Bloustein은 프라이버시를 "신성한 인격, 인간의 자주성, 존엄, 그리고 고결성을 보호하는 인간개성의 한 이해관계"로 묘사한다. Edward J. Bloustein, "*Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*", 39 N.Y.U. L. Rev. 962, 971 (1964).

8) Saumel Warren and Luise Brandeis, "*The Right to Privacy*", 4 Harvard L. R., 193-220 (1890).

Allen Westin은 어떠한 환경이든 프라이버시를 개인의 신체나 태도 및 행위를 타인에게 얼마나 노출 할 것인지 자신이 자유롭게 선택할 수 있는 자유로 파악하였다.[9] Edward Bloustine은 프라이버시를 인격권으로서 인격의 침해, 개인의 자주성, 존엄과 완전성을 보호하는 것이라고 한다.[10] Ruth Gavison은 프라이버시가 '삶의 조건 또는 상태'를 의미하는 것으로 이해하고 있고, 프라이버시의 3요소로서 비밀(secrecy), 익명성(anonymity), 고립성(solitude)을 가지며, 그것이 자신의 의사나 또는 타인의 행위에 의해서 상실될 수 있는 상태라고 한다.[11] 영국의 Calcutt Committee는 프라이버시 정의를 만족할만한 법률은 찾아보기 어렵기 때문에 "개인의 일과 사생활 또는 그 가족의 그것을 직접 유형적인 수단이나 공개에 의해서 침해되는 것을 억제하는 권리"로 선언하였다. 또한 호주의 프라이버시 헌장의 서문에는 "자유민주사회는 개인의 자주성을 존중하고, 그러한 자주성을 침해하는 국가나 민간단체의 권한을 제한한다. 프라이버시는 인간존엄의 본질인 동시에 결사와 표현의 자유의 핵심이다. 이는 기본적 인권이고 또 모든 인간의 합리적인 기대"라고 선언하고 있다.[12]

프라이버시는 사회적·문화적 개념이며 상황적 개념으로서 다양한 사람들 사이에 다양한 의미로 사용되기 때문에 통일적 개념을 파악하는 것은 매우 곤란하나, Ruth Givison 등과 같이[13] 프라이버시를 삶의 조건이라고 파악할 때에 그것은 타인의 접근을 방해한다는 함축적 의미를 가지므로 안전관념을 중심으로 하여 개인의 정신적 안정에 관한 것을 보호하는 것이고, 이는 프라이버시권을 '마음의 비밀권'이라고 번역하는 것에서도 알 수 있다. 이는 프라이버시가 사회에서 본질적인 것이며, 프라이버시의 관념이 사회에서 발전된 개인의 도덕적 또는 직관적 관념이라는 것에 연유한다. 즉 이러한 도덕적·직관적 프라이버시 관념이 법률로써 프라이버시를 인식하고 보호하려는 정치적·사회적 압력의 근원이며, 법적 프라이버시권을 인정하고 정립하려는 정당성의 자연법적 근거가 되는 것이다.[14] 이는 프라이버시권이 미국에서 처음에 사인

---

9) Alan F. Westin, Privacy and Freedom, Atheneum, New York, 1967, p. 7.

10) Edward Bloustine, "*Privacy as an Aspect of Human Dignity*", 39 New York Univ. L. R., 971 (1964).

11) Ruth Gavison, "*Privacy and the Limits of Law*", 89 Yale L. J. 425-440 (1980).

12) 위의 Edward Bloustine, Ruth Gavison, 영국의 Calcutt Committee와 호주의 프라이버시 헌장 등은 대부분 인격권의 일부로서 프라이버시를 보고 있다.

13) Anita L. Allen, Uneasy Access: Privacy for women in a Free Society, pp. 13-15 (1988).; Richard C. Turkington, "*Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*", 10 N. Ill. Univ. L. R. 479, 509-510 (1990).

간의 불법행위법상의 문제로 인식되어 오다가 헌법상의 기본권으로 성장하여 왔다는 연혁에 의해서도 알 수 있듯이 프라이버시권이 국가에 의해 정책적으로 인정된 것이 아니고 인간으로서의 존재에 근거하는 기본적인 것으로 인정되어 온 것이다. 그러므로 프라이버시는 사람과 사람이 생활하면서 당연히 발생하는 것이다. 따라서 프라이버시권의 보편성, 즉 전국가적 권리로서의 성격을 확인할 수 있다. 이러한 프라이버시의 성질은 사법적 측면과 공법적 측면 모두에서 논하여지지만 그 본질적인 내용은 동일하다고 할 수 있다. 어느 경우나 기본적 인권, 나아가서는 그 근거로서의 인간의 존엄을 지키기 위한 기본적 권리이기 때문이다.

이러한 프라이버시권의 인권상의 위치는 내심의 자유에서 발생하는 근원적 권리라고 할 수 있다. 즉, 프라이버시는 내심의 자유에서 유래하는 것으로 내심의 자유를 보호하기 위한 것이다. 내심의 자유를 보호하기 위해서 자기의 사적영역의 불가침성을 주장하고, 그에 따라 내심의 자유를 현실적으로 보호하는 것이 프라이버시의 진정한 의미이다. 이러한 프라이버시는 내심의 자유를 기초로 하여 발생하면서도 그 보호범위를 확장한 개념이다. 즉 개인의 행동을 감시하거나, 개인간의 대화를 도청하거나, 사적 영역에 대한 간섭을 하는 것이 프라이버시를 침해하는 것이라고 하는 것에서 알 수 있듯이, 내심의 정신활동의 자유뿐만 아니라 행동이나 환경의 측면에서의 사적 영역에 대하여도 간섭을 배제하는 것으로서 장소적·공간적 영역을 포함하는 포괄적 개념을 의미하는 것이다. 그러므로 프라이버시권은 내심의 자유에 장소적·공간적 개념을 부가하여 그 보호범위를 확장한 권리인 것이다.[15]

2. 미국 프라이버시 개념의 토대

미국헌법(the U.S. Constitution)은 프라이버시권에 대한 명백한 규정을 두고 있지 않다.[16] 프라이버시와 관련한 많은 사례들은 수정헌법 제4조[17](the Fourth Amendment)에 근거한다. 미국대법원(the U.S. Supreme Court)은 정부의 프라이버시

14) Richard C. Turkinton and Anita L. Allen, Privacy Law, West Group, p.26 (1999).

15) 牧野二郎, "プライバシーとはなにか·「プライバシー保護」と「個人情報保護」のし違いに關する考察", pp. 2-4, <http://www.justnet.ne.jp/--ilc.journal.990828_1.htm> (2001. 2. 9.).

16) Fred H. Cate, "*The Changing Face of Privacy Protection in the European Union and the United States*", 33 Ind. L. Rev. 174, 196 (1999).

17) 수정헌법 제4조는 수정헌법 제14조를 통하여 주들(States)에 적용된다. Mapp v. Ohio, 367 U.S. 643, 655, 6 L.Ed.2d 1081, 81 S.Ct. 1684 (1961).

침해행위에 대한 다양한 사적 프라이버시의 요소들에 대하여 일정한 보호를 주기 위하여 권리장전(Bill of Rights)을 구성하는 수정헌법들을 많이 해석하여 왔다.[18]

미국에서의 프라이버시 개념은 수정헌법 제4조와 19세기 프라이버시 보호를 위한 근간을 이루었던 조화된 원칙들 이상의 의미로 확장하여 왔다.[19] 오늘날의 프라이버시는 여전히 경찰이 영장 없는 가택수색을 할 수 없음을 의미한다. 또한 오늘날의 프라이버시는 국민이 출산기능을 결정하는데 대한 정부의 권리가 제한된다는 것을 의미한다.[20] 더욱이 일정한 프라이버시권은 사적 부문의 행위(private sector activity)를 제한하기 위하여 성장하였다.[21]

미국헌법은 정부에 대한 국민의 권리를 설정한다. 따라서 사적 국민이나 기업이 다른 사적 국민이나 기업에 관한 정보를 수집할 때는 어떠한 국가행위(state action)도 존재하지 않는다.[22] 미국헌법의 초안자들은 언론의 자유권과 마찬가지로 재산권을 프라이버시의 근간으로 파악하였다.[23]

20세기 초에 미국대법원은 전화대화도청과 관련한 사건에서 사적 정보를 재산권으로 보는 견해에 도전하는 사례를 다루게 되었고,[24] 미국대법원은 도청은 수정헌법 제4조에 순응할 필요가 없다고 판시하였다.[25] 그러나 Katz v. United States 사건[26]에서 법원은 심지어 도청이 불법침해(trespass)를 구성하지 않는다 할지라도 도청자들은 수정헌법 제4조를 따라야 한다고 판결하였다.[27] 이 사건으로 인하여 미국법원은 프라이버시권을 독자적인 재산권으로 인정하게 되었다.

---

18) Cate, *supra note 16)*, pp. 49-66.

19) Solveig Singleton, "*Privacy Versus the First Amendment: A Skeptical Approach*", 11 Fordham I. P., Media & Ent. L. J. 97 (2000).

20) *Id.*

21) *Id.*

22) 예컨대, United States v. McAllister, 18 F. 3d 1412, 1417-18 (7th Cir. 1994); United States v. Reed, 15 F. 3d 928, 931 (9th Cir. 1993); Pleasant v. Lovell, 974 F. 2d 1222, 1226 (10th Cir. 1992); United States v. Attson, 900 F. 2d 1427, 1432 (9th Cir. 1990) 참조.

23) William C. Hefferman, "*Property, Privacy, and the Fourth Amendment*", 60 Brook. L. Rev. 633 (1994). 여기서는 재산권이 개인적 자유에 대한 하나의 개선이자 표현이며 동일한 보호를 받아야 할 것이라고 주장한다.

24) Olmstead v. United States, 277 U.S. 438 (1928).

25) *Id.* p. 466.

26) 389 U.S. 347 (1967).

27) *Id.* p. 359.

오늘날 프라이버시의 재산권이론은 수정헌법 제4조가 프라이버시의 합리적 기대(a reasonable expectation of privacy)에 대한 침해로부터 국민들을 보호한다는 신이론에 굴복하였다.[28] 그러나 프라이버시의 합리적 기대이론은 완전히 새로운 감시방식을 채택할 때 법원의 지침이 되지 않는다. 예컨대, 오늘날 사람들이 인터넷상 프라이버시의 기대를 가진다면, 그 기대는 기술 그 자체가 지속적으로 정보를 교류한다는 것을 이해하지 못하는 경우에만 오로지 존재할 것이다. 합리적 기대기준은 제3자가 보유한 개인기록으로 프라이버시권을 창설하지 않는다.[29] 누구나 정보를 제3자에게 노출할 때 그 자신의 프라이버시 기대를 포기하기 때문이다.[30] 노출된 정보의 소유권을 보유하지 않는 한 수정헌법 제4조의 재산권 이론하에서 비슷한 결과를 획득할 수 있다.[31]

고려해야 할 또 다른 요소는 수정헌법 제4조에서 직접 추출되지 않는 프라이버시의 헌법적 권리이다. 프라이버시의 헌법적 권리는 수정헌법 제1조, 제3조, 제4조, 제5조, 제9조 그리고 제14조의 '경계영역'(penumbra)으로부터 추론된다.[32] 한가지 예외[33]

---

28) California v. Greenwood, 486 U.S. 35, 39 (1988); California v. Ciraolo, 476 U.S. 207, 211 (1986); Oliver v. United States, 466 U.S. 170, 177 (1984) 참조.

29) Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494-95 (1975). 이 사건은 일반적인 프라이버시법은 정보가 이미 공공기록에 나와 있는 경우 프라이버시 이해관계가 사라진다는 점을 대체로 인식하고 있다고 인정하였다; Walls v. City of Petersburg, 895 F.2d 188, 193 (4th Cir. 1990)에서는 프라이버시 보호는 개인이 프라이버시에 대한 합리적인 기대를 가지는 정보에만 적용한다는 것을 설명한다. 공공기록에서 쉽게 가용한 정보에까지 보호가 확산되지는 않을 것이다.

30) 예컨대, United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990). 이 사건에서는 형사 피고인은 그의 호출기 번호에서 프라이버시의 기대를 가지지 않는다고 판시하였다. 그 이유는 그가 자발적으로 다른 사람에게 그의 호출기 번호를 넘겨주었기 때문이다; United States v. Miller, 425 U.S. 435, 437-40 (1976). 이 사건에서는 형사 피고인은 그의 은행에 의하여 보관되는 금융기록에 대하여 수정헌법 제4조의 보호를 받지 못한다고 판결하였는데, 이는 그가 기록의 소유권을 가지거나 점유권을 행사하지 못하기 때문이다.

