가상공간에 있어서의 프라이버시 권리*

류 시 조**

Ⅰ. 머리말

가상공간(Cyberspace)은 "추상적 데이터로 이루어진 환상적 공간으로서 매일매일 수억의 사람들을 합의된 환각에 빠지게 하는 컴퓨터 통신 네트워크"상의 공간을 말한다.[1] 가상공간은 전자과학기술의 발전에 따른 새로운 공간을 뜻한다. 가상공간은 아직 우리에게는 비교적 새로운 미지의 영역이고, 이에 대한 문제의 제기도 아직 미흡한 상태라고 할 수 있다. 이는 모든 학문의 관심과 연구의 대상이기도 하며, 법학의 경우에 있어서도 어느 특정한 법영역의 문제만이 아님은 물론이다. 특히 가상공간을 중심으로 한 헌법학상의 문제점은 물리적 공간인 실제공간(Real Space)상의 헌법적 관점을 비물리적 공간인 가상공간에 그대로 적용할 수 있는가 하는 점이다. 즉 3차원적 공간인 물리적 공간에

* 본 연구는 1997년도 한국학술진흥재단 인문·사회과학분야 중점영역연구비지원에 의한 것임.

** 부산외국어대학교 법학부 교수

1) Cyberspace라는 용어는 William Gibson의 소설 "Neuromancer(Ace Books,N.Y.:1984)"에서 「인간의 정신,데이터 무리와 배열이 전기선로를 통하여 이동하는 교감적 환상」이란 의미로 처음 사용되었으며(in:Neuromancer, p.51), 오늘날에는 'Net', 'Web', 'Matrix' 등으로 알려져 있기도 하나 'Internet'으로 구체화되고 있다.

있어서 제기된 국민주권주의·권력분립주의·의회주의·법치주의·민주주의·자유와 권리 등의 문제도 무차원적 공간인 가상공간이란 영역에서는 새로운 논의를 예정하고 있다 하겠다.

특히 가상공간에 있어서 개인의 프라이버시에 관한 문제는 전자거래·신용내용·금융거래실적, 교육·의료·자격 등에 관계된 각종의 개인정보가 단순히 데이터로 기록·보존·관리되는 것에 그치는 것이 아니라 데이터베이스화하고 네트워크화되어 각종 자료가 상호유기적으로 결합·가공·처리되고, 공간적 시간적 제한을 받지 않고 유통되고 있다. 이와 같이 정보화가 진행되면 될수록 개인에 관한 사적 정보 뿐만 아니라 공적 정보가 확대 재생산되면서 동시에 보호되어야할 개인정보 및 사생활의 영역은 점점 확대되고 있다. 그리고 컴퓨터와 디지털통신기술은 한편으로는 경제적 사회적 변화에 부응하여 개인의 자유를 신장시키기도 하지만 다른 한편으로는 부적절한 보안체계를 가진 시스템으로 인해 비밀기록과 데이터가 해킹 당하는 등 개인 사생활에 심각한 도전으로 간주되기도 한다. 이렇게 정보는 개인·기업·국가 등에 의하여 무수한 유저들과 서버들에 의하여 여러 단계를 거쳐 네트워킹되고, 인테엑팅되는 과정 중에서 국내적으로 또는 국제적으로 각 단계마다 본래의 목적과는 무관하게 다른 의도로 악용되고, 침해될 소지를 안고 있다. 특히 오늘날 온라인 공간에서 프라이버시침해의 잠재적 가능성은 그 이전에는 생각할 수도 없는 것들이라 할 수 있다. 이러한 현상들에 대한 현행의 법제도는 과연 개인의 프라이버시에 충분한 보호를 주고 있는가의 문제를 안고 있다. 그리고 가상공간에 관한 법적 문제는 기존의 법체계로는 해결할 수 없는 새로운 법적 문제를 함축하고 있어 이에 대한 새로운 헌법적 논의를 예정하고 있다 할 수 있다. 여기서는 가상공간에 있어서 프라이버시보호문제와 관련한 논의가 아직 우리 나라에서는 본격적으로 제기된 바가 없어 최근의 미국의 사례를 중심으로 하여 제기되는 몇 가지 논쟁을 살펴보면서, 가상공간상의 프라이버시권의

문제 상황을 살펴보고자 한다.

Ⅱ. 가상공간에 있어서 행위와 프라이버시 침해의 특수성

1. 가상공간의 범주와 행위

가상공간은 "기계라기보다는 에코시스템으로서 전화선·동축케이블·광섬유선이나 전자기파가 있는 곳이면 어디에나 존재할 수 있는 보편적인 생체전자적 환경(bioelectronic environment)을 뜻하고 이 곳은 전자적 형태로 존재하는 지식으로 채워져 있어 사람들이 무엇이 안에 있는 가를 보고 지식을 채워넣고 지식을 바꾸며 또한 지식을 꺼내게 하는 문에 의하여 물적 환경으로 연결된다. 이 문들의 일부는 일방향이거나 쌍방향이며 사이버스페이스에서의 지식은 점점 더 1과 0이라는 디지털 형태로 데이터·지식·정보를 담는 디스크·테잎·CD롬과 같은 물리적 형태의 사이버스페이스적 저장수단(warehouses)에 기록되면서 정확한 종류의 문과 열쇠를 가지고 있는 사람만이 이것에 접근가능하다. 열쇠는 사이버스페이스를 항해하도록 하고, 그 내용을 문자·영상·음성의 형태로 인간의 감각으로 이해가능케 하는 전자적 지식의 특수한 형태의 소프트웨어이다."[2] 그리고 이러한 전자공간의 개념은 더 빠른 컴퓨터와 더 값싼 전자적 저장수단들에 의하여 소프트웨어와 케이블 통신 채널들이 개선되면서 우리는 더욱 빠른 속도로 사이버스페스적 환경을 창조·정의·확장하면서 이 각 각의 요소들이 독자적으로 가상공간으로 불리어지기도 하고, 또 이제까지 우리가 알지 못하는 방식으로 작동하

2) E.Dyson · G.Gilder · J.Keyworth and A.Toffler, Cyberspace and the American Dream:A Magna Carta for the Knowledge Age, August 22, 1994 (http://www.pff.org/position.html).

는 이 모두의 결합으로 가상공간은 폭발적으로 확장되는 것이다. 이렇게 가상공간이란 개념은 통신개념만을 의미하는 전자통신(Electronic Telecommunication)과는 다른 새로운 모습의 생체전자적 환경을 일컫는 것이다. 그러나 가상공간이 기본적으로는 전자통신을 매개로 하는 경우가 많다는 점에서 전자통신과 개념적으로 혼란을 일으키기도 한다. 이 점이 다음에 보는 가상공간법제의 특수성을
부인하는 주장을 뒷받침하는 유력한 근거가 되기도 한다.

오늘날 가상공간이라 일컫는 경우에 주로 상업적 온라인서비스·전자게시판(BBS)·개인컴퓨터시스템·네트워크와 같은 유형의 범주를 통하여 경험할 수 있으며, 이들은 각각 서로 다른 기능과 특성을 가진다고 할 수 있다. 가상공간에서의 유저의 행위유형은 목적과 기능에 따라 다르겠으나 대개는 전자우편(E-Mail)·공개메시지시스템(Public Messaging systems)·전자출판·채팅,교육·연구조사·상업적 활용 등의 형태로 나타난다.[3] 이 중에서 온라인상의 활동 중에 전자우편이 가장 일반적이라 할 수 있다. 전자우편시스템은 전통적인 우편제도와 같이 발신자와 수신자는 각자의 이름과 주소를 가지며, 메시지를 작성하여 발송하면 모두 자동으로 우편함에 저장되며, 많은 유저들에게 동시에 대량으로 우송할 수 있는 전통적 우편보다 훨씬 편리한 기술이다. 온라인서비스나 BBS에서는 시스템계정을 가진 유저들만이 메일링할 수 있게 제한되기도 하나 그 시스템이 네트워크이거나 네트워크로 제어되면 교신할 수 있는 상대방은 엄청나게 증가한다. E-mail이 사적 교신이라면 공개메시지시스템은 메시지베이스로 우송된 메시지를 공적으로 접근할 수 있고, 대중은 그 메시지를 읽고 응답할 수 있는 공적 기능을 가진 시스템이다. 이러한 시스템들이 다른 시스템과 네트워크되어 뉴스그룹이라는 대량의 메시지를 전송함으로 각지에 퍼져있는 유저들을 결합하기도 한다. 또한 전자출판시스템의 출현은 디지털정보로 작성된 신문이나 잡지

3) E.A.Cavazos/G.Morin, Cyberspace and the Law, 1996, p.2 f.

