EU의 인터넷 개인정보보호법에 관한 연구
A Study on the EU Internet Privacy Protection Rules

김은미(EunMi Kim)*

요 약 (ABSTRACT)

IT 산업은 인터넷을 발달시킴으로써 새로운 경제 시대 (New Economic Era)를 열게 하였을 뿐만 아니라 민주주의제도의 발전가능성을 한층 더 앞당기는 계기를 마련하고 있다. 그러나 개인들은 그들의 개인정보가 국가기관이나 민간기관에 자신도 모르는 사이 누출되어 국가기관의 감시체제를 구축하거나 불공정한 상업적 목적으로 쓰일 수 있다는 우려 때문에 온라인상의 구매활동이나 정치활동을 주저하고 있다. 특히 유럽민족은 과거의 역사적인 사건들로 인해 개인정보 유출문제에 매우 민감하게 반응한다. 이러한 이유로 EU는 EU국가들 내에서의 인터넷관련 개인정보처리문제와 EU와 제3국간의 개인정보 이전 문제를 규정하는 지침을 1995년 재정하고 1998년부터 시행하고 있다. 동 지침은 또한 미국과의 정보이전협상인 safe harbor를 탄생시켰다. 본 고에서는 왜 개인정보 보호법이 필요한지 그 이유와 개인정보보호에 대한 국제적인 논의 그리고 EU의 개인정보지침 내용을 연구한다.

Key Word : EU 프라이버시 보호 법 (EU Privacy Protection Law), 개인정보보호 (Protection of Personal Data), 세이프하버 (Safe Harbor), 무역장벽 (International Trade Barrier)

목 차

Ⅰ. 서론

Ⅱ. 인터넷 프라이버시 보호에 관한 국제적 논의

Ⅲ. EU의 인터넷 관련 개인정보 보호법

Ⅳ. 결론

참고문헌

Ⅰ. 서론

정보기술(IT: Information Technology)산업의 발달[1]은 인터넷의 활용을 급속도로 대중화시켰으며[2] 이는 개인 간, 기업 간 그리고 소비자와 기업 간의 정보흐름 형태를 바꾸어 놓고 있다. 또한 기업과 시장의 구조를 바꾸어 놓았으며 마침내는 상거래 방식을 오프라인(Off-Line)에서 온라인(On-Line)으로 즉 전자상거래(EC: Electronic Commerce)의 형태로 바꾸어 놓고있다.

선진국 특히 미국의 주도 하에 꾸준히 증가되어 오고 있고 앞으로도 증가될 것으로 예상되는 전자상거래는[3] '새로운 경제 시대' (New Economy Era)를 이끌어 나아갈 결정적인 요인이다. 그러

* 전북대학교 상과대학 무역학과 강사

1) 1998년 미국의 IT 산업 투자는 미 달러 44.8조 이었으며 이는 전체 회사들 연구개발투자비의 1/3을 차지한다.(US Department of Commerce, 1999)

2) 인터넷 인구는 1995년 22만에서 1997년 58만으로 증가되었다. (Ibid., 2000)

나 소비자들은 인터넷을 통하여 수집되어지고 사용되어지는 그들 자신의 정보가 타인으로부터 보호받지 못할 것이라는 우려 때문에 온라인상의 구매를 주저하고 있다.[4]

프라이버시(privacy)의 보호를 위한 제도는 전자상거래의 개발을 위한 전제조건[5] 일 뿐만 아니라 참여민주주의[6]를 활성화시키기 위한 전제조건이기도 하다. 민주주의를 발전시킬 수 있는 요소 중의 하나가 커뮤니케이션 수단의 발전이라 할 수 있다. 왜냐하면 주권을 가진 국민들은 그들이 뽑은 대표자들을 감시할 수 있어야 하며 그러기 위해서는 그들이 주도하는 정치, 경제, 복지 등의 정책 내용을 알고 심사할 수 있어야 하기 때문이다. 최근 케이블 텔레비전, 컴퓨터 통신, 인공위성 통신, 인터넷 등의 뉴미디어라는 커뮤니케이션 수단이 새로이 등장하고 있다. 이러한 뉴 미디어를 통하여 근대 민주주의의 제도는 변화를 가져올 수 있다.[7] 예를 들어 선거운동, 선거구 책정, 투표 등의 민주주의 활동이 뉴미디어 특히 컴퓨터 통신과 인터넷을 통하여 이루어진다면 그 비용도 저렴하고 보다 많은 유권자들이 참여할 수 있게 될 것이다. 그러나 프라이버시, 특히 개인정보를 보호할 수 있는 제도가 확립되어 있지 않다면, 인터넷의 발달은 오히려 민주주의에 악영향을 미칠 수 있다. 개인들은 여권 신청, 신용카드 신청, 물건 구입, 정보 취득을 위해 자신들의 신상정보를 등록할 수밖에 없기 때문에 개인정보가 유출될 수 있는 경로는 점점 많아지고 있다. 그러므로 국가기관과 학교, 신용카드 회사, 은행, 홍신소 등의 사기관들은 개인 정보를 정보주체 모르게 구축할 수 있으며 국가기관에서는 이를 감시체제에 이용할 우려가 있다.