31) California v. Greenwood, 486 U.S. 35, 40-41 (1988). 이 사건에서는 쓰레기 수거인과 같은 제3자에게 양도할 목적으로 길모퉁이에 둔 쓰레기에 대하여는 수정헌법 제4조 프라이버시 보호에 대한 합리적인 기대를 가질 수 없다고 결론지었다; Katz v. U.S., 389 U.S. 347, 351 (1967)에서 법원은 "개인이 알면서 대중에게 노출한 사항은 수정헌법 제4조의 보호대상이 아니다"라고 판시하였다.

32) 예컨대 Roe v. Wade, 410 U.S. 113, 152-53 (1973). 이 사건에서는 다양한 헌법적 규정들이 만들어 내는 '프라이버시의 영역 또는 지대'(areas or zones of privacy)에서 발생하는 프라이버시권을 구한다; Thornburgh v. American College of Obstetricians, 476 U.S. 747, 772 (1986)에서는 낙태규제와 관련한 한 주의 법령을 위헌으로 판결한다; Whalen v. Roe, 429 U.S. 589, 599-600 (1977)에서는 혼인, 출산, 피임, 가족관계, 자녀양육 및 교육과 관련한 이전의 대법원 결정들은 일정한 종류의 기본적 결정들을 규율하기 위한 주의 권력을 일반적으로 제한하려는 것으로 특성화하고 있다.

와 함께 경계영역은 신체 또는 가정의 프라이버시 맥락에서 출산 또는 성적 기능(reproductive or sexual functions)과 관련한 사례에서 인식되어 왔다.[34] 수정헌법 제4조와 경계영역 사례에서 가능한 한가지 기초적인 관측은 정부침해에 대한 프라이버시의 헌법적 권리는 수정헌법 제1조와 거의 충돌하지 않는다는 것이다.[35] 어떤 점에서 헌법적 프라이버시 사례는 또 다른 방식으로 표현된 수정헌법 제1조의 권리이다. 영장 없이 수색당하지 않을 권리는 수정헌법 제1조가 또한 보호하고 있는 말하지 않을 권리(the right not to speak)의 자격과 동등하다.[36] 결국 수정헌법 제1조와 제4조는 정부의 권력을 비슷한 방법으로 제한한다.[37]

3. 미국 프라이버시 법제의 특성

미국의 프라이버시법의 특성중의 하나는 여러 가지 형태의 다양한 프라이버시를 수집한 것이라 할 것이다. 특정한 프라이버시 문제에 초점을 두는 프라이버시법의 경향은 미국에서의 프라이버시법이 단편적(piecemeal)이라는 비판을 초래하였다.[38] 미국 대법원장 Rehnquist는 미국대법원의 견해에서 프라이버시를 분류묘사가 불가능하다고까지 하였다.[39] 이러한 프라이버시의 다양성(diversity)은 그 생명력에 기여하면서 인

33) 그러나 Stanley v. Georgia, 394 U.S. 557, 568 (1969) 사건에서는 집에서 외설자료를 소유하는 것은 특히 수정헌법 제1조의 프라이버시권의 관점에서 헌법적으로 보호된다고 판결하였다.

34) 예를 들면 Roe v. Wade, 410 U.S. at 153 사건에서는 자주적인 출산행위를 할 여성의 권리에 대한 프라이버시권을 확대하였다; Payton v. N.Y., 445 U.S. 573, 601 (1980). 여기서는 미국이 허가되지 않은 침입이라는 문맥에서 가정의 신성함을 오랫동안 인식해왔다고 지적한다; Russell D. Workman, "*Balancing the Right to Privacy and the First Amendment*", 29 Hous. L. Rev. 1059, 1962-63 (1992)에서는 혼인, 자녀양육 및 가족관계를 포함하는 헌법의 경계영역(the penumbras of the Constitution)에서의 프라이버시권의 역사에 대하여 토론한다.

35) 예컨대, Hudgens v. NLRB, 424 U.S. 507, 520-21 (1976)에서는 시위대들은 신발가게에 대항하는 그들의 시위를 선전하기 위하여 쇼핑센터를 불법침입(trespass)할 수정헌법 제1조의 권리를 가지지 않는다고 판결한다.

36) Wooley v. Maynard, 430 U.S. 705, 713 (1977).

37) Ken Gormley, "*One Hundred Years of Privacy*", 1992 Wis L. Rev. 1335, 1383-84 (1992). 이 사건에서 미국 대법원은 수정헌법 제1조의 언론의 자유에 대한 프라이버시권을 본질적으로 공생관계로 조직하면서 자동적으로 조화시키려는 경향을 보인다.

38) Dorothy J. Glancy, "*Symposium on Internet Privacy: At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*", 16 Computer & High Tech. L. J. 357, 359 (2000).

39) Paul v. Davis, 424 U.S. 693, 713 (1976).

터넷 이해관계에 대한 프라이버시 이론적용을 가능하게 한다.

미국에서의 프라이버시법의 다양성에 대한 하나의 측면은 여러 형태의 민사적 또는 형사적 프라이버시법들이 프라이버시 이해관계를 보호하고 지지한다는 점이다. 비록 대부분이 인터넷 이전에 발전된 것이지만, 다양한 형태의 프라이버시법들은 인터넷 사용자들의 온라인 행위에 적용할 수 있다. 예컨대, 헌법, 보통법(common law), 성문 및 규제적 프라이버시법 그리고 비정부적 자기규제법 등은 인터넷 사용자들을 위한 법적 프라이버시권을 위한 근거가 될 수 있다.

웹(web)에서의 특정한 프라이버시법의 적용은 프라이버시 침해의 문맥에 의존한다. 이러한 문맥 의존성은 적어도 프라이버시법이 지난 세기동안 진보해 온 방식[40]이나 특정한 프라이버시 침해의 반응에서 부분적으로 설명된다. 비록 몇몇 프라이버시법은 전자감시(electronic surveillance)적인 정보수집과 같이 프라이버시 침해의 일반적 형태에 광범위하게 적용되지만, 전형적으로 프라이버시법은 개인정보의 특정상황이나 형태에 초점을 둔다.[41] 프라이버시법은 특정형태의 프라이버시 문제를 해결하거나, 프라이버시의 침해에 반응하거나, 아니면 개인정보의 특정형태를 보호하는 특징을 가지면서 진보하여 왔기 때문에, 문맥이 프라이버시법의 다양성에서 중대한 역할을 한다는 것은 당연하다 할 것이다.

미국 프라이버시법의 또 다른 특성인 분산성(decentralization)은 인터넷과 프라이버시법의 교차점에 대한 이해를 한층 복잡하게 한다. 서로 다른 문맥에서 작동하는 다양한 형태의 프라이버시법들이 있을 뿐만 아니라, 이들 법의 근원 역시도 서로 다르다. 연방법과 주법은 미국에서의 프라이버시법의 주요근간이 된다. 더욱이 이들 주와 연방의 프라이버시법들은 프라이버시 정책과 산업 프라이버시 기준과 관련하여 사적 부문의 대표들과 상호작용한다.[42]

연방주의는 왜 미국 프라이버시법이 집중화된 일괄타결접근법(one-size-fits-all)을 일반적으로 피해왔는지를 설명하는 주된 이유이다. 연방주의를 반영하면서 미국 프라이버시법은 연방과 주법 모두를 혼합하고, 주마다 상당히 다양한 주의 프라이버시법(state privacy laws)의 다양한 형태를 조정한다. 연방과 주 프라이버시법의 분산화된 형태의 좋은 예는 전자감시(electronic surveillance)와 관련한 연방과 주의 프라이버시법의 복합적 규제이다.[43] 최초로 연방헌법과 성문법규에 근거한 전자감시법

40) Samuel D. Warren & Louis D. Brandeis, "*The Right to Privacy*", 4 Harv. L. Rev. 195 (1890).

41) Glancy, *supra note* 38, p. 374.

42) *Id.*

(electronic surveillance laws)은 이제 인터넷 통신의 전자감시에 적용할 수 있는 연방과 주의 프라이버시법의 다양성을 포용한다.

미국에서의 프라이버시 보호는 전형적으로 연방과 주의 프라이버시법의 혼합에서 나온다 할지라도, 연방과 주의 프라이버시법의 분산화된 형태에 대한 한가지 흥미로운 예는 연방 공정신용평가법(Federal Fair Credit Reporting Act)[44]하에서의 소비자의 신용기록에 대한 프라이버시에 적용하는 법이다. 몇 가지 제한된 예외와 함께 오직 연방법만이 공정 신용 보고법과 관련한 문제에 적용한다.[45] 공정신용평가법과는 별도로 주의 프라이버시법은 일반적으로 연방법에 의해 선점당하지 않는다. 인터넷 사용자들은 통일된 연방 프라이버시법에 대한 흥미를 표명하지 않아 왔다. 오히려 연방 프라이버시법과 주의 프라이버시법 사이에서와 마찬가지로, 주의 프라이버시법들 사이에 양성(良性)적 변동(benign variation)이라는 Brandeis의 개념이 미국에서 선호되는 프라이버시법의 형태이다.[46]

미국 프라이버시법의 세 번째 특성은 미국 프라이버시법의 다양성(diversity)과 분산성(decentralization)을 조합하는 역동성(dynamism)이다. 19세기의 시초부터 프라이버시법은 개인의 프라이버시 이해에 대한 새로운 도전들, 특히 신기술에 의하여 생성된 도전들에 대한 응답에서 전개하였다. 이전의 프라이버시법이 인터넷에 의하여 야기되는 새로운 도전에 직면하는 것과 마찬가지로 프라이버시법의 동적인 본질은 명백하다.[47] 미국에서 프라이버시권의 인식에 대한 본질적 주장은 사회적·기술적 변화에 대한 응답의 필요성에 근거한다.

라디오나 방송의 토크쇼와 같은 대중문화의 측면에서 명백한 개인생활의 세부사항을 엿보는 현대사회의 관음증적 이해관계는 프라이버시를 더욱 보호하려는 법률의 발전에 대항하는 하나의 반대세력이다.[48] 모든 종류의 일상생활을 포함하는 인터넷은

---

43) 예컨대, Electronic Communications Privacy Act, 18 U.S.C. 2701-11 (1994); Privacy Protection Act, 42 U.S.C. 2000aa to 2000aa-12 (1994); McVeigh v. Cohen, 983 F.Supp. 215 (D.D.C. 1998); 연방법규는 전자통신프라이버시법(Electronic Communications Privacy Act, 18 U.S.C. 2510-22 (1994))과 컴퓨터사기및남용법(Computer Fraud and Abuse Act, 18 U.S.C. 1030 (1994))을 포함하고 있다.

44) 15 U.S.C. 1681-81t (1994).

45) *Id.*

46) New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis 대법관의 반대의견). Brandeis 대법관은 "하나의 용감한 주(State)가 그 시민들의 선택하에 하나의 실험실로 기능하면서 새로운 사회적·경제적 실험들을 시도할 수 있다는 것은 연방주의의 큰 장점들 가운데 하나"라고 지적하였다.

47) Glancy, *supra note* 38, p. 380.

개인의 생활을 사실상 어느 때든지 웹(web)상으로 이동하게 한다. 인터넷 그 자체가 급속히 발전함에 따라 새로운 프라이버시 문제들이 발생할 것은 명백하다. 이러한 새로운 프라이버시법 이슈에는 무선 인터넷 통신의 보안성과 관련한 강화된 프라이버시 문제들 뿐만 아니라, 인터넷 사용자가 인터넷상에서 다양한 사이트들로 접속할 때 개인의 지리학적 위치를 정확히 찾아내는 정보에 대한 개인의 통제같은 프라이버시 문제들을 포함할 것이다.