를 정기적으로 구독자의 전자우편함에 메일로 보냄으로써 실시간으로 간행물의 구독과 출판이 가능해 졌으며, 레크레이션활동이 가상공간에 넘쳐 나고 있고, 가정에서도 세계각지의 사람들과 대화하며 게임을 즐길 수 있다. 그리고 가상공간에 있어서 통신의 가장 직접적인 형식이 채팅이라는 유저들 간의 실시간 대화이며, 많은 전자게시판이 서로 신분과 얼굴도 모르는 유저들간의 채팅에 이용되기도 한다. 가상공간은 다양한 데이터베이스의 구축으로 인하여 교육이나 연구목적으로 시스템을 이용하는 것이 가능해 졌을 뿐만 아니라 인증제도의 확립으로 인하여 상거래 뿐만 아니라 기타 법률적 행위도 가능케 하고 있다. 물론 가상공간에서의 유저와 정보제공업자 및 망사업자의 행위에도 일정한 한계와 책임이 있기 마련이다.[4]

2. 가상공간상의 프라이버시침해의 용의성

가상공간에서는 종래의 실제공간에서 형성되었던 기존의 관념들, 즉 재산의 본질과 재산권개념이 변질되고, 시장·자유·공동체 등의 본질과 정부의 역할이 변질되며, 익명성으로 인하여 사이버인격도 실재인격과 유리되기 쉬워 유저들은 자제력을 상실하거나 책임있는 행위로부터 일탈되기 쉬운 사이버인격을 일상화·사회화한다. 더욱이 새로운 의학적 연구와 의료보장·전자통신·개량된 운송시스템 및 금융거래 등의 발전으로 개인에 대한 정보는 비약적으로 증가하고 있고, 이러한 것들은 고속통신망과 결합하고 각 컴퓨터로 링크됨으로써 광범위하게 개인정보를 더욱 확대·재생산케 하였다. 따라서 보호되어야할 프라이버시도 더욱 확대되어 새로운 법적 과제를 양산하게 됨과 동시에 정보보안

4) Vint Cerf, Guidelines for Conduct On and Use Of Internet (http://www.isoc.org/internet /conduct/cerf-Aug-draft.shtml). 여기서 유저·정보제공업체 및 네트워크사업자의 행위에 대한 가이드 라인을 제시하고 있다.

산업기술의 발달도 비약적으로 개선되고 있다. 물론 가상공간에 있어서의 활동과 인터넷사용의 가이드라인으로 프라이버시보호가 강조되고 있음에도 불구하고 아이덴티티카드나 유전자데이터베이스·새로운 감시시스템 등을 포함해서 새로운 기술의 진보로 인해 개인의 프라이버시 침해는 더욱 더 심화되어 가고 있으며, 나아가 이러한 신기술이 개인에 대한 적절한 보호를 주지 못하는 개발도상국가에서는 그 침해 정도가 심화되어 가고 있는 실정이다. 따라서 개인의 프라이버시침해에 대한 두려움은 역사상 어느 시대보다도 더 커가고 있다. 이러한 인식으로 인해 세계 각국은 포괄적인 프라이버시 및 정보보호법을 제정·시행하는 경향이 증가하고 있다. 그러나 프라이버시의 침해는 민주국가에 있어서조차 경찰이나 국가감독기관 등의 보안기관을 중심으로 주로 정치 노동 사상 인종 등을 이유로 이루어 지며, 기업은 법의 미명 아래 개인정보를 수집·유포하기도 한다. 개인신용정보에 관한 법을 오랫동안 시행해 온 미국에서조차도 기업들이 영업목적으로 개인정보를 악용하기도 한다.

특히 정보의 사회적 영향력의 확대와 함께 정보기술의 용량과 속도가 급속히 빨라짐에 따라 프라이버시의 침해의 범위와 정도·침해의 잠재성은 그 침해적 환경으로 인하여 점점 증가되어 간다. 즉, 그로벌 테그놀로지의 가장 대표적인 예인 인터넷의 발전으로 인한 정보 그로벌라이제이션은 정보흐름의 지역적 한계를 초월하게 되었다. 그리고 기술에 대한 편의성의 요청은 시스템간의 기술적 장벽을 무너뜨려 다른 시스템간의 호환성을 증대하고 다양한 형태로 정보의 상호교환과 처리를 가능케 하였으며, 멀티미디어는 수많은 형태의 데이터와 이미지의 전송 및 표현을 융합하여 어떤 형식으로 수집된 정보가 다른 형식의 정보로 용의하게 변형되기도 한다. 오늘날 ID카드의 제도화·통신감청, 인터넷이나 전자메일의 도청,국가보안시스템·전자광학적 감시 등에 의하여 개인의 프라이버시는 항상 침해의 위험성에 노출되어 있다. 따라

서 이와 같은 상황에 대응하기 위한 논의는 헌법학의 주요과제 중의 하나이다.

Ⅲ. 가상공간에 있어서 프라이버시의 보호입법

1. 프라이버시보호법제의 동향

프라이버시권은 1890년 처음으로 그 개념이 형성된 이후 헌법상 주거의 자유나 통신의 자유의 확대해석을 통하여 헌법상의 기본적 권리로 인정되기 시작한 이래 국제조약과 협약에 의하여 기본적 인권으로 인정되기에 이르러, 오늘날 헌법상의 기본권의 하나로서 프라이버시권을 성문화를 하고 있는 나라가 늘어가고 있음은 주지의 사실이다.[5] 특히 프라이버시의 권리에 대한 관심은 '60년대와 '70년대에 디지털 정보기술의 출현으로 증가되기 시작하여 강력한 전신·전자시스템에 의한 감시가능성으로 인하여 개인정보의 수집과 취급을 하는데 필요한 특별한 규범이 요청되게 되면서부터 였다. 그러나 이러한 영역의 현대적 입법은 1970년 독일 헤센주에서 시행된 최초의 데이터보호법이라 할 수 있다. 이어서 스웨덴(1973), 미국(1974), 독일(1977), 프랑스(1978)가 그 뒤를 이었다. 이러한 일련의 각국의 입법과정을 이어서 '80년 유럽위원회 각료회의와 유엔 경제협력개발기구에 의한 두개의 국제적 프라이버시보호규범의 제정으로 승화되었으며,[6] 이 두 규범은 뒤이은 각국의

5) 프라이버시권에 대한 헌법례를 보면 몇몇 불문헌법국가를 포함해서 프라이버시가 헌법상 명시적으로 규정되지 않은 나라에서는 프라이버시권을 주거의 불가침이나 통신의 자유의 내포로서 보나(미국·아일랜드·인도·영국·싱가포르·말레이시아·스위스 등), 대부분의 성문국가에서는 자기정보접근권과 자기정보통제권을 명시적으로 규정하는 국가가 많아지고 있다(남아공·헝가리·네델란드·폴란드·포르투칼·러시아·스페인·터어키 등).

데이터보호입법에 깊은 영향을 주었다. 1970년대가 개별국가의 개인 프라이버시보호를 위한 기본적 골격을 짜기 위한 광범위한 입법운동이었다면, 1980년대는 국제적 프라이버시보호입법의 기준모델을 제시하고자 한 노력의 시기였다고 할 수 있다. 그리고 1990년대에 들어와서는 UN이 새로운 데이터보호입법의 기준을 제시하고,[7] 1995년에는 유럽연합 각료회의가 개인데이타통신의 보호기준에 관한 권고안을 채택하고[8] 이어 1997년에는 입법의 불충분과 각국의 보호수준의 차이를 의식해서 유럽연합이 전유럽에 걸쳐 적용될 시민의 개인정보의 남용에 대한 광범위한 보호를 제공하는 규약을 통과시켰는데, 이 규정은 회원국에 대하여 유럽시민에 관한 개인정보가 역외국가에 수출되거나 소유될 경우 이 법의 적용을 받을 것을 명하고 있다.[9] 이 규정으로 인해 역외국가

---

6) Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data(1981.1.18.서명), OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data(1980.9.23.채택).여기서 OECD는 다음과 같은 8가지의 프라이버시에 관한 가이드라인을 제시하였다. 1.Openness. 2.Data quality principle. 3.Purpose specification. 4.Use limitation principle. 5.Security safeguards principle. 6.Openness principle. 7.Individual participation principle. 8.Accountability principle.