IT 산업의 발전은 인터넷을 통한 전자상거래를 촉진시켜 새로운 경제시대를 펼칠 수 있게 하여주고, 민주주의제도를 근본적으로 변화시킬 수 있다. 그러나 이러한 발전을 저해하고 있는 것은 기술적 문제가 아니고 기술 발전을 따라 잡지 못하고 있는 법적인 장치들이다.

본 연구에서는 인터넷 프라이버시에 관련된 국제적인 논의와 인터넷 프라이버시 문제 특히 프라이버시권 중에서도 현대의 인터넷활용과 직접적으로 관련된 문제 중 개인정보보호문제를 다루고 있는 EU의 '개인정보보호지침' 과 EU와 미국간의 개인정보이전에 관한 협상인 'safe harbor'를 고찰하여 보고자 한다.

II. 인터넷 프라이버시 보호에 관한 국제적 논의

프라이버시에 대한 논의는 1978년부터 OECD에서 이미 시작되었고 개인정보보호문제에 대한 논의는 1970년대부터 유럽과 미국을 중심으로 이루어 졌다.

개인정보보호의 입법방향은 크게 유럽형과 미국형으로 나눌 수 있다. 첫째는 하나의 법률에 의

3) 전자상거래의 세계시장규모는 미국 달러 3조 2천억(미국시장규모는 미국달러 1조)으로 추정되는데 이는 1998년의 세계시장규모인 미국 달러 810억의 약 40배이다. (Ibid., 1999)

4) 예를 들면 네트웍의 안전성의 장해에 대한 우려가 68%, 물품의 배송상의 문제에 대한 우려가 58%, 타인의 개인정보 침해에 대한 우려가 55%, 판매자의 신용에 대한 우려가 68%, 물품의 차이가 49%, 기타 이유 20% (정영화, 2000)

5) Mario Monti. Rome, 9 May 1998, www.europa.eu.int/comm/internal_market/en/speeches/rome0598.htm

6) http://freespeech.jinbo.net/white/98-2/98-2.htm#2.1

7) 김주환

하여 국가, 지방자치단체와 같은 공적 부문과 민간기업과 같은 민간 부문의 양 부문을 포함하는 방식(Ombudsman System)이며 둘째는 공적 부문과 민간 부문을 분리하여 개별적인 법률로 규율하는 방식(분리방식)이다.[8] 전자는 법과 제도를 중심으로 강한 보호정책을 갖는 것이며 주로 유럽의 나라들이 관련법의 제정을 위해 채택하고 있고, 후자는 자율규제를 중심에 두고 개별법안, 판례 등을 통해 보완해 나가는 방식으로 주로 미국, 일본 등이 채택하고 있다. 그러므로 본 장에서는 세계 각국의 개인정보보호관련 입법의 기준이 되고있는 OECD가이드라인, 미국형 관련 입법, 유럽형의 관련 입법에 대하여 개략적으로 살펴보겠다.

1. OECD

OECD는 1978년부터 이루어진 프라이버시 보호에 대한 논의의 결과 1980년 이후 다음과 같은 여러 지침과 가이드라인이 채택되었다. "프라이버시 가이드라인 "(Privay Guideline, 1980), "개인정보의 자동처리에 대한 개인정보보호에 관한 협약 (Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, 1981), " 프라이버시 보호와 개인 데이터의 국제유통에 관한 가이드라인에 관한 이사회 권고" (OECD Guidelines Governing the Protectionof Privacy and Transborder Data Flows of Personal Data, 1981), 암호가이드라인(Cryptography Guideline, 1997), 글로벌네트웍에서 프라이버시보호의 정부간 선언(Ministrial Declaration on the Protection of Privacy on Global Networks, 1998) 등이 그것이다.