III. 미국의 프라이버시 법제의 현황

1. 프라이버시에 대한 미국헌법 및 연방법의 보호

미국에서 개인의 프라이버시는 헌법적 보장, 연방 및 주의 성문법규, 규칙, 자율적 행위규범 등을 통하여 보호되며, 이들 모두는 서로 다른 방법으로 공적·사적 부문에 적용된다. 비록 미국헌법(the U.S. Constitution)이 프라이버시권을 명백히 규정하고 있지는 않지만, 미국대법원은 수십년전 기본적인 프라이버시권 또는 혼자 있을 권리(the right to be left alone)를 인정하였다.[49] 그 이후 법원은 권리장전(Bill of Rights)이 "개인의 프라이버시 또는 프라이버시의 일정한 영역이 헌법상 존재함을 보장"하는 창조적 성격을 가지는 것으로 해석한다.[50] 헌법적 보장과는 별개로 프라이버시에 관한 미국의 입법적 접근은 전통적으로 분야별로 이루어졌다. 즉, 미국의 프라이버시법은 특정한 데이터 형태나 사용자들을 다루기 위하여 발전하였다.[51] 역사적으로 사적 데이터를 정부가 사용하는 것에 대한 두려움이 최초의 근심거리였다. 따라서 어떤 성문법규는 정부가 보관하는 사적으로 신분확인이 가능한 데이터의 사용을 제한한다.[52] 어떤 법규들은 산업체에 의하여 보관되는 개인정보에 대한 정부의 사용을 제한

48) Richard Posner 판사는 프라이버시에서의 이해관계와 비교하여 사회의 관음증은 훔쳐보기의 이해관계로 묘사하였다. Richard Posner, "*The Right of Privacy*", 12 Ga. L. Rev. 393, 394-97 (1978).

49) Griswold v. Connecticut, 381 U.S. 479, 483-86 (1965).

50) Roe v. Wade, 410 U.S. 113, 152 (1973).

51) 예를 들어 1994년 운전자프라이버시보호법(Driver's Privacy Protection Act of 1994, 18 U.S.C.A. 2721-25 (West Supp. 1999))은 주의 운전면허국(Department of Motor Vehicles)이 관리하는 기록에 포함된 개인정보의 공개나 판매를 규제한다. 최근 South Carolina 주는 이 법이 연방주의의 기본원칙을 침해한다고 주장하면서 위헌여부를 위한 소송을 제기하였다. 미국 대법원은 결국 운전자의 프라이버시 보호법이 합헌이라 판결하였다. Reno v. Condon, 120 S.Ct 666 (2000).

한다.[53] 또 어떤 법규들은 개인정보에 대한 회사의 사용을 제한한다.[54] 하나의 단일 법이나 규제가 정보 프라이버시에 대한 미국시민의 일반적 권리를 특정하게 인식하지는 않지만, 열거된 바와 같은 일정한 법들은 소비자들의 프라이버시를 상당부분 보호한다.

정부의 데이터 수집과 사용에 관한 프라이버시 규제는 비정부적 조직들에 대하여 가용한 것보다 훨씬 광범위하게 이루어진다. 예컨대, 연방 프라이버시법(Federal Privacy Act)은 정부기관들이 ① 관련한 필수적인 개인정보만을 저장하고, ② 데이터 목적을 위하여 가능한 범위까지만 정보를 수집하며, ③ 정확하고 완전한 기록을 유지하고, ④ 기록의 보안성을 유지하기 위하여 행적적·기술적 안전장치를 마련하도록 의무 지우고 있다.[55] 프라이버시법(Privacy Act) 또한 개인의 기록에 대한 노출을 제한한다.[56] 그러나 이 법은 법규정이 정보 자유법(Freedom of Information Act)(이하 FOIA)하에 공개가 요구되는 어떠한 자료의 공개를 금지하는 것을 명백히 제한한다. FOIA는 아홉가지의 열거된 면제(exemptions)를 제외한 모든 연방기관의 기록들에 대한 접근을 허용한다.[57] 더욱이 프라이버시법은 다른 정부기관에 정보공개를 허용하는 열두가지의 면제를 부여한다.[58]

---

52) 예컨대, 세금개혁법(Tax Reform Act of 1976, 26 U.S.C. 6103 (1994 & Supp. I 1995))은 납세보고의 기밀성과 납세관련 정보를 보호하며 개인적 납세 데이터의 보급을 제한한다. 또 다른 예는 1974년 프라이버시법(Privacy Act of 1974, 5 U.S.C. 552a (1994))이며, 이 법은 이름이나 다른 사적 정보로 개인을 특정할 수 있는 기록들에 대한 정부의 창조, 수집, 사용, 보급을 규제한다.

53) 예컨대 전자통신프라이버시법(Electronic Communications Privacy Act, 18 U.S.C. 2510-22, 2701 (1994))은 연방정부와 주정부들이 구두, 유선 및 전자 통신에 접근할 수 있는 상황을 제한한다.

54) 개인 사업을 규제하는 프라이버시 법규에는 금융프라이버시권법(Right to Financial Privacy Act, 12 U.S.C. 3401-22 (1994)), 공정신용평가법(Fair Credit Reporting Act, 15 U.S.C. 1681-81t (1994)), 가족교육권및프라이버시법(Family Educational Rights and Privacy Act, 20 U.S.C. 1232g (1994)), 텔레마케팅보호법(Telemarketing Protections Act, 47 U.S.C. 227 (1994)), 케이블통신정책법(Cable Communications Policy Act, 47 U.S.C. 551(a) (1994)) 등이 있다.

55) 5 U.S.C. 552a(e)(1)-(5) (1994).

56) *Id.* 552a(b).

57) 5 U.S.C. 552 (1994). 아홉 가지의 면제중에 두 가지는 프라이버시를 보호하기 위하여 고안되었다. 면제 6 (Exemption 6)은 인사와 의료파일 및 공개가 명백히 개인적 프라이버시의 침해를 구성할 수 있는 유사한 파일들의 공개를 금지한다. 면제 7(C) (Exemption 7(C))는 개인의 프라이버시가 침해될 것이라고 합리적으로 예상가능한 법집행 목적을 위하여 수집된 기록이나 정보의 공개를 금지한다. Id. 552(b)(6)-(7)(C). 미국의 많은 주들이 FOIA에서 제시된 것과 유사한 프라이버시 본위의 면제들(privacy-based exemptions)을 가진 정부공개법령들을 가지고 있다.

58) *Id.* 552(a)(b)(1)-(12).

이 밖에 정부의 데이터 공개로부터 시민정보의 프라이버시를 보호하는 다른 법규와 규제가 많이 있다. 예컨대, 연방법은 건강및인류봉사국(Department of Health and Human Services)이 사회보장기록(social security records)의 공개를 금지시키지만, 달리 연방법이나 규제에 의하여 제공되는 모든 공개는 허용한다.[59]

미국의회도 금융거래와 같은 사적 산업부문에서의 개인정보보호를 다루는 다양한 법을 제정하였다. 1970년 공정신용평가법[60](Fair Credit Reporting Act of 1970)은 개인의 신용가치, 신용상태, 신용능력, 성격, 평판, 생활양식 또는 개성 등에 관한 소비자 보고에서 개인정보의 준비와 보급과 연관한 개인들의 권리와 소비자 신용평가기관의 책임을 규정하였다.[61]

1996년 9월 30일 의회는 공정신용평가법에 의하여 규정된 정보 프라이버시의 보호를 강화하는 소비자신용평가개혁법[62](Consumer Credit Reporting Reform Act)을 통과시켰다. 수정된 개정법의 통과이후에 공정신용평가법은 개인정보의 수집과 사용을 일반적으로 다루지 않는 반면, 신용정보의 내용, 공개, 그리고 사용을 현저히 제한하였다.[63]

또 다른 법규들은 특정 프라이버시 관련 이익을 보호한다. 예컨대, 1986년 전자통신프라이버시법[64](Electronic Communications Privacy Act of 1986)은 전화통화나 이메일 등 모든 전자통신의 내용에 대한 방해나 공개를 금지한다. 이 전자통신에는 심지어 참가자가 "그 통신이 정당한 상황하에 방해를 받지 않을 것이 기대"[65]되는 모든 대화를 포함한다. 명백히 광범위하다 할 수 있는 이러한 프라이버시권에는 수 많은 예외가 있고, 그 중 가장 중요한 것은 만일 통신의 어느 일방이 공개에 동의한다면 금지는 적용하지 않는다는 것이다.[66]

1996년 이전에는 전화번호나 시간, 장소, 통화기간과 같은 원격통신거래에 관한 정보의 성문법적 보호가 없었다.[67] 전자통신프라이버시법(Electronic Communications

59) 42 U.S.C. 1305 (1994).

60) 15 U.S.C. 1681-81t (1994).

61) Joel R. Reidenberg, "*Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*", 44 Fed. Comm. L. J. 195, 210 (1992).

62) 15 U.S.C. 1681-81t (Supp. 1997).

63) *Id.* 1681a(f), (d) (1944 & Supp. 1997).

64) 18 U.S.C. 2510-20 (1994 & Supp. 1997).

65) *Id.* 2510-11(2) (1994).

66) *Id.* 2511(2)(c).

Privacy Act)은 '거래적 정보'(transactional information)에 적용하지 않았고, 따라서 서비스 공급자들은 그러한 데이터의 수집, 저장, 공개에 관한 어떠한 법적 제한도 받지 않았다.[68] 그러나 1996년 2월 1일 의회는 1996년 전기통신법(Telecommunications Act of 1996)을 통과시켰고, 이 법은 소비자 소유의 네트워크 정보 프라이버시를 보호하는 규정을 포함한다.[69]

미국의회의 최근의 프라이버시법인 아동온라인프라이버시보호법[70](Children's Online Privacy Protection Act)은 13세 이하의 어린이들에 대한 정보의 온라인 수집을 금지한다. 어린이들을 주 대상으로 하는 이 법은 어린이들로부터의 정보수집을 인식하는 상업적 웹사이트들의 운영자들은 데이터 수집정책을 고지하고, 어린이들로부터의 정보수집 이전에 부모의 동의를 구하도록 요구한다.[71] 이 법은 연방거래위원회(Federal Trade Commission)에게 부모에 대한 고지와 동의의 형태 및 실체적 내용에 대한 대부분의 핵심이슈들을 위임한다.

2. 미국 프라이버시 관련 법제현황

미국은 각 부문별로 개인정보 또는 프라이버시와 관련한 법률을 제정하여 시행중에 있다. 이러한 제정법은 헌법이나 판례법에서 보장하는 권리보호를 해당 부문에서 더욱 명확하게 규정하여 원칙을 확립하고 있다는 점에 그 의의를 찾을 수 있다. 미국의 대표적인 개인정보관련 입법현황을 분류하여 보면 다음과 같다.

3. 세이프 하버 원칙

미국은 제정법이나 판례법 이외에도 개인정보보호를 위한 지침으로 세이프 하버 원칙을 정립하고 있다. 이 원칙은 1998년 10월 25일 발효된 EU지침에 대응하여 세워

---

67) 연방통신위원회(Federal Communications Commission)은 전화회사들 사이의 경쟁을 심화시키는 것과 같은 정보의 공개를 규제하였다. 47 C.F.R. 64. 702(d)(3) (1997); 위원회의 규제하에서 통신 서비스 공급업자들은 통신거래에 관한 정보를 경쟁자들에게도 공개하지 않는다면 서비스를 제공했던 자신들 소유의 회사들에게 그 정보를 공급할 수 없었다. 이에 관한 일반적 설명은 Fred H. Cate, "*Privacy and Telecommunications*", 33 Wake Forest L. Rev. 1, 37-41 (1998) 참조.

68) 18 U.S.C. 2511(2)(h)(i) (1994).

69) Pub. L. No. 104-104, 11 Stat. 56.702 (47 U.S.C. 222 (Supp. 1996)으로 성문화).

70) Pub. L. No. 105-277, 112 Stat. 2681 (15 U.S.C. 6501로 성문화).

71) *Id.*

진 원칙으로써, 해당지침의 규정의 수준에 맞는 개인정보보호 체계를 갖추지 못한 제3국으로의 개인정보 국외이전에 대한 제한에 대하여 미국이 자국의 피해를 방지하기 위하여 세운 원칙이다.