7) United Nations Guidelines Concerning Computerized Personal Data Files(1990.12.14. 채택)는 컴퓨터 개인데이터파일에 관한 규정을 충족하는 절차는 각국의 주권에 유보하면서 다음과 같은 최소보장기준을 제시하였다.

1. Principle of LAawfulness & Fairness 2. Principle of Accuracy 3. Principle of the Purpose-Specification 4. Principle of Interested-Person Access 5. Principle of Non-Discrimination 6. Power to Make Exceptions 7. Principle of Security 8. Supervision and Sanctions 9. Transborder Data Flows 10. Field of Application.

8) 유럽위원회각료회의 "Protection of personal Data in the Area of Telecommunication Services, with Particular reference to Telephone Service"(1995.2.7.채택)에 관한 권고에는 다음과 같은 기준을 제시하고 있다. 1. Scope and definitions 2. Respect for privacy 3. Collection and processing of data 4. Communication of data 5. Rights of access and rectification 6. Security 7. Implementation of principles.

9) 정식 이름이 「전기통신 데이타보호에 관한 유럽규약(European Directive on

들에 대하여 프라이버시보호법의 통과를 강제하는 압력으로 작용하여 40여개국 이상이 정보보호법이나 정보프라이버시법을 보유하게 되었거나 보다 많은 나라들이 입법과정에 있다.[10] 이러한 입법은 각국마다 차이가 있으나 대체로 과거 권위주의정부 밑에서 프라이버시침해의 구제를 위해서이거나 전자상거래를 촉진시키기 위해서 또는 범유럽적 수준의 보호를 요구하는 EU법의 영향을 받아 포괄적인 프라이버시 및 정보보호법을 채택하고 있다.[11] 그러나 이러한 각국의 입법은 개인의

Dataprotection in Telecommunications)」인 이 규정은 개별국가적 보호수준을 정하고, 각 EU회원국은 1998년 8월까지 보충적 입법을 통과시킬 것을 규정하고 있다.

10) Report of An international survey of privacy laws and practice by Privacy International (http://www.gilc.org/privacy/survey/);최근 유럽연합(EU)이 1998년 10월 25일부터 사생활보호를 위한 명령을 발하여 유럽 내에서 영업 중인 기업이 고객으로부터 얻은 각종신상정보를 판매할 수 없도록 금지하고, 동시에 유럽과 상응한 사생활 보호조치를 보장하지 않는 국가의 기업에게 자료를 넘기지 못하도록 규정하여 유럽연합 15개 회원국 중 6개국에서 이미 법으로 제정되었거나 입법과정에 있다. 이 명령은 EU회원국이 그 동안 사생활보호에 중점을 두고 개인신상정보관리를 강화해 온 것과는 달리 미국은 업계의 고객신상정보거래에 대하여 자율규제를 허용하는 자유방임적 정책을 취하는 등 고객의 신상정보관리에 큰 시각차를 드러내어 미국과 EU간의 전자상거래가 중단 위기에 처해 있다(한국일보,1998.10.27.자). 우리 나라도 이러한 입법경향에 따라 한국공법학회의 노력으로 1994년 개인정보보호법인 「공공기관의 개인정보보호에 관한 법률」을 제정하였다.

11) Report of An international survey of privacy laws practice(article) by Privacy International 최근 ;유럽연합(EU)이 1998년 10월 25일부터 사생활보호를 위한 명령을 발해 유럽 내에서 영업 중인 기업이 고객으로부터 얻은 각종신상정보를 판매할 수 없도록 금지하고, 동시에 유럽과 상응한 사생활 보호조치를 보장하지 않는 국가의 기업에게 자료를 넘기지 못하도록 규정하여 유럽연합 15개 회원국 중 6개국에서 이미 법으로 제정되거나 입법과정에 있다. 이 명령은 EU회원국이 그 동안 사생활보호에 중점을 두고 개인신상정보관리를 강화해 온 것과는 달리 미국은 업계의 고객신상정보거래에 대해 자율규제를 허용하는 자유방임적 정책을 취하는 등 고객의 신상정보관리에 큰 시각차를 드러내어 미국과 EU간의 전자상거래가 중단 위기에 처해 있다(한국일보,1998.10.27.자).

프라이버시보호에 관한 전반적인 사항을 다룰려고 하고 있기 때문에 가상공간에 있어서의 문제를 직접 커버하지 못하고 있다는 우려를 자아내고 있다. 우리 나라의 경우에는 개인정보보호에 관해 개별적으로 각 법률에 산재되어 규정되어 있으나 개인 프라이버시보호에 관한 포괄적 보호규정을 담고 있지 못하고, 이 규정들은 프라이버시보호를 위해 그렇게 체계적이지도 못하는 대증요법적인 규정으로 가상공간에서 제기되는 프라이버시의 보호수준을 충족하기에는 역부족이라 할 수 있다.[12]

2. 가상공간에 있어서 프라이버시보호법제

1) 가상공간상의 프라이버시이보호법제의 성격

정보화사회를 촉진시키는 정보화 기술은 실로 복잡다기하며 이에 관한 법적 대응도 바빠지고 있다. 그 중에서도 네트워크를 중심으로 한 가상공간을 전자통신과 구별되는 특수성을 인정 할 수 있는가에 따라 가상공간법의 법제적 독자성에 대한 견해를 크게 두 가지로 나눌 수 있다. 하나는 가상공간도 인간의 실제공간의 연장에 불과하므로 이에 관한 제 법리적인 문제도 일반 법리적인 문제이므로 프라이버시문제도 기존의 법이론적으로도 접근·해결 가능한 것으로 보고, 다만 특수한 문제에는 개별법적으로, 또는 예외 입법론적으로 해결하면 충분하다는 가상공간법의 특수성부인론의 입장이 그 것이다. 따라서 가상공간법제의 독자성을 인정하지 않거나 인정할 필요를 느끼지 않으며, 이에 관한 법규정은 일반 프라이버시권의 법리로도 충분히 포섭할 수 있다는 생각

12) 우리 나라의 프라이버시보호규정은 형법·전상망보급확장과 이용촉진에 관한 법률·전기통신사업법·신용정보의 이용 및 보호에 관한 법률·무역업무자동화촉진에 관한 법률·화물유통촉진법·공공기관의 개인정보보호에 관한 법률·통신비밀보호법 등에 산재되어 있다.

이 그것이다. 그리고 다른 하나는 가상공간 그 자체가 산업사회적 이데올로기에 바탕을 두고 있는 종래의 시민법적 영역과는 전혀 성질을 달리하는 정보화사회에 대응하는 새로운 패러다임의 법영역으로 보아 가상공간법의 특수성긍정론의 입장이 그것이라 할 수 있다. 특히 인터넷은 어떠한 특정국가에 의해서 규제되거나 검열될 수 없는 세계광역통신망으로서 몇몇 나라가 구축하려고 하는 규제와 검열에 의해 치명적인 영향을 받는 매우 복잡하고 광대(廣大)한 통신망이다. 따라서 다른 형태의 통신을 위해 제정된 법은 인터넷에 그대로 적용하는 것은 적절하지 않으며, 새로운 사이버패러다임을 반영하는 법제의 특수성을 긍정하려는 입장이 그것이다.