OECD 이사회가 1981년 채택한 프라이버시보호와 개인정보의 국제유통에 대한 지침[9]은 개인정보의 수집 및 관리에 관한 국제사회의 일치된 의견을 반영한 것으로써, 비록 법적 구속력을 가지지는 않지만 개인정보 보호의 중요한 기준이며 전 세계적으로 개인정보보호 입법시 반영되는 것이다. 그 대상은 공적, 사적부문에서의 특정 개인과 관련된 모든 정보이며 개인정보의 사생활권 보호, 정보의 자유로운 유통장려, 국내사생활보호입법에 의한 자유로운 정보유통에 대한 부당한 제한방지, 관련국 내법규정과의 조화를 주목적으로 하고 있다. 이는 또 회원국의 관련 입법시 그 방향을 제시하기 위해 8대 원칙[10]을 규정하였으며 그 내용이 기술 중립적이기 때문에 인터넷에서 발생하는 프라이버시

8) 김진아, 2000

9) 이는 크게 총칙, 국내적용상의 기본원칙, 국제적 적용상의 기본원칙, 국내실현, 국제협력에 관한 5개장으로 구성되어 있다.

10) 국내적용상의 기본 원칙으로 그 내용을 요약하면, 첫째, 개인정보수집제한의 원칙: 개인정보는 정보주체의 동의 하에 적법하고 공정하게 수집되어야 한다. 둘째, 개인정보 특성의 원칙: 개인정보는 사용되는 목적에 관련되어야 하며, 정확하고 완전하여 항상 최신의 것이어야 한다. 셋째, 목적 특정화 원칙: 개인정보 수집의 목적은 명확해야 하며, 개인정보의 이용은 당해 수집목적에 모순되지 않아야 한다. 넷째, 개인정보 사용제한의 원칙: 개인정보는 정보주체의 동의나 법령에 의한 경우를 제외하고는 수집된 목적 이외의 목적으로 사용되어서는 안 된다. 다섯째, 개인정보안전의 원칙: 개인정보는 부당한 접근, 사용, 수정의 위험으로부터 합리적인 안전보장조치에 의해 보호되어야 한다. 여섯째, 공개의 원칙: 개인정보에 대한 관행 및 정책은 공개되어야 한다. 일곱째, 개인참여의 원칙: 정보주체는 다음과 같은 권리를 가진다. i)데이터 통제자가 자기에 관한 정보를 가지고 있는지의 여부를 확인할 수 있다. ii) 정보주체는 자신에 관한 정보를 정당한 기간 내에 통지 받아야 한다. iii) 위의 두 가지 권리가 거부되었을 경우, 그 거부에 대한 이의를 제기할 수 있다. iv) 정보주체는 자신의 정보가 잘못되었을 경우 그 정보를 수정, 삭제, 종료할 수 있다.
이 외에도 국제적 적용상의 원칙으로는 첫 번째, 가맹국간에 적용되는 것으로 개인 정보의 국내처리

침해 관련 입법시에도 가이드라인으로서 기능할 수 있다.[11]

2. 미국

미국은 1972년의 워터게이트사건을 계기로 프라이버시 보호 논의를 시작하였다.[12] 미국의 프라이버시 관련법은 부문별 입법형식을 취한다. 즉 연방행정기관에 대해서는 프라이버시법이 적용되며, 민간부문에 대해서는 개인의 신용정보보호법이 개별적으로 적용된다. 미국의 프라이버시법은 정보공개제도를 전제하고 있으며 그로 인한 개인의 피해를 막는 것을 원칙으로 하고 있다. 프라이버시법과 정보공개 제도는 맞물려 있는 경우가 많은데 대부분의 경우 정보공개관련법이 프라이버시 관련법의 우위에 있어 그 충돌을 피하고 있다.[13]

미국의 개인정보보호 법체계는 초기 정부기관을 중심으로 이루어진 후 전산망 이용의 확대에 따라 민간부문의 개인정보보호 요구를 기존 법에 포함시키는 과정으로 발전되었다. 개인정보보호와 관련하여 미국은 프라이버시법(1974), 금융프라이버시권리법(1978), 전기통신보호법(1986), 전자통신프라이버시법(1986), 컴퓨터자료의 상호비교 및 프라이버시보호법(1988), 컴퓨터연결 및 프라이버시보호법(1988), 비디오프라이시법(1988), 전화판촉으로부터 소비자 보호법(1991), 개인운전기록보호법(1994), 통신법 및 의료기록비밀보호법(1996), 아동온라인프라이시보호법(1999) 등을 제정하여 시행하고 있다. 한편 미국에서는 이러한 연방법이외에 주법과 판례에 의해 개인정보보호가 이루어지기도 한다.