미국은 EU와 그 회원국에 대하여 미국 시스템이 적절한 보호를 갖추고 있다는 점을 설득하기 위하여 강력한 로비를 펼쳤다. 1998년 미국은 EU와 개인데이터의 국가간 유통을 지속하기 위하여 세이프 하버 동의("Safe Harbor" agreement)를 위한 협상을 개시하였다. 세이프 하버 원칙이란 유럽연합 회원국과의 국제교류와 관련하여 유럽 시민들의 개인정보를 전달받아 처리하는 미국 기업이 EU지침에서 규정한 '적정성'을 갖추고 있는지를 자발적으로 확인할 수 있도록 제시한 프라이버시 원칙들이다.[72]

세이프 하버 원칙은 개인정보 취급의 적정성 여부를 판단하기 위한 특정한 목적을 가진 원칙이기 때문에 국제조약의 성격을 가지지는 않는다. 즉, 이 원칙에 따를 것인지의 여부는 전적으로 미국기업들에게 달려 있는 것이다. 그러나 실질적으로 이 원칙을 따를 경우 유럽위원회로부터 개인정보의 적정성을 확인받게 되는 결과가 되기 때문에, EU 회원국과 별도의 협의와 논의를 진행할 필요가 없이 적정성이 추정되게 된다. 따라서 현재 미국에서는 이 원칙의 장점에 따라 다수의 기업체가 참여하고 있다. 세이프 하버 원칙은 고지(notice), 선택(choice), 정보이전(onward transfer), 접근(access), 안전(security), 데이터 무결(data integration), 집행(enforcement)의 총 7개 원칙으로 구성되어 있다.

결국 미국 상부부(U.S. Department of Commerce)와 유럽위원회(European Commission)는 2000년 6월 그들이 세이프 하버 협정을 체결하였음을 발표하였다. 따라서 미국 회사들은 지속적으로 유럽으로부터의 데이터를 전송받을 수 있게 되었다. 유럽의회(European Parliament)는 협정에 대하여 더 강력한 프라이버시 보호를 구하도록 하는 결의안을 채택하였으나, 유럽위원회는 미국과의 세이프 하버 협정을 그대로 지속 추진할 것임을 발표하였다.

IV. 미국의 프라이버시 관련 법률의 주요내용

1. 공정신용평가법(Fair Credit Reporting Act, 1970)

72) M. Hicks, Passing the Safe Harbor By, eWEEK (2001. 6. 11.), <www.eweek.com/article2/0,3959,220471,00.asp.>

공정신용평가법은 미국의 신용평가기관들(Credit Reporting Agencies)에 의한 개인정보의 오·남용을 막고 개인정보를 보호하기 위해 1970년 제정된 대표적인 개인신용정보보호법이다. 이 법은 신용평가기관들이 개인신용정보의 비밀성과 정확성을 보고하기 위한 '합리적 절차'를 준수할 것을 강제하는 내용을 담고 있다. 이 법은 합리적 절차를 판단하기 위한 기준으로서, 개인의 정보접근권, 개인정보 보안, 개인정보의 파기, 필요한 사항에 대한 고지, 정보주체의 동의, 신용평가기관들의 책임성에 관한 내용을 포함하는 공정한 정보관행체계를 규정하고 있는데, 이에 의하면 신용평가기관들은 은행, 신용카드회사, 기업, 임대업자 등의 사업자가 개인의 신용을 평가하기 위해서만 정보를 사용할 것을 합리적인 믿음이 있는 경우나 기록의 주체로부터 서면동의가 있는 경우가 아니면 개인정보를 제공할 수 없다.

또한 신용평가기관이 정보요구자가 신용평가·고용평가·보험평가나 면허의 부여 또는 다른 정부수혜와 관련하는 경우 등에 정보를 사용할 것이라고 믿은 경우가 아니면 개인정보 공개를 제공할 수 없다.

2. 프라이버시법(Privacy Act, 1974)

1974년 프라이버시법은 미국 정부기관들이 보유한 기록을 보호하며, 정부기관들이 기본적으로 공정한 정보수행을 하도록 요구한다. 이 법은 정보주체의 열람 및 정정요구권, 필요한 범위 내에서의 정보수집원칙, 어떠한 정보가 수집되었는지에 대한 고지의무, 정보공유의 원칙적 금지 등의 내용을 담고 있다. 이 법은 개인들이 그들의 기록에 무슨 정보가 포함되며 어떻게 사용되는지를 알 수 있어야 하고, 사전동의 없이 하나의 목적으로 수집된 정보가 다른 용도로 사용되는 것을 방지한다. 그러나 이 법은 공공기관이 본래의 수집목적과 양립할 수 있는 '일상적인 이용'(routine use)을 위하여 해당하는 개인정보를 공개할 수 있도록 하고 있고, 특정한 공공기관의 경우에는 정보 정확성이나 기타 법적 의무로부터 면제되도록 하고 있어 실효성을 가지고 있지 못하다는 비난을 받고 있다.[73]

3. 정보공개법(Freedom of Information Act, 1974)

73) EPIC & PI, "Privacy and Human Rights 2003 - An International Survey of Privacy Laws and Developments", <http://www.privacyinternational.org/survey/phr2003/countries/unitedstates.htm>.

정보공개법은 거의 모든 정보요구자에 대하여 정부에 의하여 수집된 개인정보의 공개를 허용한다. 미국의 정보공개법은 모두 9가지의 비공개사항(exemptions)을 열거하고 있는데, 이 중 개인정보보호와 관련되는 조항은 여섯 번째와 일곱 번째이다.[74]

여섯 번째 비공개사항(5 U.S.C. 552(b)(6))은 공개하게 되면 개인의 프라이버시가 명백히 침해당하는 인사 및 의료에 관한 파일 및 이와 유사한 자료에 대하여 비공개를 유지할 것을 요구한다. 이 비공개사항은 개인의 프라이버시와 국민의 알권리 사이의 이익형량을 요구하고 있다. 프라이버시의 이익과 형량되어야 할 것은 정보공개에서의 국민의 이익이다.

일곱 번째 비공개사항(5 U.S.C. 552(b)(7)(C))은 법집행목적을 위하여 수집된 기록 또는 정보가 개인의 프라이버시에 대한 부당한 침해가 될 것이 합리적으로 예상되는 경우 그 기록 또는 정보를 공개할 수 없도록 하고 있다.

4. 가족의교육권및프라이버시법(Family Education Rights and Privacy Act, 1974)

가족의교육권및프라이버시법은 학생의 교육정보에 대하여 학부모와 학생의 자기정보결정권을 강화하고 프라이버시의 관점에서 교육정보를 보호하기 위하여 제정된 법이다. 이 법은 학교와 같은 교육기관이 연방기금을 수여받지 못하게 되는 몇 가지 사항에 대하여 적시하고, 이에 대한 감독권을 교육부에 부과함으로써 학생 및 학부모의 교육정보에 대한 권리를 보장한다. 즉, 연방기금의 수여조건으로 정보처리자인 교육기관이 교육정보를 수집·이용·보유·공개 등 처리과정에서 지켜야할 몇 가지 의무를 부과하고 있다. 따라서 연방기금을 지속적으로 수여받고자 하는 교육기관은 이 법에서 규정하는 의무를 준수하여야 한다.

이 법에 따르면, 학생 또는 학부모는 교육기관이 보유한 자신 또는 아동의 교육정보에 대하여 조사·심사하고 이를 통해 잘못된 내용이 있으면 정정을 요청할 수 있도록 하고 있고, 나아가 개인식별정보(personally identifiable information)의 공개를 중지하도록 요구할 수 있는 권리를 행사할 있다. 또한 교육기관은 '교육기록내 개인식별정보'를 학생 또는 학부모의 서면동의 없이 공개할 수 없으며, 학교가 유지·관리하고 있는 교육정보에 대해 자격있는 학생 및 학부모에게 고지하여야 한다.

---

74) 5 U.S.C. 552(b)(6); 5 U.S.C. 552(b)(7)(C).

5. 금융프라이버시권법(Right to Financial Privacy Act, 1978)

금융프라이버시권법은 은행기록을 위한 수정헌법 제4조의 성문적 보호에 근거하여 개인금융기록의 비밀을 보장하기 위하여 제정된 법이다. 금융프라이버시권법에 따르면, 어떠한 정부관계자(Government authority)라도 금융기록이 합리적으로 기록되지 않은한 금융기관으로부터 고객의 금융기록에 포함된 정보 및 그 사본에 접근하거나 그를 획득할 수 없다. 그러나 이 법은 개인정보를 예외적으로 공개할 수 있는 경우도 규정하고 있는데, 고객이 접근을 허락한 경우, 적절한 행정소환장이나 출두명령이 발부된 경우, 적법한 수색영장이 발부된 경우, 적절한 법원소환장이 발부된 경우, 그리고 공인된 정부당국으로부터의 적절한 서면요구가 있는 경우가 그 예이다.

6. 프라이버시보호법(Privacy Protection Act, 1980)

미국의회는 출간자에 대한 수색 및 압수집행의 효력을 경감하기 위하여 프라이버시보호법을 제정하였다. 이 법은 미국 정부공무원이 출간자가 출간물이 범죄와 관련하였거나 관련하게 될 것이라고 믿을만한 충분한 개연성(probable cause)이 없는 한, "신문, 방송, 또는 이와 유사한 형태의 통신매체를 통하여 일반에게 공개할 목적을 가지고 있다고 믿은 개인"이 보유한 어떠한 작품, 산출물, 또는 문서자료에 대한 수색이나 압수를 금한다. 프라이버시보호법은 수정헌법 제1조 행위에 종사하는 자들로부터 증거를 획득하기 위한 소환장이나 자발적 협조를 구하기 위한 법집행에 효과적으로 사용된다.[75]

7. 케이블통신정책법(Cable Communications Policy Act, 1984)

1984년 미국 의회는 케이블TV 기술의 진보 및 양방향 케이블 시스템의 개발이 초래할 부당한 개인정보의 수집에 대한 위험에 대비하여 케이블통신정책법[76]을 제정하였다. 이 법은 케이블을 통해 서비스를 제공하는 자에 대하여 여러 가지 의무를 부과한다.

이 법은 케이블통신회사에게 적어도 1년에 한 번씩 고객에게 회사의 개인정보 수집 및 보유현황에 대하여 고지토록 강제하여, 고객이 사업자의 개인정보 수집 및 이

75) Federal Trade Commission (2001) <www.ftc.gov> 참조.

76) 47 U.S.C. 551.

용을 제한할 수 있는 기회를 가질 수 있도록 하고 있다. 케이블통신회사가 고지하여야 할 내용으로는 수집목적, 수집정보의 내용, 정보공개 예상시 보유기간 및 개인정보 열람요구절차 등에 관한 사항이다. 또한 이 법은 고객에 관한 정보가 사전동의 없이 이용 또는 제3자에 대한 제공을 금지한다. 단, 서비스의 제공에 관한 합법적인 영업활동과정에서 이루어진 정보의 공개는 예외이다.

8. 전자통신프라이버시법(Electronic Communications Privacy Act, 1986)

전자통신프라이버시법은 전자기록에 관한 정부의 접근절차 및 방법에 대하여 통제함으로써, 전자기록의 비밀성을 보호하는 규칙을 그 내용으로 담고 있다. 이 법은 수색영장이나 수신자의 동의 없이 서신을 개봉하는 것을 금지하는 법률 및 당사자의 동의가 없는 전화, 테이터 전송, 라디오 통신의 차단 또는 도청장치의 사용을 금지하는 법률의 통신 프라이버시 보호의 내용을 전자메일이나 기타 컴퓨터를 통한 데이터 전송과 같은 새로운 통신분야에 확장시킨다는 의미를 가진다. 특히 이 법은 저장된 음성메일 및 전자메일에 대한 권한 없는 접근이나 이용을 금지하고, 이러한 저장된 이메일 내용을 해당 전자통신 서비스제공자가 외부에 공개하는 것을 금지한다. 이러한 금지규정을 위반한 자는 형사상 제재뿐만 아니라, 고의적 위반행위로 인하여 피해를 입은 자는 민사소송을 통해 금지명령 등의 피해구제를 청구하거나 금전적 배상을 요구할 수 있다.[77]

전자통신프라이버시법의 중요한 세 가지 예외는 다음과 같다.

첫째, 온라인 서비스는 송신자가 시스템이나 다른 사용자에게 해를 입히려고 의심할 만한 이유가 있으면 사적인 이메일을 검열할 수 있다. 그러나 무작위적인 이메일 모니터링은 금지된다.

둘째, 온라인 서비스는 메시지의 송신자 또는 수신자가 검열이나 공개에 동의한 경우 적법하게 사적 메일을 검열 또는 공개할 수 있다. 많은 상업적 서비스들은 새로운 회원이 서비스를 위하여 계약할 때 동의를 구하여야 한다.