그러나 아직 가상공간법의 성격에 관한 논의는 우리 나라의 경우에 그렇게 본격적으로 제기되었다고 볼 수 없다.[13] 가상공간이라는 기술적·기능적·환경적 특수성으로 인하여 가상공간상의 프라이버시문제를 일반적 프라이버시보호법적 패러다임으로 수렴하는 데는 일정한 한계가 있고, 일반적 프라이버시보호에 관한 논의와 문제를 가상공간에 있어서도 원칙적으로 원용할 수 있는 것이라고 하더라도 가상공간에서의 프라이버시의 문제는 가상공간이란 비교적 특수한 제한된 영역에서의 문제를 다룬다는 점에서 새로이 조망해 볼 필요성이 있다 하겠다. 앞에서 살펴 본 바와 같이 비교적 생소한 영역인 가상공간에 관하여 그 개별적 특수성을 인정하지 않으려 하거나, 기존의 프라이버시법제의 적용영역의 확장문제 만으로 인식하려는 태도는 재고하여야 할 것이다. 일반적으로 개인정보의 보호와 관리를 목적으로 하는 정태적인 정보보호법이나 데이터관리법과 동태적인 가상공간상의 행동규범 정립을 목적으로 하는 가상공간법과는 구별되어야 할 것으로 생각한다.

---

13) 최근 제72회 공법학회 학술발표회(1997.11.), 정보사회에 대비한 일반법 연구(Ⅰ)(1977. 통신개발연구원) 등에서 정보화사회에 있어서 법적 과제와 대응을 중심으로 한 문제 제기가 잇따르고 있다.

2) 미국의 전자통신프라이버시보호법

미국의 1986년「전자통신프라이버시보호법」(The Electronic Communications Privacy Act: ECPA)은 전자통신을 통한 컴퓨터사용자의 증가 및 기타 통신기술의 혁신으로 인한 법적 프라이버시를 보호하고자 채택되었다. 이미 1986년 ECPA시행 이전에 1968년 「종합범죄단속 및 도로안전에 관한 법」(The Omnibus Crime Control and Safe Street Act: OCSA)이 있었으나 이 법은 기본적으로 전화도청방지법이었으며, 또한 제3장(TitleⅢ)에 전자감시에 관한 규정을 두었으나 전자메일과 같은 새로운 디지털 통신기술이 확산되고 전자감시기술의 혁신으로 인하여 이전의 헌법적 보호나 법률적 보호를 능가하는 도청이 국가나 개인에 의하여 광범위하게 이루어 지게 되면서 프라이버시의 권리를 심각하게 위협하게 되었다. 따라서 ECPA는 1968년의 OCSA 제3장을 개정하여, 전자감시를 포함한 프라이버시침해를 명확히 규정하고 무선호출기·전자메일·셀룰러폰·개인통신수단·컴퓨터전송을 추가하여 법적용의 범위를 확대함으로써 프라이버시보호를 강화하였다. 오늘날 ECPA는 개인적 통신을 엿듣거나 폭로하는 것을 불법화하고 동시에 이러한 행위에 대하여 제소할 수 있는 권리를 규정하고 있다. 이 법은 또한 고용주가 피고용인의 전자메일을 감독하는 등과 같은 종래 보호를 받지 못한 특수한 상황과 전송형식을 인정하였다. 이상과 같이 미국의 경우에도 기존의 전자통신을 중심으로 하여 프라이버시 보호범주를 강화한 것이지만, 그래도 비교적으로 미국에 있어서 ECPA는 가상공간에 있어서 프라이버시를 다루는 가장 중요한 법령의 하나로 인식되고 있다.

이 법 중 제3장은 종래의 기존의 통신수단에 의한 프라이버시의 보호를 새로운 통신기술의 등장으로 인한 영역으로까지 보호를 주고자 한다. 여기는 오늘날 현대적 전자통신수단에 관한 것을 망라하여 프라이버시를 보호하고자 한다. 이 법은 아직 가상공간법의 독자성이 확고하게 인식되지 못하고 있는 상황에서 전자통신법제에 최신의 통신수단

이나 기술적 환경에 맞추는 수준에 머물고 있으나 가상공간적 문제의식을 어느 정도 담고 있다는 점에서 오늘날의 가상공간법의 대표적 예라고 할 수 있다. 여기서 제3장을 중심으로한 주요내용을 살펴보면 다음과 같다.

첫째, ECPA 제3장은 프라이버시보호를 전자우편(Electronic Mail)에 의한 디지털 정보의 전송과 저장에 까지 확장하고, 음성통신 데이터나 디지털부분과 같이 유선통신의 비음성부분을 도청하는 것이 불법임을 명확히 함으로써 도청(intercept)의 의미를 명확히 하였다.[14] 여기 비음성부분은 전자통신을 포함하고, 유선·무선·전자기·광전자·사진광학 시스템에 의하여 전부 혹은 일부로 전송된 어떠한 성질의 기호·신호·문서·영상·음성·데이터의 이동도 전자통신으로 규정하였다. 또한 저장된 전자우편·음성메일 및 원거리 컴퓨터서비스의 콘텐츠를 보호하도록 하면서 동시에 전자통신의 사업자가 통신을 한 자의 적법한 동의 없이 전자적으로 저장되는 통신콘텐츠를 폐쇄하는 것을 금지하고 있다. 둘째, 이 법은 일반 공중이 이용하는 일상통신(common carrier)설비의 감시를 위하여 프라이버시보호를 제한되었다. 보호를 개인전화시스템·전화교환사업자 및 근거리지역통신망을 포함하는 모든 통신장비의 이용에까지 확대한다.[15] 셋째, 통신이 두 개의 셀룰러폰간에 혹은 셀룰러폰과 유선전화간에 이루어지는지를 불문하며, 교환국에서 유선·케이블 혹은 기타 라인의 연결을 활용하는 통신을 포함하도록 유선통신규정을 개정하였다.[16] 하지만 도청방지와 암호문과 같은 보호기술 수단의 이

14) Interception은 ECPA에 있어서 가장 중요한 개념으로서 "일체의 전자적 기계적 혹은 다른 장치를 사용하여 일체의 유선·전자·음성에 의한 통신의 내용을 청각 혹은 기타의 방법으로 획득"하는 것을 의미한다.

15) 하원사법위원회(The House Judiciary Committee)는 州間 혹은 해외영업에 영향을 미치는 어떠한 설비라도 이를 공급하고 운용하는 사람을 망라하여 규율함으로써 최대한 헌법적 제한이 허용 가능한 데까지 연방관할권을 확대하고자 하였다.

16) 1973 미국순회항소원은 통신의 일부가 유선전화(landline telephone)로 운송될

용을 장려하기 위하여 비암호문·도청방지가 안된 셀룰러폰 호출의 도청에 관한 처벌을 경감시킴으로써 암호문통신을 장려하였다. 이 법은 무선전화상의 대화 중의 유선부분을 위한 보호를 규정하였다. 그러나 특별히 제3장에서 보호되는 유선통신은 무선전화휴대장치와 본체간의 전송되는 전화의 무선부분은 포함하지 않는다. 넷째, 이 법은 무선호출기사용에 관한 프라이버시보호를 명확히 하였다. 법무성은 음성 및 디지털 호출기를 제3장의 보호를 가정하는 원래의 유선통신의 연장으로 규정하였다. 특히 신호전용(tone-only)호출기를 이용하는 경우는 제3장의 보호를 받지 못한다고 규정하였다. 다섯째, 이 법은 정부가 전자서비스사업자에게 속한 등록자와 고객기록에 접근하는 것을 제한하였다. 정부기관은 먼저 등록자나 고객에게 알리지 않고 서비스공급자의 기록에 접근하기 위해서는 먼저 수색영장·법원명령 혹은 정당한 권한을 가진 행정부나 대배심의 영장을 얻어야 한다. 여섯째, 이 법은 1984년 케이블통신정책법(the Cable Communications Policy Act)을 비암호화케이블프로그램의 가정수신을 규율하는 배타적 보호정책의 근거로서 인정된다. 1984년의 법은 프라이버시문제보다는 상사회사의 행위에 관한 케이블위성수신문제를 규정하기 위하여 별개의 일련 특화된 정책을 세웠다. 동시에 위성송신도달을 방해하는 악의적 고의적 간섭에 관한 형사처벌을 강화하였다.

때 이동전화상의 대화는 제3장의 보호를 받는다고 결정하였다(Hall vs. U.S., a 1973). 하지만 이 결정은 셀룰러폰과 무선전화의 대화에 제3장의 보호가 적용되는지를 명확히 하는데 실패하였다.