이러한 법률적인 제도이외에 미국은 국가정보통신기반정책을 추진하고 있으며, 정보정책위원회를 구성하여 정보통신기반을 전담하고 있다. 또한 정보정책위원회 3개의 작업반 가운데 하나인 프라이버시 작업반이 1995년 '프라이버시와 개인정보제공 및 이용의 원칙'을 작성하여 사용하고 있다. 이 원칙은 계약적 접근방법에 의하여 제공자의 통지와 소비자의 동의라는 두 개의 필수요건 성립에 기반을 두고 업계의 자율적인 규제가 우선함을 강조하고 있다.[14]

이 외에도 미국은 각 국별로 다르게 나타나는 개인정보보호관련제도의 차이로 인한 갈등을 해결하려 노력하고 있다. 이로 인하여 자칫 미국기업들의 영리행위를 저해할 수 있기 때문이다. 즉 미국은 국가 간의 자유로운 정보유통을 제도화하려 하고 있으며 2000년 11월부터 시행되는 safe harbor가 그 예이다.

3. 유럽

유럽인들은 히틀러와 게스타포, 러시아와 KGB, 그리고 동독과 비밀경찰 등으로부터의 프라이버시

및 재유출의 타국에 대한 영향배려, 두 번째, 개인정보의 국제유통의 안전하고 효과적인 유통을 위한 수단 강구, 세 번째, 가맹국간의 개인정보 유통억제, 특수한 개인정보에 대한 상호주의적 유통억제 수단, 개인정보의 국제적 유통제한에 대한 과잉 금지원칙 등이 있다.

11) Ibid.

12) 김윤명

13) Ibid.

14) 김진아, 2000

침해에 대한 아픈 기억들 때문에 다른 어느 민족보다도 자신들의 사생활에 관한 정보를 공개하는 데에 있어 민감하며, 그들은 일반적으로 국가차원의 강력한 제도를 통하여 보호받고자 원한다.[15]

유럽형의 특징은 제도를 중심으로 하는 프라이버시 보호이다. 따라서 프라이버시와 관련된 법이 중심이 되고 이를 보완하기 위한 Ombudsman 형태의 제도를 채택하는 등 제도적 장치에 강점을 지니고 있다.

(1) EU

개인정보보호에 관하여 강력한 정책을 추진하고 있는 EU의 유럽의회와 유럽이사회는 일반적인 개인 정보 취급에 대한 규정으로 회원국 국민의 기본권과 자유권를 보호하고 개인정보 처리와 관련한 프라이버시권을 보호하며 EU 국가 간의 개인정보의 자유로운 유통을 촉진하기 위하여 1995년 '개인정보처리관련 개인의 보호 및 정보의 자유이동에 관한 지침'을 제정하였는데 이는 1998년부터 시행되고 있다. 1997년 12월에는 동 지침을 보완하기 위하여 「정보통신부문에서의 개인정보 처리 및 프라이버시보호에 관한 지침」을 채택하였다. 이는 주로 ISDN(the Integrated Services Digital 네트워크)이나 디지털 이동 네트워크(public digital mobile 네트워크)를 통한 정보통신 서비스에 적용되며 그 목적은 주로 개인데이터의 처리와 관련한 기본적 인권과 자유, 특히 프라이버시권의 균등한 보호수준을 보장하고, EU에서의 데이터와 통신설비 및 서비스의 자유로운 이동이 보장되도록 각 회원국 규정들간의 조화를 이루는 것이다. 또한, 1999년 2월에는 인터넷에서의 프라이버시 보호를 위한 각료위원회 권고(No. R(99)5)인 「정보고속도로에서 신상정보의 수집처리와 관련한 개인의 보호를 위한 지침」을 채택하였는데 이는 인터넷 이용자와 서비스 제공자(ISP)의 권리와 의무를 담고 있다.