셋째, 고용주가 이메일 시스템을 소유할 때, 고용주는 시스템상 고용인 이메일의 동의를 검열할 수 있다. 따라서 하나의 사업지역으로부터 발송된 모든 이메일은 사적

77) Ronald L. Plesser and Sheldon Krantz, "*Privacy and Related Issues*", Internet and Online Law (Kent D. Stuckey with Contributing Authors), Law Journal Press, 2000, pp. 5-9.

이 아닐 개연성이 높다. 일부 법원의 판례는 고용주가 그들 고용인의 이메일 메시지를 모니터할 권리를 가지는 것으로 판결하였다.

9. 컴퓨터사기및남용방지법(Computer Fraud and Abuse Act, 1986)

컴퓨터사기및남용방지법은 1994년, 1996년, 2001년 개정된 바 있다. 이 법은 연방컴퓨터 범죄에 해당하는 형사사기와 남용의 정의를 구체화하고, 이러한 범죄에 대한 기소를 위한 법적 장애물을 제거하기 위하여 제정되었다. 이 법은 '연방이해관계'와 관련한 컴퓨터에 대한 비공인된 접근에 대한 두 가지 중범죄와 컴퓨터 패스워드의 비공인된 유통에 대한 한 가지 경범죄를 규정한다.

중범죄중의 하나는 사기절도(fraudulent theft)를 수행할 목적으로 연방이해와 관련한 컴퓨터에 대한 비공인된 접속을 다루기 위하여 제정되었다. 또 다른 중범죄는 연방이해와 관련한 컴퓨터내의 정보를 변경하거나 그 컴퓨터의 사용을 방지하는 것을 포함한 '악의적 손상'(malicious damage)을 다루기 위하여 제정되었다. 악의적 손상이라는 침해는 의료기록의 변조를 포함하는 사례를 제외하고 1,000불 이상 피해자에게 손상을 초래해야만 한다.

또한 이 법은 주간통상(interstate commerce)에 영향을 주는 사기에 가담할 의도로 컴퓨터 패스워드를 유통하는 것을 연방 경범죄로 규정한다. 이 규정은 기밀컴퓨터 패스워드가 노출된 '불법전자게시판'(pirate bulletin boards)의 창조, 유지 및 사용에 대응하기 위한 규정이다.

10. 컴퓨터보안법(Computer Security Act, 1987)

컴퓨터보안법은 국가표준국(National Bureau of Standards)에게 연방컴퓨터시스템의 보안을 위한 표준과 가이드라인을 발전시킬 책임을 부여한다. 이 법은 컴퓨터시스템 자문회의(Computer Systems Advisory Board)가 제기되는 연방컴퓨터보안과 프라이버시 이슈들을 적시하여 이러한 이슈에 대하여 국가표준국에 자문을 하고, 관리예산처(Office of Management and Budget), 국가안보원(National Security Agency), 그리고 연방의회에 그 결과를 보고할 것을 규정한다.

이 법은 연방컴퓨터시스템내의 민감한 정보의 보안과 프라이버시를 향상시키기 위한 목적을 가진다. 이 목적은 민감한 정보를 보호하기 위한 컴퓨터시스템 보안 표준

과 가이드라인을 발전시키기 위하여 정부내에 초점을 두고, 정부기관들이 컴퓨터시스템보안계획을 수립함으로써, 컴퓨터시스템보안에 관한 연방공무원의 의식을 제고하기 위한 향상된 훈련을 통하여 달성된다.

11. 비디오프라이버시보호법(Video Privacy Protection Act, 1988)

비디오프라이버시보호법은 비디오테이프 판매사업자 또는 대여사업자가 개인정보를 포함한 비디오 대여기록을 고객의 동의 또는 법원의 승인 없이 제3자에게 제공하는 것을 금지함으로써 상업적 비디오테이프 이용자 또는 구매자의 프라이버시권을 보호하고 있다. 이 법은 당해 비디오를 빌려준 소비자에게 공개하는 경우, 소비자의 서면동의가 있는 경우, 연방형사법원의 영장 및 관할 주법원의 영장, 대배심의 소환장 도는 특별한 지침에 Ekfms 법원 명령에 의한 공개의 경우, 제3자에게 비디오 대여자의 이름과 주소만 공개된다고 할 때 해당 소비자가 반대할 기회를 가졌던 경우, 정보의 공개가 채권추심 등과 같이 비디오 대여사업자의 일상적인 영업행위 과정에서 부수적으로 발생하는 경우, 그리고 민사법원의 명령에 의한 경우에는 개인정보를 포함한 비디오 대여기록 정보의 공개를 허용한다.

이 법에 의하면 비디오 대여사업자가 이 법에 위반하였다고 주장하는 소비자는 언제든지 민사소송을 통하여 손해배상을 청구할 수 있다. 또한 불법적으로 획득된 비디오 대여기록 정보는 모든 법원의 소송에서 증거로 사용될 수 없으며, 이는 일정 기간내에 파기되어야 한다.

12. 컴퓨터정보조합및프라이버시보호법(Computer Matching and Privacy Protection Act, 1988)

1988년 컴퓨터정보조합및프라이버시보호법[78]은 연방기관을 포함하는 컴퓨터 정보조합은 연방혜택을 지원하는 개인이나 그 혜택을 받는 개인들에게 일정한 보호를 주는 경우에만 수행될 수 있도록 하고 있다. 이 법은 프라이버시법에 대하여 다음 사항을 요구한다. 즉, 컴퓨터를 이용한 정보조합 프로그램에 관계한 연방기관들에게 정보조합 프로그램에 참여하는 다른 기관과 서면동의를 협상하고, 데이터무결회(Data Integrity Board)의 승인을 득하여야 한다. 또한 의회와 관리예산처(OMB)에 정보조합

78) 5 U.S.C. 552a(o).

프로그램의 세부보고서를 제출하고, 지원자나 수혜자들에게 그들의 기록이 정보조합의 대상임을 고지하여야 하며, 개인의 혜택이나 지불을 감경, 연장, 또는 거부하기 이전에 정보조합 결과물을 확인할 것을 요구한다.[79]

13. 근로자거짓말탐지기보호법(Employee Polygraph Protection Act, 1988)

근로자거짓말탐지기보호법은 대부분의 민간부문 근로자들에 대한 거짓말탐지테스트 및 부과된 제약에 대한 가이드라인을 설립하기 위하여 제정되었다. 이 입법은 오직 상업적 민간부문에만 적용된다. 지방, 주, 그리고 정책부서와 같은 연방정부기관은 이 법의 영향을 받지 않는다. 학교기관이나 교정기관과 같은 공공기관도 이 법의 영향을 받지 않는다.

이 법에 따르면 민간사업자들은 입사지원자들에 대하여 사전고용에 대한 거짓말탐지테스트를 요구할 수 없다. 또한 이 법은 사업자들이 특정한 조건을 만족한 경우에만 거짓말탐지테스트를 실시 또는 실시에 대한 권유를 할 수 있게 하고 있다. 그러나 고용주들은 현재의 근로자가 테스트 요구나 제안을 거부하는 경우 이를 강제할 수 없으며, 거부에 근거한 처벌이나 불이익을 줄 수 없다.[80]

14. 전화소비자보호법(Telephone Consumer Protection Act, 1991)

1991년 전화소비자보호법은 침해적 텔레마케팅 수행의 확산과 소비자 프라이버시에 관한 그러한 수행에 관한 염려에 대한 소비자들의 불만에 응답하기 위하여 제정되었다. 이 법은 1934년 통신법 제2장을 수정하였는데, 이는 연방통신위원회(FCC)가 거주자인 전화가입자의 프라이버시권을 보호하는 규칙을 공표하도록 요구한 것이다. 전화소비자보호법에 따라 연방통신위원회는 텔레마케팅에 종사하는 모든 자에 대하여 전화를 받지 않을 것을 요구한 소비자들의 명단을 유지하도록 요구하는 보고서 및 명령을 내리게 되었다.

15. 운전자프라이버시보호법(Driver's Privacy Protection Act, 1994)

---

79) <http://www.privacilla.org/government/cmppa.html>.

80) <http://www.fas.org/sgp/othergov/polygraph/eppa.html>.

운전자프라이버시보호법은 주의 차량관리국(DMV: Department of Motor Vehicle)의 기록에 포함된 개인정보의 대중에 대한 공개를 제한하고 있다. 운전자프라이버시보호법이 일반적으로 차량관리국 공무원들이 인지하고 있으면서 기록내에 포함된 개인식별정보를 공개하는 것을 금지하는 반면, 몇 가지 광범위한 예외조항도 규정하고 있다. 2000년 1월 연방대법원은 이 법을 만장일치로 지지하였다. 연방대법원은 운전자의 면허증과 차량등록증으로부터 정보를 식별은 다른 공동체와 같이 연방의회에 의하여 규제될 수 있는 '주간통상에 관한 것'(thing in interstate commerce)이라고 판결하였다.

16. 법집행을위한통신지원법(Communications Assistance for Law Enforcement Act, 1994)

연방의회는 디지털 네트워크상의 통신에 개입하기 위하여 법원명령이나 다른 법적 권위에 따르는 정부의 능력을 보존하기 위하여 일명 디지털전화법(Digital Telephony Act)으로도 통하는 법집행을위한통신원조법을 제정하였다. 이 법은 전화회사가 발신자추적정보는 물론 모든 유선 및 전자통신에 대한 정부접근을 보장하도록 네트워크를 설정하도록 요구한다. 프라이버시 옹호자들은 입법의 초안단계에서 온라인 서비스 공급자들에 대한 정부접근을 보장하도록 설비를 갖출 것을 요구하던 규정을 제거할 수 있었다. 이 법은 거래데이터에 대한 정부접근을 위한 표준을 개선하는 부분과 함께 프라이버시를 강화하는 규정을 포함한다.

17. 전기통신법(Telecommunications Act, 1996)

연방의회는 1996년 전기통신법에 개인기록에 대한 전화회사의 오용에 관한 우려를 다루는 규정을 포함하였다. 이 규정은 새로운 서비스를 판매하기 위하여 전화가입자의 통화유형(calling patterns)에 관한 정보를 이용하기 전에 통신회사들이 고객으로부터 승인을 얻도록 하고 있다. 이 법은 통신회사들에게 고객의 정보를 사용하기 이전에 승인을 얻도록 요구하는 반면에, 연방의회는 통신회사들이 어떻게 그 승인을 얻어야 한다는 점은 적시하지 않고 있다. 가이드라인을 요청하는 전화회사들을 위하여 연방통신위원회(FCC)는 1998년 2월 '승인' 요구를 해설하는 명령을 내리게 되었다. 연방통신위원회의 규칙하에 통신회사들은 고객들에게 통화패턴의 사용을 통제할 회사

의 권리에 대한 명백한 고지(explicit notice)를 주어야 하고, 그 사용을 위하여 명확한 서면, 구두, 또는 전자적 승인을 획득하여야 한다.

18. 건강보험책임법(Health Insurance Portability and Accountability Act, 1996)

연방의회는 건강보험책임법을 제정함으로써 전자적 형태의 건강정보에 대한 프라이버시를 관할하기 위한 연방정책을 처음으로 보장하게 되었다. 이 법은 건강정보의 전자적 교류를 위한 표준의 발전 및 채택을 강제하는 '행정간소화'(Administrative Simplication)라는 장을 포함한다. 또한 이 법은 연방의회나 보건및인류서비스부(Secretary of Health and Human Services)가 그러한 전자적 교류를 통제할 프라이버시 규칙을 개발하도록 요구한다. 그러나 이 규칙은 전자시스템이 가동하기 이전에 적용될 수는 없다. 건강정보의 전자적 교류를 위한 표준의 신속한 개발 및 채택을 강제하는 이 법의 규정들은 환자의 프라이버시를 보호하는 강한 법률이 없으면 집행하기가 곤란하다. 따라서 이 법은 연방의회나 행정분과(Executive Branch)가 1999년 8월 21일 이전에 프라이버시 규칙을 제정하도록 요구하였다. 1999년 10월 연방의회가 자체 부여한 최종시한을 넘기면서, 미국 클린턴 행정부는 의료정보를 보호하기 위한 최초의 연방프라이버시 규칙을 제안하였다. 클린턴-고어의 제안발의(Clinton-Gore initiative)로 알려진 이 제안은 회사들이 의료 데이터나 고객소비습성에 관한 상세한 정보를 공유하기 전에 고객의 동의를 요구하는 것을 그 목적으로 한다. 또한 이 제안은 회사들이 사용자와의 데이터 거래 이전에 그들의 프라이버시 정책을 공개하도록 요구한다.[81] 이 제안은 다음 몇 가지 사항을 강제한다.