Ⅳ. 가상공간에 있어서 프라이버시보호를 위한 대응과 갈등

1. 익명성(Anonymity) 문제

ID(Identification)에 관한 논의는 크게 두 가지 방향에서 논의되고 있다. 하나는 국가의 행정전산망구축과 관련한 개인의 ID카드(Identification Card)의 문제와 다른 하나는 네트워크상의 ID의 문제이다. ID카드는 실공간에서의 개인정보기록을 저장한 것으로서 그 목적에 따라 유형·기능·보전 등에 있어서 여러 가지 형식을 가지고 있다. 일찍이 인종·정치·종교가 ID로 기능하여 정치적·종교적 목적으로 개인에 관한 정보를 강제적으로 등록하게 하여 차별을 가하였던 것이 아이디시스템을 확립하는 가장 일반적인 동기였다. 오늘날에는 磁氣帶(magnetic stripe)와 마이크로프로세서 기술의 출현으로 이러한 카드는 국가서비스 수령권과 신원증명을 결합하는 등 국가행정의 기초인 국가등록시스템(국가행정전산망)과 링크되고 있고, 이러한 시스템으로 인하여 헌법상 프라이버시권은 여느 때와 달리 훨씬 심각한 위협을 받고 있다.[17]

그러나 가상공간에서 ID에 관한 논의는 현실의 개인정보를 기록한 ID카드문제와는 그 성격을 전혀 달리한다. 즉 국가정보전산화의 일환으로 제기되는 ID문제는 실공간에서의 개인의 신분의 진정을 밝히기 위한 것이라면, 가상공간에서는 실제적인 신분증명으로 기능하지 않고 가상공간으로 들어가기 위한 문과 열쇠의 하나로서 기능한다는 점이다. 그리고 가상공간에서 일어나는 많은 행위가 가명이나 별명(handles)으로 이루어지는 ID를 사용하는 것이 일반적이다. 가명사용으로 인해 보다

17) 1991년 헝가리헌법법원은 다목적 개인 신분증명번호를 만들 수 있는 법률이 헌법상의 프라이버시권을 침해한다는 결정을 내렸으며, 1998년 필리핀최고재판소는 국가아디시스템은 헌법상의 프라이버시권을 침해한다는 결정을 내렸다. 현재 우리 나라에서도 전자주민카드도입 문제를 두고 개인의 프라이버시침해의 문제로서 많은 논란을 불러일으킨 바 있다.

편안함을 느끼는 전자게시판이나 네트워크 참여자들에게는 통신상의 권리로 간주되며, 온라인문화에 익숙지 못한 사람들에게는 현실적 책임으로 부터 도피를 의미하는 것으로 인식되어 위협적인 것으로 생각되기도 한다. 그리고 실제로 시스템이나 네트워크상의 가상공간에 있어서의 별명을 사용하는 것은 전혀 위법한 것이 아니며, 어떤 별명을 사용하든 합법적이다.[18] 네트워크상의 유저들이 익명사용을 고집하는 하나의 이유는 메시지에 대한 책임으로부터 벗어나 현실공간으로부터의 해방감을 만끽하고자 하는 표현의 자유에 대한 욕구 때문이다. 이와 같이 유저들은 가상공간에 있어서 익명성을 통하여 실재의 자기(ego)와 다른, 새로운 제2의 자아(alter ego), 즉 사이버인격(cyberego)을 경험한다고 할 수 있다. 그리고 이를 가능케 하는 프로그램이 추적불가능한 신분확인정보없이 메일을 받고 보내는 익명의 리메일러시스템이기도 하다.[19] 그러나 보통 계정설정을 필요로 하는 시스템은 사용협약에 따라 시샵이 확인할 수 있는 비전자수단에 의하여 신상자료의 진정을 요구하는 경우가 있으며, 그리고 시스템사용협약에 따라 신상정보의 보안이

18) 이른바 책과 논문에서 사용되는 필명(penname)은 작가의 표현의 자유를 보장하는 중요한 수단적 권리의 하나이다. 가상공간에서 유저의 익명성의 보장은 통신의 자유를 보장하는 중요한 권리로 인식되고 있으며, 또한 현실의 자아와 달리 가상공간에서 창조되는 제2의 자아, 즉 사비버에고의 보장을 뜻한다.

19) FTP(File transfer protocol)이라는 파일전송규약은 인터넷상의 파일을 고속으로 다른 검퓨터로 전송하는 기술로서 많은 사이트(sites)는 유저들이 익명으로 로그인하고 파일을 전송하는 익명의 FTP능력을 가지고 있다. 많은 익명의 FTP 사이트는 시스템이용자의 메일주소를 포함한 시스템활동을 감시하고 기록되나 대개 이러한 서비스는 신용이 불안정하여 주의를 기울여야한다. 어떤 시스템은 메일 수신자가 발신자에게 응답하는 임의의 신분확인 코드를 할당한다. 이리하여 리메일러는 수신자가 발신자의 신분을 알 수 없도록 하는 필터사용을 익명의 서버(anonymous server)라 한다. 인터넷에는 공적 목적을 위해 이용할 수 있는 서버와 리메일러가 있기도 하고, 가끔 시스템관리자나 운영자 모르게 이용되기도 하지만 불안정하다. 그러나 리메일러서버와 익명의 서버는 감시될 수 있고 서비스를 운영하는 개인이 시스템기록을 보존하기 때문에 절대적으로 익명성은 보장되지 않는다.

유지되기도 하나 이러한 신상정보요구로 인해 사실상 가상공간에서의 익명사용이 매우 위축받기도 한다.[20] 인터넷에 접속된 시스템은 단순한 키보드동작 만으로도 다른 인터넷유저에 대한 계정정보를 디스플레이 할 수 있고, 또한 시스템은 공적 목적을 위하여 시스템 이용자의 상세한 개인정보를 담은 유저기록을 만들기도 한다. 그리고 자기의 개인정보의 공개를 원하지 않는 경우에는 시스템관리자에게 그 사실을 통지함으로써 보호를 받는 경우도 있다. 미국 최고재판소는 인쇄물을 작성 출판 배포하는 사람들의 이름과 주소를 명확히 밝힐 것을 명하는 명령을 무효화함으로써 익명에 의한 표현의 자유를 보장하고 있다.[21] 따라서 가상공간에 있어서 여러 가지 형식에 의한 유저들의 익명사용권(Rights of Anonymity)은 헌법상의 표현행위의 하나로서 보장받고 있음과 동시에 유저의 프라이버시보호을 위한 강력한 수단이 되기도 한다. 가상공간에서 프라이버시의 문제는 개인의 인격권보호의 문제이기도 하다는 점에서 표현의 자유와 동전의 양면과 같은 성격을 가지고 있다.

그리고 가상공간에서 유저들은 네트워킹을 통하여 그들만의 공통적인 연대감을 가지고 각종 동호회와 대화방, 특정 사이트에 접속 등의 형태로 사이버공동체를 형성하기도 한다. 이러한 사이버공동체에서 유

---

20) 우리 나라의 경우에 최근 가상공간에 있어서 익명성을 악용한 사례가 빈발함에 따라 온라인서비스실명제를 실시하기로 하고, 온라인서비스사업자는 한국정보통신진흥협회에서 운영하는 신용정보관리시스템을 이용해 신상자료의 진정을 확인하여 허위기재사실이 있을 경우 가입을 불허하고, 기가입자는 실명으로 전환하도록 하며 가입자가 이에 응하지 않을 경우 가입해제 등의 강제조치를 취하도록 하고 있다(동아일보, 1998.12.7.).

21) NAACP v. Alabama, 357,U.S..449(1958); Talley v. California, 362U.S.60(1960).; 이 판례에서 어떤 장소나 어떤 상황 아래에서도 작성·배포·후원한 사람의 이름과 주소를 인쇄하지 않은 전단의 배포를 금하는 로스안젤레스시의 명령을 언론·출판의 자유를 보장한 수정헌법 제1조의 위반이라고 하여 무효화하였다. 여기는 가공인물에 의한 출판도 인정하여 疑似匿名權(correlative rights to anonymity)을 보장한다고 확인하였다.