(2) 영국, 스웨덴, 프랑스

영국은 주거침입·저작권침해·비밀침해·명예훼손 등을 대상으로 한 개별 법률을 통해 프라이버시 영역에 속하는 모든 권리를 보호해왔다. 개인정보 보호에 관한 입법은 1975년 컴퓨터와 프라이버시 컴퓨터와 프라이버시에 대한 보호조치 라는 백서의 발간을 계기로 시작됐다. 이후 개인정보보호기구인 데이터보호위원회가 1976년 설립됐고, 1984년 데이터보호법이 제정됐다. 1987년에는 '개인기록접근법 을 제정하여 정보주체가 자신의 정보에 접근할 수 있는 권리를 확대시켰다. 스웨덴은 1973년 세계 최초로 '데이타법'을 만들었으며 '데이타검사원'이라는 감독기관을 설치하였다. 프랑스는 1978년 '정보처리·축적 및 자유에 관한 법률'을 제정하였으며 개인정보처리업무의 감독을 위해 '국가정보처리자유위원회'라는 기관을 설치하였다.

III. EU의 인터넷 관련 개인정보 보호법

1995년 10월 EU의 유럽의회(European Parliament)와 각료회의 (European Council)에 의해 제정되고 1998년 10월부터 시행되어온 '개인정보처리관련 개인의 보호 및 정보의 자유이동에 관한 지침'(이하 지침이라 칭함)은 인터넷을 통한 프라이버시의 침해로부터 EU의 시민들을 보호하여 주고 있

15) http://www.privacy.org/pi/

다.[16] 지침은 OECD의 개인정보보호를 위한 8가지 원칙을 모델로 하여 감독기관의 문제, 정보보호자 제도, 개인정보 제3국 이전규제, 수기정보도 대상화, 정보주체의 접근, 삭제, 정정 청구권에 더하여 반대, 폐쇄권, 관리자의 과실입증책임, 정보 직접판매에 대한 동의권 등의 원칙을 제시하고 있다.

지침은 다음 두 가지의 큰 특징을 지니고 있다. 첫째, 이는 EU의 15개 멤버 국가들이 만들어 이행할 수 있는 프라이버시 보호를 위한 법적인 원칙을 제시하였다. 둘째 이는 EU 국가로부터 EU 시민들의 개인정보가 적절한 데이터 보호 관련법을 갖추지 못한 제3국으로 이전되는 것을 금지시킴으로써 미국과 유럽간의 협의인 safe harbor를 정립시켰다. 이러한 특징을 지닌 지침은 비록 국제적인 협약이 아니지만 전자상거래와 전자무역의 발전과 더불어 발생하고 있는 개인정보보호에 대한 국가내의 구체적 정책방향의 제시라는 점에서, 그리고 EU와 같이 명시적으로 프라이버시와 개인정보의 보호를 규정하고 있는 나라와 미국과 같이 자율규제를 택하는 나라간의 개인정보의 흐름을 보장하는 방안이 제시되었다는 점에서 그 중요성이 매우 크다고 볼 수 있다.

지침은 개인정보보호 문제를 다루는 데 있어 크게 두 분야로 구분된다. 첫 째는 EU 내에서 즉 회원국들내에서 발생할 수 있는 개인정보노출 문제를 규제하는 내용이며 둘째는 EU와 제3국간의 개인정보의 흐름을 규제하는 내용이다. 그러므로 본 연구에서는 이 두 가지를 구분하여 논하고자 한다.

1. EU내에서의 인터넷 프라이버시 노출문제[17]

EU의 개인정보보호 지침은 개인정보에 대하여 취하여지는 모든 행위, 즉 개인정보[18]의 수집, 처리, 저장, 공개 등에 대해 적용되는데 그 주요내용을 살펴보면 다음과 같다.

첫째, 지침은 정보주체(data subject)에게 본인의 정보에 대한 권리를 다음과 같이 부여한다 (12조, 14조). (i) 정보소유 본인은 수집되어진 자신에 관한 정보에 접근할 수 있다. 즉 누구든지 어떤 정보처리자가 본인의 개인정보를 처리하고 있는지 알기 위해, 그리고 그 개인정보의 사본을 받기 위해 정보통제자에게 접근할 권리가 있다. (ii) 본인에 관한 정보가 불완전하거나 정확하지 않을 때는 그것을 수정할 수 있다. 이 경우 정보주체는 정확하지 않은 정보를 전에 이용했던 제3자에게 통지하도록 정보통제자에게 요구할 수 있다. (iii) 정보주체는 본인에 관한 정보가 수집되는 것을 반대할 수 있으며 그 반대의 이유가 정당한 경우에는 인정된다. 그러나 인종, 정치적 의견, 종교적 혹은 철학적 믿음, 노동조합가입여부, 건강 상태와 같은 민감한 신상정보들에 대해서는 무조건적으