첫째, 환자들은 어떻게 정보가 사용, 보관 및 공개되는지에 관하여 명백한 서면 설명을 받아야 한다.

둘째, 환자들은 그들의 기록에 대한 사본의 획득과 수정을 요구할 수 있어야 한다.

셋째, 환자들은 정보가 공개되기 전에 그 권한을 주어야 하며 공개에 관한 제한을 요구할 수 있어야 한다.

넷째, 정보제공자와 건강계획은 치료가 행하여지기 이전에 환자로부터 포괄적인 승인(blanket approval)을 요구할 수 없다.

---

81) Grant Du Bois, "Privacy Standards Grant Patients' Rights"(2001. 1. 18), <http://www.eweek.com/article2/0,3959,114476,00.asp>.

다섯째, 건강정보는 몇 가지 예외를 제외하고는 건강의 목적 자체로만 활용될 수 있다.

여섯째, 정보제공자와 건강계획은 반드시 서면 프라이버시 절차를 채택하고, 고용인을 훈련하며, 프라이버시 관리인을 지정하여야 한다.

이와 함께 건강보험책임법은 중소기업과 대기업에 대하여는 2002년 10월까지, 소기업은 2003년 10월까지 이 법을 준수할 것을 강제하였다.

19. 아동온라인프라이버시보호법(Child Online Privacy Protection Act, 1998)

아동온라인프라이버시보호법[82]은 13세 이하의 어린이들에 대한 정보의 온라인 수집을 금지한다. 어린이들을 주 대상으로 하는 이 법은 어린이들로부터의 정보수집을 인식하는 상업적 웹사이트들의 운영자들은 데이터 수집정책을 고지하고, 어린이들로부터의 정보수집 이전에 부모의 동의를 구하도록 요구한다.[83] 이 법은 연방거래위원회(Federal Trade Commission)에게 부모에 대한 고지와 동의의 형태 및 실체적 내용에 대한 대부분의 핵심이슈들을 위임한다.

이 법의 적용을 받는 웹사이트는 13세 이하의 아동과 직접적으로 관련된 서비스를 제공하는 상업적 웹사이트 운영자 뿐만 아니라 모든 일반인을 대상으로 서비스를 제공하더라도 13세 미만의 아동으로부터 개인정보를 수집하는 모든 웹사이트이다.

이 법의 적용을 받는 웹사이트는 반드시 홈페이지에 프라이버시 정책을 고지하고 개인정보를 수집하는 페이지에 프라이버시 정책이 링크되도록 하여야 한다. 또한 접근권을 보장하여 부모에게 아동의 개인정보가 제3자에게 제공되도록 허락할 것인지 여부를 선택하거나 개인정보를 삭제할 기회를 보장하여야 한다. 또한 인터넷 웹사이트 운영자는 인터넷 게임이나 설문조사 등 기타 활동에 아동이 참여할 때 그러한 활동에 참여하는데 합리적으로 필요한 수준 이상으로 더 많은 개인정보를 제공하여서는 안되며, 아동으로부터 수집한 개인정보의 비밀성, 안전성, 무결성을 유지하기 위한 노력을 기울여야 한다.[84]

---

82) Pub. L. No. 105-277, 112 Stat. 2681 (15 U.S.C. 6501로 성문화).

83) *Id.*

84) FTC, “Children's Privacy: The Children's Online Privacy Act”, <http://www.ftc.gov>.

20. 금융현대화법(Gramm-Leach-Bliley Act, 1999)

금융현대화법은 금융기관이 보유하는 고객의 금융정보를 보호하기 위하여 제정된 법이다. 이 법은 은행, 증권사, 보험사와 같은 금융기관 및 대부업과 같은 대출서비스 기관, 중개업, 자금전송 또는 보관업, 금융자문이나 신용컨설팅회사, 채권추심업 등과 같은 금융상품 또는 서비스를 제공하는 모든 회사에 적용된다. 이 법은 금융 프라이버시에 관한 원칙, 세이프가드 원칙, 프리텍스팅(pretexting)과 같은 세 가지 주요한 내용을 담고 있다.

금융 프라이버시 원칙이란 금융기관에 의한 고객의 개인금융정보의 수집 및 이용을 규제하는 것으로, 금융기관으로부터 금융정보를 제공받는 기업에도 제공되므로 해당 기관이 금융기관인지의 여부에 관계하지 않는다. 따라서 금융기관은 소비자에게 회사의 개인금융정보에 대한 정책을 고지하여야 하고, 소비자 개인정보를 이해관계가 없는 제3자에게 제공하혀 정보를 공유하기 전에 반드시 소비자에게 이 사실을 알리고 반대할 권리를 부여하여야 한다.

세이프가드 원칙은 모든 금융기관이 소비자의 정보를 보호하기 위한 안전장치를 고안하고 시행하며 유지할 것을 요구하는 것이다. 이 원칙은 소비자로부터 직접 정보를 수집하는 금융기관 뿐 아니라 다른 금융기관으로부터 고객정보를 받는 신용평가회사 등의 금융기관에도 적용된다.

프리텍스팅 규정은 소비자를 기만하여 개인의 금융정보를 취득하는 개인 또는 기업으로부터 소비자를 보호하는 규정이다.

21. 대테러감시법(Patriot Act, 2001)

미국 대테러감시법은 9/11 테러사건의 결과로 나온 법에 대한 첫 번째의 직접적 변화이다. 대테러감시법은 342페이지 분량으로 무려 15개의 서로 다른 법령을 개정한다. 주요 내용으로는 전자감시, 수색영장, 조사단 기금, 돈세탁, 금융기록, 기금압류, 화폐위조, 국경보호, 이민신분 및 구금, 이민자를 위한 혜택, 정보에 대한 보상권, 테러의 희생자를 위한 지원, 정부기관간 정보공유, 테러에 대한 형벌규정 강화, 그리고 정보의 개선 등이다. 법집행기관에게 더 강력한 권한을 부여하는 대부분의 조항은 2005년 12월 31일까지 유효할 것이다.[85]

---

85) Department of Justice, The US Patriot Act of 2001(2001),

22. 전자정부법(E-government Act, 2002)

미국 전자정부법은 국민 중심의 전자정부를 통합적으로 추진하고, 행정기관간의 협력 및 민간부문과 정부사이의 협력을 증진하여 국민의 권익을 보다 충실하게 보장하고자 제정되었다. 이 법은 관리예산처(OMB)내에 전자정부국을 두어 연방정부의 리더쉽을 효과적으로 발휘하여 전자정부 서비스 및 그 업무의 개발을 촉진할 수 있도록 한다.

전자정부법은 정보시스템 뿐만 아니라 정보도 함께 보호하는 규정을 두고 있다. 특히 개인정보의 보호와 관련하여서는 정보기술 도입 전에 프라이버시 영향평가를 실시하도록 하고 있다.

V. 최근 미국연방의회의 프라이버시 보호 관련 입법안 및 주요내용

1. 인터넷스파이웨어방지법안(Internet Spyware(I-SPY) Prevention Act of 2004, H.R. 4661)

이 법안은 미국법전(United States Code)의 제18장(title 18)을 스파이웨어를 경감하는 근거규정을 두도록 수정하기 위한 목적으로 2004년 10월 8일 연방상원에 제출된 상태이다. 이 법안은 연방형법전(Federal criminal code)이 허가 없이 보호대상의 컴퓨터에 고의적으로 접근하거나 허가된 접근범위를 초과하여 컴퓨터 프로그램이나 코드를 해당컴퓨터에 복제하는 것을 금지하도록 수정한다. 처벌의 대상이 되는 사항은 또 다른 연방범죄에 해당하는 컴퓨터 프로그램이나 코드를 고의적으로 사용하는 것, 보호대상인 컴퓨터에 손상을 주거나 개인을 속이거나 상해를 입히기 위한 목적으로 개인정보를 획득 도는 전송하는 것, 해당컴퓨터의 보안장치를 손상하는 것 등을 들 수 있다.

이 법안은 이 법안을 위반하는 피고가 주법하에 민사소송을 제기할 수 없음을 명시하여 연방법의 우월적 지위를 명시하고 있다.[86]

<www.ins.usdoj.gov/graphics/lawsregs/patriot.pdf>.

86) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR04661:@@@L&summ2=m&>.

2. 프라이버시침해에대한세이프가드법안(Safeguard Against Privacy Invasions Act of 2004, H.R. 2929)

이 법안은 스파이웨어 프로그램을 통하여 개인적으로 식별가능한 정보를 몰래 전송하는 것으로부터 인터넷 사용자들을 보호하기 위한 목적으로 2004년 10월 6일 미국연방상원에 제출된 상태이다. 이 법안이 연방하원을 통과할 당시 개명된 법안의 명칭은 "사이버불법침해에대한안전보호법안"(Securely Protect Yourself Against Cyber Trespass Act)으로 일명 "스파이법안"(SPY Act)으로도 불린다.

이 법안에 의하면 금융기관에서의 사용을 위한 컴퓨터, 미국정부의 사용을 위한 컴퓨터, 주간 또는 국제통상이나 통신에 사용되는 컴퓨터 등 보호되는 컴퓨터의 소유자 또는 공인된 사용자가 아닌 자가 행하게 되면 불법인 행위들을 열거하고 있다. 이러한 행위에는 다른 사람들에게 원치 않는 자료(unsolicited material)를 보내서 해당컴퓨터를 통제하는 행위, 허가 없이 인터넷 브라우저를 전환시키는 행위들과, 개인적으로 식별가능한 정보를 수집하는 행위 및 사용자에게 소프트웨어 구성요소를 해당컴퓨터상에 설치할 것을 권유하는 행위 등을 포함한다.

이 법안에서의 프라이버시 침해에 대한 구성요건을 만족하기 위하여는 사실상 인지(actual knowledge) 또는 객관적 상황에 근거하여 명백히 내재된 지식(knowledge fairly implied on the basis of objective circumstances)으로 침해에 가담하였을 것을 요구한다.[87]

3. 사회보장보호법(Social Security Protection Act of 2004)

이 법안은 사회보장법(Social Security Act)과 내국세법(Internal Revenue Code of 1986)이 사회보장 및 추가적인 보호세 수혜자들에게 부가적인 안전장치를 줄 수 있도록 수정하기 위한 목적으로 입안되어 2004년 3월 2일 법으로 통과되었다.[88]

이 법의 제II장 프로그램 보호(Title II: Program Protections)의 제201조(Sec. 201)는 사회보장법 제XI장(Title XI)에 대하여 사회보장국이 사회보장금 수혜자의 적격성이나 수혜금의 변동에 대한 상황을 고지하여야 하는 공무원이 알면서 또는 알아야만 하는

87) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR02929:@@@L&summ2=m&>.

88) Public Law No: 108-203.

상태에서 그 고지에 실패한 자에 대한 민사적 처벌규정을 부과하도록 수정한다.[89]

4. ID도용피해자구제법(Identify Theft Victims Assistance Act of 2003, S. 1581)

이 법안은 ID 도용을 방지하기 위한 목적으로 ID 도용으로 피해를 받은 개인들의 해를 경감하고자 입안되었다. 이 법안은 연방형법전이 사업체에게 ID 도용과 관련된 모든 가입원서 및 사업체정보에 관한 복사본을 피해자, 모든 연방, 주 및 지방정부 법집행관 또는 피해자에 의하여 적시된 공무원, 또는 ID 도용을 조사하는 모든 법집행관이나 피해자에게 그 기록을 받는 것을 허가받은 법집행관에게 무료로 해당 거래기록을 공급하도록 수정한다.

이 법안은 피해자가 다른 방법으로는 피해자의 신원을 확인할 수 없는 사업체에게 피해자의 ID에 대한 구체적 증거를 제시하고 ID 도용청구가 가능하게 할 것을 요구한다. 법안은 또한 연방 법무부장관 및 주 법무부장관들이 이 법에 대한 민사소송을 제기하는 것을 인정한다. 이 법의 위반은 연방거래위원회(FTC)에 의한 강제집행이 가능한 불공정 또는 사기적 행위나 수행에 해당하는 것으로 간주한다.