저들은 인터액션을 하는 과정에서 사이버에고를 획득하면서 온라인상 공유하는 연대의식은 물리적 공간에 있어서의 실제적 결합을 통해 누리게 되는 결사체의식과 유사한 것이기도 하다. 그러면 가상공간에서 유저들은 결사권과 같은 집단적 권리를 가지는가가 문제이다. 가상공간에 있어서 메일리스트와 전자게시판의 등록명단은 실제공간에 있어서의 결사체의 조직회원명단에 해당한다고 볼 수 있다. 일정한 조건하에서 시샵은 유저의 기록에 담긴 정보에 관해 정부의 접근을 봉쇄할 수 있다. 이는 정부로 하여금 타인과 결사하는 시민의 권리를 박탈을 금하는 수정헌법 제1조의 표현 및 결사의 자유의 결과이다. 결사의 자유는 민주주의의의 기능을 보장하는데 중요한 조직 및 집단의 프라이버시를 보장한다. 이에 관하여 미국의 연방최고재판소는 결사의 권리에 근거해서 정부의 손으로부터 그의 회원명단을 보호할 수 있는 NAACP의 권리를 지지하였다.[22] 이 판례는 결사적 행동을 하는 등록자나 유저의 이름을 사적으로 보호하고자 하는 시스템운영자나 기타 사람들에 의하여 원용되고 있고, 주로 시스템운영자에게 적용되겠지만 온라인상의 공동체성(연대성)으로 볼 때 실제공간상의 결사와 동질직인 것이라 할 수 있으며, 이들의 신분을 밝히고자 하는 법률은 헌법상의 결사의 자유를 침해할 우려가 있게 된다. 이 결사의 자유는 가상공간에 있어서 유저들의 익명권과 함께 프라이버시보호의 중요한 한 수단으로 평가될 수 있다.

---

22) Gibson v. Florida Legislative Investigation Committee,372 U.S.539(1963).; 이 판례는 미국 플로리다주입법정보위원회가 공산주의자의 색출을 위하여 전미흑인권익향상협회(NAACP) 마이애미지부장 Gibson에게 회원명단의 제출을 명한 사건으로서 연방최고재판소는 이 명령을 결사적 프라이버시(associational privacy)를 보호하는 결사의 자유를 침해할 우려가 있다고 무효화하였다.

2. 암호문(Cryptography) 문제

인터넷의 능력·속도·신뢰도가 날로 향상되고 있고 새로운 용도로 끊임없이 발전되고 있지만 유동체성의 구조로 인하여 개인이나 국가기관의 도청과 통제로부터 끊임없이 도전을 받고 있다. 개인통신과 정보를 침해하는 행위는 법으로 금지되지만 인터넷이란 새로운 미디어에 있어서 기존의 프라이버시보호법적 사고를 가지고는 전통적인 전화시스템에서와 같은 정도의 법적 보호를 주지 못하는 경우가 많으며, 도청기술은 여전히 법의 규율을 앞서가기 때문에 항상 개인의 가상공간상의 프라이버시권은 침해받을 우려에 직면하게 된다. 따라서 네트워크상에서 암호화에 의한 활동은 도청이나 외부의 불법한 감시로부터 유저를 보호하는 중요한 도구가 된다.

개인통신의 비밀을 유지할 수 있는 강력하고 효과적인 민간 암호화기술의 출현으로 인하여 가상공간에서 개인통신을 도청할 수 있는 가능성은 완전히는 아니더라도 상당히 줄어들고 있다.[23] 즉 디지털기술을 이용한 암호화기술을 사용하면 컴퓨터 파일과 통신의 프라이버시를 비교적 효과적으로 보호할 수 있게 된다. 이 암호화기술을 이용하면 의무기록·기업비밀·개인의 물건구매습관·항공관제·신용기록·병원데이터·신용카드거래 및 전자메일 등에 관한 온라인상의 거의 모든 콘텐츠를 암호화할 수 있게 되고, 유저들은 본인이나 자기가 의도한 수신자만이 해독할 수 있는 방법으로 메시지 파일 기타 디지털정보를 교환할 수 있어 개인 프라이버시보호를 위한 매우 유용한 기술이라 할 수 있다. 그리고 진보된 암호화 기술로 작성된 암호메시지는 아무도 쉽게 해독할 수 없다. 따라서 누구든지 암호화기술을 이용한다면 프라이버시를

23) 컴퓨터에 보관되는 기록을 암호화하여 기록의 내용의 유출을 막고자 하는 디지털 기술로 암호화기계를 인코드(Encoder)라 하고, 이를 해독하는 기계를 디코더(Decoder)라 한다.

위하여 기술 그 자체가 개인에게 필요한 보호를 줄 수 있어 더 이상 법적 시스템에 매달릴 필요가 적어진다. 그러나 가상공간에서의 암호메시지와 암호화기술의 사용은 국가 보안상의 이유 등으로 인하여 도전을 받고 있고, 국가보안기관은 암호화된 정보를 해독해 볼 수 있는 마스터 키를 이용하여 전자메일과 인터넷통신을 여러 가지 이유로 도청하고, 분석하기도 한다.[24] 미국에 있어서는 FBI를 중심으로 정부로 하여금 암호화된 개인의 정보통신과 컴퓨터기록을 해독할 수 없게 하는 기술을 불법화하고자 한 적이 있었으나 끝내 관철되지는 못하였으나 몇몇 나라에서는 법으로 금지되기도 하며,[25] 미국에 있어서는 오늘에는 누구나 부당한 정부의 간섭없이 스스로를 보호할 수 있는 가장 강력한 암호화기술을 사용하여 자기의 프라이버시를 보호할 수 있게 되었다.[26] 1986년 ECPA에서 암호통신이 장려·보호되었으며, 1997년에는 합법적인 유선·전자통신과 저장전자정보의 보안·기밀성 및 프라이버시보호를

---

24) 민간의 암호기술이 급속히 발전하면서 각국은 암호 통제수단 마련에 부심하고 있다. 그 단적인 예가 민간업체가 암호제품을 만들어 팔 되 그 암호를 푸는 별도의 키를 정부에 맡기라는 '키복구'론이다. 정부는 언제든 위험 요소가 있을 때 암호를 풀 수 있도록 마스터키를 가져야 한다는 주장이 그것이다. 미국의 경우에도 클린턴 정부가 지난 93년부터 키 복구(Key Recovery)정책인 '클리퍼(Clipper)'라는 정책을 들고 나왔으나 사생활 노출의 위험을 우려하는 시민단체들이 극력 반대하고 있기 때문에 미의회 에서도 상원과 하원의 입장이 엇갈려 입법이 교착상태에 빠져있다. 경제협력개발기구(OECD)도 지난해 중반 논란 끝에 "키 복구를 의미하는 국가의 합법적 접근권(Lawful Access)을 인정할 수 있다"는 암호정책지침을 내놓았다(주간조선, 12.1). 우리 정부도 "키 복구 요건을 법률로 엄밀히 제한한다면" 키 복구 정책 도입은 필수적이라는 입장에서 있으나 국내에서도 시민단체의 반발이 예상된다.

25) FBI는 암호화"키"를 정부가 인정하는 제3자에 넘고자 하였으며, 공개키암호방식(Public Key Ecryption)은 전자우편보안기구(Preety good privacy(PGP))라 불리는 소프트패키지로 보충되어진다.

26) 미국은 "암호화에 의한 보안과 자유에 관한 법률(The Security and Freedom through Encryption Act)"을 제정하여 디지털 시대의 시민들의 헌법상의 권리인 컴퓨터상의 프라이버시를 보호하고자 하였다.

위하여 암호화방식에 관하여 개인에게 가능한 최대한 선택권을 보장하고, 암호화 통신과 정보를 해독할 수 있는 키홀더가 지켜야할 절차를 정하는 것을 내용으로 하는 암호화통신프라이버시보호법(Encrypted Communications Privacy Act)이 상원에 제출되었다. 컴퓨터암호화방식을 이용해서 작성되고 전송된 가상공간상의 정보는 모두 헌법상의 표현의 자유로 보호될 수 있으며, 암호문을 금지하거나 국가기관이 개인의 메시지를 해독할 수 있는 방법으로만 통신하게 하려는 것은 자유로운 표현을 침해하는 결과가 될 것이며, 이를 불법적으로 해독하거나 제한하려는 시도는 가상공간에서의 프라이버시 권리를 침해하게 되므로 네트워크상 자기정보에 관한 사항을 암호화하고 암호문으로 통신하는 권리, 즉 암호화권(Rights of Encryption)을 침해한다고 할 수 있다. 따라서 암호화통신을 제한하는 입법은 헌법상의 표현의 자유와 통신의 자유를 침해할 우려를 띠게 된다. 그리고 암호화통신의 해독은 불법한 수색·압수에 해당되며, 이 감청을 하고자할 경우에는 적법한 절차에 따른 감청영장을 발부받아야 할 것이다. 만약 해커(hacker)가 암호화된 컴퓨터 파일을 해독한다면 개인의 프라이버시의 보호는 기술에 의한 보호의 문제가 아니라 법적 보호의 문제로 대응할 수밖에 없다.