16) 본래 지침은 인터넷을 통하여 발생되는 문제에 대한 규정을 두고 있지 않지만 제29조에 의거하여 설치된 working party (지침은 29조에서 working party (Article 29: Working Party on the Protection of Individuals with regard to the Processing of Personal Data)를 인정했다. 이들은 각 멤버국들을 대표하며, 1996년 이후 규칙적으로 모임을 가지고 있다. 이 모임에서 이들은 여러 권고문들을 채택하는데, 인터넷의 익명성에 관한 권고는 1997년에 받아들여졌다. 그리고 이들은 더블린의 1998년 제 5 회 유럽연합 데이터 보호 이사들 컨퍼런스에서 1995년 지침을 인터넷에 적용을 시키도록 공식적인 발표를 하였다)가 공식 승인함으로써 지침은 1998년 이후 인터넷에 의해 발생되는 개인정보 침해로 인해 발생하는 문제들에도 적용되어 지고 있다.

17) Directive 95/46/EC 1995

18) 개인정보란 이름, 사진, 전화번호, 개인식별번호 등에 의해 식별 가능한 개인에 관련된 정보를 의미한다. (2조)

로 그 반대가 인정된다. 예외적으로 고용법에 의해 요구되거나, 정보주체의 동의를 얻을 수 없는 경우, 예를 들어 길에서 사고가 났을 때 그 피해자의 혈액검사를 해야 하는 경우에는 정보수집이 정보주체의 동의 없이도 가능하다 (8조).

둘째, 정보통제자(data controller, processor)[19]는 개인정보를 정보주체로부터 직접 수집하였거나, 제3자를 통하여 간접적으로 획득하였거나에 관계없이 본 지침에 의하여 다음과 같은 몇 가지 제한을 받는다.[20] (i) 개인정보는 공정하고 합법적으로 처리하여야 한다. (ii) 정보 수집의 목적이 명확하고, 투명하고 정당하여야 하며 정보의 처리 목적이 수집의 목적과 상반되어서는 안 된다. 그러나 데이터가 역사적, 통계적 혹은 과학적 목적으로 처리될 때는 수집의 목적과 상반되어도 상반되지 않는 것으로 간주한다. (iii) 수집된 정보가 해당 목적에서 벗어난 어떤 다른 용도로서 처리되어서는 안되며 (iv) 개인정보의 수집 및 재처리가 목적에 비추어 볼 때 적절성, 관련성, 정확성 등을 갖추고 있어야 하며, 개인정보는 항상 최신의 것으로 갱신되어야 한다. 또한 정보가 수집되었을 당시의 부정확한 정보를 재처리 삭제, 교정하기 위한 모든 합리적인 조치가 취해져야 한다. (v) 수집된 정보의 목적상 필요하다면, 정보주체의 신원확인을 허용하지 않는 형식을 취해야 한다. 회원국은 역사적, 통계적 혹은 과학적 사용을 위하여 개인정보가 더 오랜 기간 저장되어야 할 때를 대비한 적절한 보호 조치를 취해야 한다 (제6조). 데이터 통제자는 개인정보를 처리 할 때마다 정보주체에게 정보통제자의 신분, 정보 처리의 목적, 정보획득의 방법, 정보의 수신자, 그리고 질문에 응하는 것이 의무적인지, 자발적인지, 질문에 응하지 않았을 때 발생할 수 있는 불이익과 같은 정보주체의 특정 권리 등을 통지해 주여야 한다 (7조, 10조, 11조). 만일 정보의 소유자가 동의하지 않았음에도 불구하고 정보가 수집되었다면 이는 불공정한 것으로 여겨진다 (제14조). 또한 개인정보수집을 위한 서류가 관공서봉투를 통하여 전달되는 경우 그래서 정보소유자를 혼동시키는 경우, 이는 불공정한 행위로 여겨진다.[21]

인터넷을 통하여 정보를 수집하는 경우에도 데이터 통제자들은 본 지침에서 정보통제자들에게 부여한 의무들을 준수하여야 한다. 이유인즉 인터넷을 이용한 정보수집에 있어 정보소유자 본인이 알지 못하는 사이에 그들의 정보가 정보통제자에게 전달되어질 수 있기 때문이다. 이메일이나 뉴스그룹 등을 통하여 정보수집을 하게되는 경우에는 정보소유자들의 협력을 구하여야 하기 때문에 정보소유자들은 그들의 정보가 수집되어진다는 사실을 반드시 알 수 있다. 그러나 log file 이나 cookie를 사용하는 경우 정보 통제자들은 정보의 소유자에게 통지하지 않고도 그들의 정보를 수집할 수 있는바 이는 엄격히 불공정한 행위이다.[22] 그리고 공공기관인것처럼 가장하여 인터넷에서 개인정보를 수집하는 경우 이들은 공공기관을 사칭하여 정보의 소유자들을 혼동시킨 것이므로 불공정한 행위로 여겨진다.