이 법안은 소비자평가원이 ID 도용으로부터 초래된 해당인의 파일에 소비자에 의하여 식별되는 정보의 보고를 차단할 것을 요구하고, 만일 차단이 거절 또는 취소되는 경우 해당소비자에게 고지할 수 있도록 공정신용평가법(Fair Credit Reporting Act)을 수정한다.[90]

5. 공정하고정확한신용거래법(Fair and Accurate Credit Transactions Act of 2003, H.R. 2622)

이 법은 ID 도용을 방지하고, 소비자 분쟁해결과 소비자 기록의 정확성을 향상하는 등 신용정보에 대한 소비자의 정급을 개선하기 위하여 공정신용평가법(Fair Credit Reporting Act)을 수정하기 위한 목적으로 입안되어 2003년 12월 4일 법으로 통과되었다.[91]

---

89) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR00743:@@@L&summ2=m&>.

90) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:SN01581:@@@L&summ2=m&>.

91) Public Law No: 108-159.

이 법은 ID 도용방지 및 신용기록 회복, 신용정보의 사용 및 소비자 접근의 개선, 소비자 기록정보의 정확성 강화, 금융시스템에서의 의료정보의 사용 및 공유 제한, 금융교양 및 교육개선, 고용인에 대한 비행조사로부터의 보호 등을 규정하기 위하여 제정되었다. 이 법은 ID 도용자(Identity Theft)란 ID를 도용하였다는 주장이 제기되는 자로써, 미국우편조사국 및 모든 법집행관을 포함하여 적절한 연방, 주 또는 지방정부에 소비자에 의하여 신고된 자라고 정의한다.[92]

6. 사회보장번호프라이버시및ID도용방지법안(Social Security Number Privacy and Identity Theft Prevention Act of 2003, H.R. 2971)

이 법안은 사회보장번호의 프라이버시 보호를 강화하고, 사회보장번호의 사기적 오용을 방지하며, ID 도용에 대한 보호를 강화하기 위한 목적으로 사회보장법(Social Security Act)을 수정하기 위하여 입안되어 2004년 11월 19일을 한도로 연방하원에서 검토중인 법안이다. 이 법안은 사회보장법 제II장(title II)의 노년, 상속인 및 장애보험에 관한 장에서 연방, 주, 그리고 지방정부와 파산사건 관재인(bankruptcy case trustees)에 의한 사회보장번호의 일반대중에 대한 판매 또는 공개에 관한 제한을 명시하도록 요구한다. 이 법은 주나 지방정부에 의하여 발행된 자동차 운전면허증이나 차량등록증상에 사회보장번호를 공개하는 것을 금지한다. 또한 이 법안하에서는 연방, 주, 그리고 지방정부가 고용인의 신분증이나 전자태그상에 사회보장번호를 공개하도록 하는 것을 금지한다.

이 법에서 소비자의 사회보장번호는 공정신용평가법(Fair Credit Reporting Act)에서의 정보에 해당하며, 개인의 사회보장번호를 공개하는 것에 동의하지 않았음을 이유로 그 개인에 대한 거래를 거부한 모든 사람은 연방거래위원회법(FTC Act)에 위반하는 불공정 또는 사기적인 행위에 가담한 것으로 고려하게 된다.[93]

7. 의료정보프라이버시침해금지법안(Stop Taking Our Health Privacy Act of 2003, H.R. 1709)

이 법안은 2002년 8월 약화되었던 개인적으로 식별가능한 의료정보에 대한 프라이

92) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR02622:@@@L&summ2=m&>.

93) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR02622:@@@L&summ2=m&>.

버시를 보호하기 위한 기준을 복원하기 위한 의도로 제시되었다. 이 법안은 치료, 지불, 도는 의료보장시설의 운영을 위한 사용 또는 공개에 대한 동의와 관련한 연방규제법전(CFR: Code of Federal Regulations)의 조항에서의 의료 프라이버시에 영향을 미쳤던 2002년 8월 14일의 수정을 무효로 하도록 한다. 따라서 이 법안은 연방규제법전의 조항은 의료공급자가 구체적 상황하에서의 사전동의 없이 개인의 보호되는 건강정보의 사용 또는 공개를 허용하는 것으로 해석한다.[94]

8. 소비자프라이버시보호법안(Consumer Privacy Protection Act, H.R. 1636)

이 법안은 소비자 프라이버시를 보호 및 강화하기 위한 것이다. 이 법안은 데이터 수집기관이 일정한 상황하에 소비자에 대하여 (1) 수집당시에 그들의 개인식별가능정보가 관련없는 거래의 목적을 위하여 사용되어질 수 있음과, (2) 그 기관의 프라이버시 정책문구의 중대한 변화에 대하여 즉각 고지할 것을 요구한다. 이 법안은 데이터 수집 기관들에게 수집, 판매, 대가의 공개 또는 소비자 정보의 사용에 관한 프라이버시 정책을 수립하도록 요구한다. 소비자들은 해당 데이터수집기관의 정보공유파트너가 아닌 기관에게 그들의 정보를 판매 또는 공개하는 것을 배제할 기회를 소비자들에게 무료로 제공할 것을 요구할 수 있다.[95]

9. 프라이버시법안(Privacy Act of 2003, S. 745)

이 법안은 개인의 개별적 식별 가능 정보에 대한 판매 또는 마케팅 이전에 개인의 동의를 획득할 것을 요구할 목적으로 2003년 3월 31일 상원에 제출된 상태이다. 이 법안은 상업체가 사전에 기술된 절차나 그러한 공개가 있을 수 있다는 것을 고지 않은 상태로 개인적으로 식별가능한 정보를 제휴되지 않은 제3자에게 판매 및 공개를 금지한다. 이 법안은 연방거래위원회(FTC)에게 강제집행권을 부여한다. 이 법안은 또한 개인에게 확실히 명백한 동의가 없이 사회보장번호를 공개, 판매, 도는 구매하는 것을 금지하도록 연방형법을 수정한다.

이 법안은 비공공개인금융정보에 대한 금융산업 판매 및 공유에 대한 제한을 두도

94) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR01709:@@@L&summ2=m&>.

95) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR01636:@@@L&summ2=m&>.

록 수정하며, 특정 사업체에 의한 보호되는 건강정보의 판매 또는 마케팅에 대한 금지행위를 설정하고 있다.[96]

10. 전화송신차단법(Do-Not-Call Implementation Act)

이 법은 연방거래위원회(FTC)가 "전화송신차단"의 명부를 집행하기 위한 비용을 수집하도록 허가하기 위한 목적으로 2003년 3월 11일 법으로 통과되었다.[97] 이 법은 전화소비자사기및남용방지법에 공포된 '텔레마케팅판매규칙'(Telemarketing Sales Rule)의 전화송신차단 명부(do-not-call registry)와 관련한 규정을 이행하고 강제하기 충분한 비용을 충당할 규칙들을 연방거래위원회가 공포할 것을 인정한다. 비용으로 수집된 금액은 텔레마케팅규칙 및 그 행위에 부수하는 이행 및 강제에 드는 비용을 충당하기 위하여만 사용가능하다.[98]

11. 프라이버시방어법안(Defense of Privacy Act, H.R. 338)

이 법안은 연방기관이 규칙을 공포할 때 개인의 프라이버시에 관한 규칙들의 영향을 고려할 것을 요구하도록 미국연방법전(United States Code) 제5장(title 5)를 수정할 목적으로 2004년 7월 7일 제시되어 일부 수정된 상태이다. 이 법안은 내국세법과 관련한 해석용 규칙을 위한 제안된 규칙제정의 고지 또는 어떠한 제안된 규칙을 위한 제안된 규칙제정의 일반적 고지를 출간할 때, 그리고 그러한 규칙이나 제안된 규칙제정이 10인 이상으로부터 개인적으로 식별가능한 정보를 수집, 유지, 사용, 또는 공개에 해당할 때, 개인의 프라이버시에 대한 그 규칙의 영향평가를 공표하도록 한다.[99]

12. 사회보장번호오용방지법안(Social Security Number Misuse Prevention Act, S 228)

이 법안은 미국연방법전(United States Code)의 제18장(title 18)이 사회보장번호의 오용을 제한하고 그러한 오용에 대한 형사적 처벌근거를 두도록 수정하기 위하여

96) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:SN00745:@@@L&summ2=m&>.

97) Public Law No: 108-10.

98) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR00395:@@@L&summ2=m&>.

99) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR00338:@@@L&summ2=m&>.

2003년 1월 29일 연방상원에 제출된 상태이다. 이 법안은 특정한 상황을 제외하고는 개인에 대한 확실히 명백한 동의 없이 사회보장번호를 공개, 판매, 또는 구매하는 것을 금지하도록 연방형법전(Federal criminal code)를 수정한다. 이 법안은 법무부장관에게 모든 연방법하에서 허용, 요구, 공인, 또는 제외되는 사회보장번호의 모든 사용에 대하여 의회에 연구보고할 것을 지시한다.

이 법안은 사회보장법(SSA: Social Security Act)의 제II장(title II)를 수정하는데, 그 내용은 정부기관에 지불하기 위한 개인수표상에 사회보장번호의 사용과 운전면허증이나 자동차등록증상에 사회보장번호의 명시를 금지하는 것 등이다.[100]

13. ID도용방지법안(Identity Theft Prevention Act, S. 223)

이 법안은 ID 도용을 방지하기 위하여 2003년 1월 28일 상원에 제출된 법안이다. 임대진실법(Truth in Lending Act)가 신용카드 발급자가 주소의 변경을 확인하여야 하는 절차적 가이드라인을 규정하도록 수정한다. 이 법안은 연방거래위원회(FTC)와 특정한 상황하에서의 지정된 연방기관에게 집행권을 부여한다.

이 법안은 공정신용평가법(Fair Credit Reporting Act)가 절차적 가이드라인을 제시하도록 요구하는데, 소비자평가원은 소비자 파일에 있는 주소의 불일치를 요구자에게 고지하여야 하며, 요구하는 소비자의 파일내에 사기경보를 포함하여야 한다. 이 법안은 거래를 위하여 신용카드를 받는 사업체가 신용카드 끝번호 다섯자리 이상을 출력하는 것을 금지하도록 강제한다.[101]

14. 데이터채굴금지법안(Data-Mining Moratorium Act of 2003, S. 188)

이 법안은 미국 국방부(Department of Defense)의 총체적 정보 경계 프로그램(Total Information Awareness Program)하에 데이터채굴의 이행에 관한 일시적 정지를 부과하는 내용으로 2003년 1월 16일 상원위원회에 이송되었다.

이 법안은 국방부(DOD: Department of Defense) 또는 국가방위부(DHS: Department of Homeland Security)의 공무원이나 고용인이 국방부의 총체적 정보경계프로그램이나 어떠한 다른 데이터채굴 프로그램이나 이 프로그램과 유사 또는 관련한 국가방위

100) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:SN00228:@@@L&summ2=m&>.

101) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:SN00223:@@@L&summ2=m&>.

부의 데이터채굴 프로그램을 수행하지 못하도록 금지하고 있다. 이 법안은 이 법의 제정일로부터 연방부서에 의한 데이터채굴이 특별히 인정되는 법의 제정일까지 그러한 금지가 효력이 있도록 하고 있다.[102]

VI. 결론

미국은 프라이버시를 헌법적인 권리로 인정하고 있지만, 유럽국가들과는 달리 포괄적이고 기본법적인 개인정보 관련 법체계를 가지고 있지 않다. 그러나 기본법이 부재한 상황에서도 사회적 변화나 기술의 발달에 맞춰 공공·통신·온라인 등 각 영역별로 개인정보와 관련한 개별법적인 접근을 취하여 대응하고 있다. 이는 미국의 개인정보보호를 위한 접근방식이 경제적·기술적 관점을 중시하고, 특히 민간부문에서의 사적 자치의 원칙을 중시하여 정부의 간섭을 최소화하는 자유로운 시장경제의 질서를 유지하기 위함이다.