3. 인터넷검열(Censorship) 문제

국가는 공익상의 필요가 있을 경우에는 인터넷상의 콘텐츠를 검열할 수 있는 정당한 권한이 있는가? 이 문제는 다른 한편으로 가상공간에 있어서의 표현의 자유와 한계의 문제이기도 하다. 인터넷이 가진 익명성과 접속의 용의성·대중성 등으로 인해 국가 보안상의 요청이나 음란통신 감시 등의 공공의 안녕질서를 위하여 인터넷사이트나 네트워크 통신의 콘텐츠를 검열할 필요성이 증가되고 있다.[27] 그러나 이러한 검

27) 우리 나라도 최근에 언어·성·누드·폭력에 관한 인터넷·PC통신 콘텐츠를 전연

열법안이 근본적으로는 헌법상의 표현의 자유를 위축시키고, 나아가 개인의 프라이버시와 통신의 비밀을 침해할 우려를 심각하게 내포하고 있는 것이다. 그리고 사이트나 콘텐츠를 검열할 수 있는 법적 근거를 두는 경우에도 가상공간의 특수성을 인정하여 다른 미디어와 달리 특별한 보호를 줄 필요가 있는지 아니면 일반적 통신미디어와 같은 범주로 파악하고 그 정도의 보호를 주어야 할 지가 문제이다.

특히 노출·섹스·언어·폭력 등에 관한 불건전한 정보의 유통과 관련하여 인터넷상의 각종 사이트를 검열하는 문제가 논쟁거리가 되고 있다. 미국은 전자통신네트워크와 전자통신장비나 시설의 남용으로부터 공중을 보호하고자 1996년 「통신예절법(Communications Decency Act; CDA)」을 제정하였다. 이 법은 1934년 「통신법(The Communication Act)」의 전화통신시설을 이용한 음란이나 성희롱금지 규정을 새로운 전자통신설비에 맞게 개정한 것이다.[28] 그러나 이 법에 의해서도 합법적인 상업적 성인용음란물사이트로부터 미성년자를 보호할 수 없게 되자,[29] 1998년 미의회는 상업적인 성인용음란사이트에의 접속으로부터

령 이용가능 정보·18세 이상 성인용정보·등급외정보 등 3등급으로 구분하는 등급제를 실시하기로 하여 정보서비스사업자(ISP)가 등급구분을 자율적으로 하도록 하여 등급외정보의 유통을 금지하고, 정보통신윤리위원회가 사후심의를 통해 부적절한 등급구분에 대하여 권고형태로 변경 및 재조정을 요구할 수 있도록 하는 방안을 강구 중에 있다(한국경제신문,1998.12.8.).

28) 1996년 통신예절법(Communications Decency Act)은 1934년 통신법(The Communication Act) 중에서 '전화(telephone)'를 '전화통신장비(telecommunications device)'로, '어떠한 의견·요구·암시·제의를 하거나'를 '어떠한 의견·요구·암시·제의·이미지 혹은 기타 통신을 이용하거나, 전송하는'으로 개정하고, 또한 '신분을 밝히지 않고, 전화·전자통신으로 사람을 괴롭힘·학대·위협·성희롱의 의도로 전화나 전화통신장비를 이용하는' 경우를 추가하고, 또 도청과 누설을 금지하는 수단으로 '유선·구두·전자통신'에 '디지털'을 추가하였으며, 처벌을 강화하였다.

29) 1997년 펜실바니아주 최고법원은 18세 미만의 어린이로 하여금 음란하거나 유해한 자료를 알게하는 것을 범죄행위로 금지하고, 성인증명을 요구하는 CDA의 적극적 금지규정은 수정헌법 제1조의 표현의 자유에 위반된다는 전원일치결정을 내린 바 있다(Reno v. ACLU, 200 U.S. 321(1997)).

미성년자 보호를 내용으로 하는 인터넷 검열법인 소위 제2의 통신예절법(Communicatuons Decency Act Ⅱ: CDAⅡ)을 제정하였다. 이 법은 일괄세출예산안에 포함되어 있는데 두 개의 법안으로 구성되어 있다. 그 하나는 인터넷상의 미성년자보호법으로 일컬어지는 「미성년자온라인보호법(Child Online Protection Act: COPA)」으로 이 법은 온라인상 미성년자에게 有害한 자료를 상업적으로 공급하는 자로 하여금 18세 미만의 미성년자 보호를 위하여 '성인증명(adults verfication)'을 요구하도록 하는 규정이며,[30] 다른 하나는 각주가 유해하다고 인정하나 수정헌법 제1조에 의하여 보호되는 콘텐츠를 게제하는 상업적 웹사이트 운영자에 콘텐츠세를 부과하는 것을 허용하면서 다른 인터넷에 관한 과세에 관해서는 3년간 유예규정을 두는 것을 내용으로 하는 「인터넷과세면제법(Internet Tax Freedom Act: ITFA)」이다.[31] 그러나 이 두 법률은 '소수자에 유해(harmful to minors)'이란 모호한 카테고리를 사용하여 유해한 상업적 콘텐츠 공급자를 인터넷과세면제법(ITFA)의 모라토리움규정으로부터 제외함으로써 各州의 판단에 따라 성인용 웹사이트에 특별세금의 부가를 가능토록 하는 길을 열어 놓아 결과적으로

30) 이 법은 인터넷으로 국내 또는 외국과 상업적 통신을 통해 소수자에 유해한(harmful to minors) 자료를 유통시키는 자는 5만불 이하의 벌금이나 6월 이하의 징역에 처하고, 유해한 자료로부터 소수자를 보호하기 위한 적극적 조치(Affirmative defense)로서 신용카드나 수표의 사용, 성인증명을 요구하며, 전자통신망사업자 및 인터넷접속서비스업자 등에게는 적용하지 않는다. 여기서 소수자는 18세 미만의 미성년자를 일컫는(http://www.epic.org/free_speech/censorship/final_hr3783.html).

31) 이 법은 1998.10.1일부터 2001.10.21일까지 3년간 각주나 지방정부로 하여금 인터넷접속세(Taxes on Internet Access)와 전자상거래를 통한 구매자(소비자)나 판매자에게 다양하고 차별적 과세를 유예하도록 하고, 전자상거래과세에 관한 제문제의 연구와 이에 관한 실태를 의회에 보고하도록 하는 특별전자상거래자문위원회(Temporary Advisory Commission on Electronic Commerce)를 두도록 하고 있으며, 동시에 인터넷을 통한 상거래에 관해 일체의 새로운 연방과세를 금지하도록 하고 있다(http://www.house.gov/chriscox/nettax/).