---

19) 정보수집을 통제하고, 그 정보를 사용하는 사람이나 사업을 수행하는 영리단체 (1조)

20) 예를 들어 의료진이 그 환자들의 건강에 관한 정보를 처리할 때, 회사가 직원이나 고객들에 관한 정보를 처리할 때, 스포츠클럽이 멤버들의 신상정보를 처리할 때, 공공도서관이 이용자들의 정보를 공개할 때 각 정보통제자들은 지침에 의해 제약을 받게 된다. 그러나 개인적이거나 가계에서 발생하는 문제들 예를 들면 개인의 e-mali 내용이나 가족의 신변사항이 노출되거나 할 때는 본 조치가 적용되지 않는다.

21) Bejot, Michel, 2001

22) 본 지침에 의거하여 가능한 해결점은 cookie가 만들어질 때마다 web site에서 그 사용자에게 통지하는 것이다 (Bejot Michel, 2001)

셋째, 개인정보의 처리에 관해 지침은 다음과 같은 몇 가지 원칙을 제시한다. (i) 정보주체가 명백하게 동의해야 한다. 즉 정보주체가 정보처리에 대한 통보를 받은 후 자발적으로 명확히 동의하여야 한다. (ii) 데이터의 처리가 계약 성립을 위해 필요할 때 혹은 정보주체가 신청한 계약을 성립시키기 위해서는 정보주체의 동의 없이도 정보처리는 수행될 수 있다. 예를 들어 정보주체가 입사원서나 대부신청서를 제출하였을 때 정부 통제자는 필요에 의해 미리 정보주체의 정보를 처리할 수 있다. (iii) 정보처리가 법으로 요구되거나 정보주체의 중요한 이익을 보호하기 위해 필요하다거나 (iv) 정보처리가 공공의 이익을 위해서 혹은 세금징수를 위해 혹은 정부나 경찰과 같은 공공기관의 업무수행을 위해 필요한 경우 (v) 정보통제자나 제 3자가 정보처리를 함으로써 발생되는 합법적인 이익이 정보주체의 기본권, 특히 프라이버시에 대한 권리를 보호함으로써 발생하는 이익보다 클 때 정보처리는 이루어질 수 있다.

2. EU와 미국간의 개인정보 전송협정: Safe Harbor[23]

이상은 EU 역내 국에서 개인정보를 상업상의 목적으로 처리할 때 준수하여야할 원칙들이었다. 다음은 미국기업들이 영리상의 목적으로 EU시민들의 개인정보를 미국 내로 이전시키고자 할 때 지켜야 할 원칙들이다.

지침은 25조에서 EU의 시민들에 관한 개인정보가 정보 전송작업에 관련한 모든 상황에서 평가되어진 적절한 보안수준[24]을 갖추고 있지 않은 제3국으로 이전되는 것을 금지시켰다. 본 조항은 EU 시민들의 개인 정보들이 적정하지 않은 제3국으로 매매 되는 것을 금지시키고 있으며 web site를 이용하여 개인정보를 수집할 때 그 web site는 사용자들에게 그 사실을 알려야만 한다고 지시하고 있다.

미국은 유럽과 같이 광범위하고 포괄적인 입법조치에 의하기보다는 부문적이고 개별적인 입법조치[25]와 자율규제를 통하여 프라이버시를 보호하고 있다. 이러한 제도적 차이로 인해 미국의 기업들, 특히 금융기관, 여행사, 의료기관 등과 같이 개인정보를 이용하여 영리를 취하는 기업들은 EU시장의 진출에 많은 어려움을 겪게 되었다.[26]

이에 미국 상무부(US Department of Commerce)는 1998년부터 미국 산업체 등과의 협의를 통해 미국 기업이 일련의 개인정보보호원칙을 자발적으로 준수하도록 하는 safe harbor의 초안[27]을 만들