우리나라의 경우 정부에서는 공공부문의 개인정보보호를 위하여 '공공기관의개인정보보호에관한법률'을 제정·시행하고 있고, 민간부문의 개인정보 보호를 위해 '정보통신망이용촉진및개인정보보호등에관한법률'을 구비하고 있으며, '민간부문의개인정보보호에관한법률(안)'을 입법예고 하는 등 개인정보를 보호하고 온라인 상거래의 신뢰기반을 구축하기 위하여 관련 법제도를 꾸준히 구축하여 오고 있다. 이러한 법률안의 개인정보보호의 수준은 가히 국제적인 표준에 손색이 없을 것이라 하겠지만, 현행 법제도의 적용대상이 정보통신 서비스 사업자와 일부 오프라인 사업자에 국한되어 있어 광범위한 영역에서 발생하고 있는 개인정보 침해에 효율적으로 대응하기 위한 법제도적인 기반의 정비와 추진체계의 마련이 시급하다는 지적도 나오고 있다. 이러한 요청에 따라 현재 여러 영역에서 개별법적인 접근방식으로 운영되고 있는 개인정보보호 관련법을 대신하여 개인정보보호에 관한 일반법을 제정하려는 움직임도 나타나고 있다.[103]

그러나 이러한 개인정보 및 프라이버시 침해 형태 및 기존 법률과의 조화 문제 등

---

102) <http://thomas.loc.gov/cgi-bin/bdquery/z?d108:SN00188:@@@L&summ2=m&>.

103) 2004년 2월 이은영의원이 대표발의한 '개인정보보호기본법안'과 정성호의원이 대표발의한 '개인정보보호법안'은 동년 4월에 철회되었으며, 현재 2005년 7월 11일 이은영의원 대표발의를 통한 '개인정보보호법(안)'과 동년 10월 17일 이혜훈의원 대표발의를 통한 '개인정보보호법(안)'의 두 개의 법률안으로 상정되어 현재 국회에 계류 중에 있다.

다양한 법률에 산재한 개인정보보호 관련 규정을 일정하게 통합하여 일반적인 개인정보보호 법률을 제정하여야 한다는 의견은 일간 설득력이 있는 주장일 수도 있으나, '다양성'을 그 기본특성으로 하는 개인정보 및 프라이버시를 일괄타결방식의 기본법 내에 모두 담을 수 있는지는 신중한 검토를 필요로 할 것이다. 즉, 미국의 경우와 같이 그 나라의 사회적·문화적 특수성을 반영한 개인정보보호의 입법방식을 채택하는 것이 프라이버시 보호관련 국제적인 기준에 반드시 미달하는 것은 아니라는 것을 재고하여야 할 것이다.

한편, 미국의 프라이버시 보호를 위한 규제방식은 정부의 입법, 집행, 평가에 기반을 두고 있지만, 이러한 기능들이 민간부문에 의하여 수행되는 '자율규제'적 접근방식을 채택하고 있다. 미국은 민간부문에서 특별히 규제할 필요성이 인정되는 경우에만 법률을 제정할 뿐, 원칙적으로 업계가 자율적으로 개인정보보호를 위한 제도를 마련하도록 유도하는 것만 정부의 몫으로 남겨두고 있다. 이러한 자율규제적 접근방식은 개인정보를 인권으로 보아 국가가 적극 관여하여 보호해야 한다고 보는 유럽과는 다른 시각이다. 그러나 미국의 자율규제를 위한 노력은 다소 실망스러운 결과를 안겨주고 있다. 자율규제의 맹점은 적정성(adequacy)과 집행성(enforcement)에 있어서 문제를 가지고 있다는 점이다. 현재 미국, 일본, 싱가폴과 같은 나라에서의 산업체에 의한 자율규제는 프라이버시 보호에 대한 보호 및 그 강제에 있어서의 정도가 미약할 따름이기 때문이다.

미국이 유럽과 같은 수준의 지침이나 일반법을 가지고 있지 않음에도 불구하고 세이프 하버 원칙을 통하여 지속적으로 유럽으로부터의 데이터를 전송받을 수 있다. 이는 미국이 유럽연합과 그 회원국에 대하여 미국 시스템이 적절한 프라이버시 보호를 갖추고 있다는 점을 설득하기 위한 강력한 로비로 이루어졌다는 사실에 주목할 필요가 있다. 세이프 하버 원칙은 개인정보 취급의 적정성 여부를 판단하기 위한 특정한 목적만 가질뿐, 국제조약으로써의 성격을 가지지도 않는다. 그럼에도 불구하고 이 원칙을 따르게 되는 경우 유럽위원회로부터 개인정보보호의 적정성을 인정받게 되는 결과가 되기 때문에, EU 회원국과 별도의 협의와 논의를 진행할 필요가 없이 그 적정성이 추정되게 된다.

우리나라의 프라이버시권의 근거가 되는 것은 헌법 제17조의 사생활의 비밀과 자유, 제10조의 인간의 존엄성 존중 조항, 제12조의 신체의 자유, 제16조의 주거의 자유, 제18조의 통신의 자유, 제21조제4항의 타인의 명예나 권리침해 방지, 제36조제1항의 혼인과 가족생활에 있어서의 개인의 존엄과 평등 조항 등을 들 수 있고, 제37조

제1항의 헌법에 열거되지 아니한 자유와 권리의 존중 조항도 프라이버시권의 헌법상 근거가 될 수 있다. 이러한 헌법에 근거하여 프라이버시권이 구체화되는 개인정보 자기결정권[104]과 관련한 국내법은 미국의 경우와 같이 일반법의 형태를 취하고 있지 않다. 다만, 정보통신망이용촉진및정보보호등에관한법률, 신용정보의이용및보호에관한법률, 금융실명거래및비밀보장에관한법률 등이 민간부문에서의 개인정보를 보호하고 있고, 공공기관의개인정보보호에관한법률이 공공부문의 개인정보를 보호하며, 기타 전자정부법, 주민등록법, 국세기본법, 통신비밀법, 보건의료기본법, 범죄신고자보호법, 그리고 형법 등 개별 분야별로 업무상 비밀 보호 및 정보보호 규정이 산재하여 있는 상황이다. 이와 같이 우리나라의 경우 공공부문에 있어서는 개인정보 보호에 관한 일반법으로 '공공기관의개인정보보호에관한법률'이 있고, 민간부문에 있어서는 '정보통신망이용촉진및정보보호등에관한법률'이 일반법으로써의 역할을 하고 있다. 그러나, 최근 개인정보보호에 대한 관심이 높아지면서 현행 입법의 미비점을 보완하려는 측면으로 입법이 보완되거나[105], 개정을 진행 중에 있다.

개인정보보호의 문제가 선진국 주도의 새로운 무역장벽으로 대두되고 있는 현 시점에, 국제적 표준에 맞는 개인정보보호 기준을 마련하고, 이에 대한 국제협력을 강화하여야 할 필요성이 대두되고 있다. 특히 EU에서는 한국을 개인정보보호 기준을 충족하지 못하고 있는 요주의 국가로 분류하고 있기 때문에, 그 형식이 일반법의 형식이던지 개별법의 형식이던지에 불문하고 국내 개인정보보호 수준을 국제적 기준에 맞는 법제도로 정비하고, 개인정보의 국외이전에 대한 가이드라인을 시급히 마련하여야 할 것이다. 효율적인 법체계로 어떠한 방식이 맞는지나 추진주체가 누가 되어야 하는지에 대한 반복적이고 소모적인 논쟁의 피해자는 결국 우리 자신이 될 것이라는 사실을 직시하여야 한다고 본다. 더욱이 각종 국제기구에서 개최하는 국제적 논의에 적극적으로 참가함은 물론, 우리나라의 개인정보보호 법제의 특수성 및 수준에 대한

104) 개인정보 자기결정권에 대하여는 이를 헌법 제10조에 의해 보호되고 있는 인격권의 내용을 이룰 뿐만 아니라 프라이버시로서 헌법 제17조에 의해 보호된다고 보는 견해와 이를 헌법 제21조의 표현의 자유에서 찾은 견해 등으로 나누어지고 있다; 정준현, "민간 온라인 개인정보보호법제에 대한 검토", 공법연구 제29집 제3호, 2002, 150면 이하 참조.

105) '신용정보의이용및보호에관한법률'(이하 신용정보법)이 2004년 1월 개정되었는데, 신용정보 수집·조사업무의 효율성을 높이기 위하여 신용정보업자 또는 신용정보집중기관이 공공기관에 대하여 신용정보의 열람 또는 제공을 요청한 경우 공공기관이 이에 응하도록 하고, 신용정보의 오용·남용을 막고 정보보호를 강화하기 위하여 신용정보주체에게 신용정보업자 등으로부터 신용정보의 제공사실을 통보받을 수 있는 권리를 부여하는 등 현행제도의 운영상 나타난 일부 미비점을 개선·보완하여 개인정보보호를 강화하는 내용으로 개정되었다.

홍보노력이 지속적으로 병행하여야 할 것이다.

미국의 개인정보보호 관련 이슈에 대한 개별법적인 접근과 영역별 개인정보 관련 법률현황 및 주요 판례들은 정보화시대에 부수한 기술의 발전에 따라 CCTV 감시, 개인정보 프로파일링, 아이디 도용, 온라인 프라이버시, RFID 프라이버시, 유전자복제 등 생명공학과 관련한 프라이버시, 생체정보와 관련한 프라이버시 보호 등과 같은 새로운 이슈에 신속하게 응답할 수 있다. 미국에서 특정이슈에 대한 프라이버시법의 적용은 그 침해의 내용에 의존한다. 이러한 의존성은 미국 프라이버시법이 특정형태의 프라이버시 문제를 해결하거나, 또는 프라이버시의 침해에 대하여 반응하거나, 아니면 개인정보의 특정형태를 보호하는 특징 등을 가지면서 발전하여 왔기 때문이다. 특히 미국 프라이버시법은 개인의 프라이버시 이해에 대한 새로운 도전들, 특히 신기술에 의하여 생성된 도전들에 응답하면서 발전하여 왔기 때문에 새로운 이슈들에 대한 반응이 신속할 수 있는 것이다.

전통적으로 프라이버시나 개인정보보호에 대한 관념이 다소 새로운 개념으로 탄생하게 된 우리나라의 경우 개인정보보호 관련 일반법의 논의 뿐만 아니라, 개별법적인 접근방식을 병행하여 나가는 방식도 신정보사회에 대응하여 고려하여야 할 필수적 요소라 할 것이다.

조규범

프라이버시(Privacy), 개인정보(Personal Information), 세이프하버원칙(Safe Harbor Principle), 자율규제(Self-regulation), 시장위주정책(Market-dominted Policy), 권리위주정책(Rights-dominated Policy), CCTV 감시(CCTV surveillance), 개인정보프로파일링(Personal Information Profiling), ID 도용(ID Theft), 온라인프라이버시(Online Privacy), 생체프라이버시(Biometric Privacy)

[abstract]

Statutory Development of Privacy in the United States

Cho, Kyu-beom*

The concept of privacy in the United States have been developing by legal cases and scholars since the late nineteenth century. By the case of Griswold v. Connecticut in 1965, it had become clear that privacy was a common law tort right and the intrusion of privacy was admitted to be liable to damages in the United States' legal system. Although the United States' Constitution does not specifically mention privacy and have a comprehensive law related to privacy, it has a number of specific provisions that protect privacy, and it has been interpreted as providing a constituional right to privacy.

The United States regard a market-dominated policy as important for the protection of privacy and only accords limited statutory and common law rights to privacy. This approach is conspicuous phenomenon in the private sector because it is for the purpose of free marketplace which would minimize intrusions from the government.

The way of regulation for the protection of privacy is divided into two; legal enforcement and self-regulation. Self-regulation is base on traditional elements of government such as legislation, enforcement, and evaluation, this approach, however, is not by the government but the private sector. Self-regulation approach is differ from European norms which reflect a rights-dominated apporoach and require to have comprehensive statutory protections for citizens.

The development of technology incidental to the information age

* Senior Researcher, National Assembly Library.

raises more legal issues than before, such as CCTV surveillance, personal information profiling, ID theft, online privacy, RFID privacy, and biometric rrivacy, etc. The study on self-regulation approach, legal cases related to current privacy issues and statutory development for each issue in the Uniteds States would be very important because it might give some models to deal with current private issues in Korea.

This thesis comprehesively explores federal statutes in each sectors which cope with legal issues of privacy protection. Part II introduces the concept and background of privacy in the United States to provide the definition and priciples of privacy. Part III and IV examines contitutional protection of privacy and federal legislations related to privacy as well as safe harbor principle. Part V ultimately concludes that Korea should consider both individual statutory approaches and a comprehensive approach making a general privacy law to deal with privacy issues in new information society.