선택적 과세에 의해 검열을 허용하는 위헌적 요소를 안고 있다. 나아가 연방으로부터 보조금을 받는 도서관이나 학교로 하여금 '외설적' 사이트를 걸러내는 필터를 의무적으로 사용하도록 하는 것을 내용으로 하는 인터넷검열법안(The Internet School Filtering Act)이 의회에 제출됨으로써 광범위하고 다양한 합법적 자료의 수신마저도 위협을 받을 우려에 직면하고 있다.[32] 물론 이 법안은 위의 두 법률과 함께 인터넷 접속의 시간과 비용을 증가시킬 뿐만 아니라 미성년자는 물론 성인 모두에게 다양한 사상의 시장으로 기능하는 인터넷의 특성을 저해할 우려가 있을 뿐만 아니라 헌법상의 표현의 자유와 내심형성의 자유, 프라이버시의 권리를 침해할 우려가 있다는 헌법적 논쟁을 안고 있다. 이상과 같은 이러한 입법적인 규제를 내용으로 하는 움직임과는 달리 음란물 사이트를 여과하는 프로그램을 보급하여 자율적으로 규제하려는 경향이 우리 나라나 미국에 있어서도 증가되어 가고 있다.[33] 그러나 최근에는 또한 인터넷 접속비용을 늘릴 수 있는 어떤 규제도 못하도록 하는 움직임이 나타나고 있기도 하다.[34] 그리고 해킹은 각종 컴퓨터시

32) 이 법안은 1998. 2. 9일 상원의원 John McCain 등이 제출한 것으로 'Safe Schools Internet Act'라고도 한다. 이 법안은 연방인터넷보조금을 받는 학교나 도서관은 소수자에 부적절한 자료를 걸러내고 봉쇄를 하도록 시스템을 인스톨하도록 하는 것을 내용으로 하고 있다 (http://www.intergov.org /public_information /issues/school_net_filters.html).

33) 우리 나라는 정보통신윤리위원회를 중심으로 하여 불건전한 정보를 차단하기 위한 소프트웨어(NCA patrol)를 개발하여 초·중·고교와 일반인에게 무료로 보급하고 있다(http://www.icec.or.kr). 이 소프트웨어는 6천여개의 음란물사이트를 수록하여 이 사이트에의 접속을 걸러 내도록 하고, 또 요일별로 인터넷 사용시간대와 총사용시간을 관리할 수 있도록 되어 있다. 최근에 '94년 미국의 웹사이트 등급산정활동을 해 온 '오락소프트웨어자문위원회(RSAC)'를 대체하여 '99년 5월 AOL·IBM·MS 등 컴퓨터·인터넷 관련 대기업들을 중심으로 인터넷 웹사이트의 폭력 및 음란성 등급을 매기는 영국 런던에 본부를 둔 '국제컨텐츠등급부여협회(ICRA)'라는 국제기구를 결성하였다(조선일보,1999.5.14.)

34) 미국시민자유연맹(ACLU)의 노력으로 다시 1998. 11. 19일에 펜실바니아 연방지방법원은 미성년자온라인보호법(COPA)의 집행을 잠정적으로 금지하는 명령을

스템의 정보나 통신내용의 열람이나 절취뿐만 아니라 통신의 감시나 검열의 목적으로도 이용될 수 있다는 점에서 개인의 프라이버시에 대한 중대한 도전이라 하지 않을 수 없다는 점에서 금지되고 있다.[35]

V. 맺는말

이상에서 보는 바와 같이 가상공간상에서의 행위는 다른 매체와는 달리 물리공간적 한계를 초월한 관념적 공간에서 시간적 한계에 제한받지 않으면서 의도에 따라서는 신분을 불문하고 누구나 열람할 수 있으며, 또한 실시간으로 직접 상호간에 대화할 수 있어 다른 통신미디어와는 다른 특성이 인정되고 있어 다른 미디어에 적용되는 법리적 관점을 그대로 적용함에는 한계가 있다. 인터넷은 한편으로는 사적인 커뮤니케이션으로서 보장하여야 하는 측면이 있고, 다른 한 측면에서는 누구나 쉽게 접속·캐취하기 쉽고, 파급성이나 이용목적·용도의 다양성 등으로 인하여 공적 측면도 많이 가지고 있는 것이 사실이다. 이러한 관점에서 가상공간상의 정보가 웹이란 형태로 결합되면 정태적 데이터보호의 관점이 아니라 다양한 경로와 목적으로 계속적으로 시간적·공간적 제약을 받지 않고 흐르는 유동체적 성질을 띠게 되어 종래의 통신이나 데이터보호적인 관점의 프라이버시보호규정으로는 효과적으로 대

내렸으며(CIVIL ACTION NO. 98-5591)(http://www.epic.org/free_speech/copa/tro.html), 최근 미국 상원은 소비자들의 인터넷 접속 비용을 늘리는 어떤 규제도 연방통신위원회(FCC)가 제정하지 못하도록 하는 법을 도입하여 통신회사로 하여금 인터넷 접속서비스를 강화하도록 유도할 방침이다(매일경제신문,199.4.1.).

35) 우리 나라의 해킹과 관련하여 적용될 수 있는 법령으로는 형법, 전산망보급확장과 이용촉진에 관한 법률,전기통신사업법,공공기간의 개인정보보호에 관한 법률, 신용정보의 이용 및 보호에 관한 법률,공업 및 에너지기술기반조성에 관한 법률,무역업무자동화촉진에 관한 법률,화물유통촉진법 등이 있다.

응하기 어렵다는 점에서 프라이버시권에 대한 새로운 도전이기도 하다. 또한 가상공간의 제문제는 범역성으로 인하여 한 나라의 국내적 문제로나 국내법적 대응으로는 효과적이지 못하며 국제적인 대응과 보조를 같이 할 때 비로소 해결 가능한 것이라는 점이 가상공간법제의 특성이라고 할 수 있다. 특히 가상공간에 있어서의 프라이버시권은 온라인상 자기신분을 노출시키지 않고 자유롭게 항해할 수 있는 익명권보장이 요구되고, 이와 관련해서 사이버공동체로서 활동할 수 있는 결사의 권리도 프라이버시와 매우 밀접한 관계에 있음을 알 수 있다. 동시에 웹상의 암호문통신을 가능케 하는 암호화권이 프라버시보호에 중요한 권리의 하나로 존중받을 필요가 있다. 가상공간에 있어서의 음란·폭력 등의 사이버폭력은 표현의 자유의 한계의 문제와 함께 웹상의 사이트접속을 필터링하는 문제는 인터넷검열문제와 같이 개인 프라이버시를 또한 위협한다. 따라서 불건전한 정보의 유통의 차단을 위하여 정보통신윤리위원회와 같은 기관의 기능 활성화·불건전한 정보의 규제강화·인터넷정보차단을 위한 소프트웨어 개발 등의 방안은 표현의 자유나 프라이버시보호와 관련하여 신중한 접근이 필요하다.

특히 음란물 등 불건전한 정보의 폐해를 막기 위하여 이의 유통을 규제하기 위한 적절한 법적 대응의 필요성은 공감되나 일정한 범주 안에서는 이러한 정보도 유용하고 합법적인 정보로서, 표현의 한 수단으로서 인정될 수 있음에 비추어 보아 건전한 정보에 대한 취사선택의 심미안을 정립하는 것이 중요하다. 특히 인터넷이라는 통신수단을 악용하는 것을 예방하려는 법적 노력은 항상 한계가 있으며 가상공간에 있어서 프라이버시보호의 과제로서는 올바른 웹문화를 확립하는 것이 필요하다. 즉 프라이버시 권리란 지극히 문화적인 개념으로 국가나 지역에 따라서 프라이버시 권리로 보호되어야 할 범위와 내용이 다를 수 밖에 없으므로 국가나 사회 등은 가상공간에서 수용 가능한 행위와 수용 불가능한 행위의 명확한 기준을 확립하여 수용 가능한 인터넷사용

정책을 개발하여 모든 유저들이 네트워킹에 참여할 때 지켜야 할 행동 양식 (Netiquettet)을 정립하고, 가상공간에서의 부적절한 행위는 프라이버시와 관련된 기타 인간의 제권리를 침해하므로 사이버권리를 존중하는 풍토를 가꿀 수 있도록 모든 네트워커들은 책임 있게 행동할 것이 필요하다. 어쨌든 가상공간에 있어서 프라이버시 침해란 현상은 정보화사회가 진전됨으로써 더욱 크게 부각되고 있는 문제이지만 종래보다도 프라이버시 침해의 가능성과 그 형태가 다양화·복잡화한 데 있으므로, 정보화사회에 있어서 정보의 사회적·경제적 가치를 극대화하면서 정보의 공유를 확대하여 표현의 영역을 확장할 수 있는 방안이 될 수 있도록 프라이버시보호법제와 정보공개법제 또한 균형을 이루도록 하여야 할 것이다. 그리고 가상공간에서 프라이버시보호의 과제는 보호를 위한 법적 규제문제로만 접근할 것이 아니라 가상공간이란 특성과 관련해서 프라이버시의 개념부터 다시 정립하여야 할 것이다.