---

23) Safe Harbor Document, 2000

24) 적절한 데이터보호수준을 증명하기 위해서는 첫째, 데이터의 처리는 공정하여야 하며, 정보주체에게 당해 정보의 수집에 대한 정확하고 충분한 정보가 제공되어야 한다. 둘째, 데이터는 그 목적에 대해 적절하고 연관성 있는 것이어야 하며, 본래 목적에서 벗어나서는 안 된다. 셋째, 데이터의 수입과 처리목적은 명확하고 합법적이어야 하며, 이를 명시하여야 한다. 넷째 데이터의 처리는 그 주체의 의지에 따라 수행되어야 하고, 합법적 목적이 아니라면 명시된 법률 규정에 따라야 한다. 마지막으로 독립적인 통제기관은 데이터 처리 원칙의 내부적인 적용을 확인하는 능력이 부여되어야 하며, 데이터 처리가 원래의 목적에 반하여 정보주체의 권리나 자유에 영향을 주는 것을 막을 수 있는 권한이 있어야 한다.

25) 연방행정기관의 개인정보취급 원칙을 규정하는 프라이버시법(1974), 예산관리국의 정보규제사무국의 정보수집 요청을 규정하는 문서감축법(1980), 연방데이터베이스 자료의 상호비교 및 합성을 위한 요건을 규정하는 컴퓨터 연결 및 프라이버시보호법(1988) 등이 그 예이다.

26) Bejot, 2001

었고 이의 제정을 위해 EU 위원회와 꾸준히 논의하였으며 마침내 2000년 11월부터 safe harbor가 시행되기 시작했다.

safe harbor란 미국에서 자발적으로 만든 원칙으로 EU에서 요구하는 개인정보보호에 필요한 적절한 보안수준을 만족시켜주는 프라이버시 원칙이다. safe harbor에의 가입여부는 미국기업이 자발적으로 결정하며 safe harbor에 가입한 미국기업은 safe harbor의 원칙을 준수해야 하고 그 사실을 공식적으로 선언해야 한다. 즉 safe harbor 원칙의 준수를 신청한 미국 기업들은 EU 시민들의 프라이버시 보호의 이행을 약속하는 것이며 그 약속에 대해 미국의 연방무역위원회(Federal Trade commission)와 미상무부의 감독을 받겠다고 약속하는 것이다. 또한 이들 기업들은 매년 가입여부를 자기 인증의 형식으로 미상무부에 서면으로 제출해야 하며 미상무부는 이들 기업들의 리스트와, 그들이 제출한 신청서를 미상무부의 web site에 공개하도록 되어있다.

safe harbor 원칙을 준수하는 미국의 기업들은 다음과 같은 혜택을 받게 된다. 첫째 15개 EU 회원국은 safe harbor 원칙의 적정성에 대한 EU 위원회의 결정에 따르게 된다. 둘째, safe harbor에 참여한 미국기업들은 적정하다고 여겨지게 되며 그러므로 그들은 EU시민들의 개인정보들을 제공받을 수 있다. 셋째, EU회원국이 정보교류에 앞서 요구하는 사전승인을 피할 수 있거나 자동적으로 받게 된다. 넷째 safe harbor 원칙은 EU 시민들의 개인정보보호를 사용하기 위해 미국 기업들이 치러야 하는 어떠한 절차보다도 간결하고 신속하다. 다섯째, safe harbor 원칙의 참가자들은 그 원칙의 구현에 필요한 유예기간을 부여받을 수 있다.[28]

safe harbor의 주요 원칙은 다음과 같다. 첫째, 정보주체는 명확하게 정보수집의 목적, 정보통제자 및 정보를 이용할 제3자의 신분 및 그들과의 연락방법 그리고 개인정보의 사용이나 노출을 제한할 수 있는 방법 등에 대한 통지(Notice)를 받아야 한다. 둘째, 정보주체는 자기정보가 처음 통지된 목적으로 사용되지 않을 때 그 정보에 대한 수정 및 삭제 등의 선택권(Choice)을 제공받아야 한다. 셋째, 제3자에게 정보를 공개하는 경우 정보의 통제자는 위의 통지 및 선택의 원칙을 준수하여야 한다. 개인 정보를 제3자에게 제공 (Onward Transfer)하고자 할 때는 제3자가 최소한 safe harbor 원칙과 동일한 정도의 프라이버시 보호를 준수할 것을 요구 및 확인하여야 한다. 넷째, 개인정보를 처리(수집, 유지, 이용, 보급)하는 정보통제자는 손실과 오용, 비인가접근, 공개, 변경이나 파기로부터 그 개인정보를 안전 (Security)하게 보호하기 위한 합리적 예방조치를 취해야 한다. 다섯 째, 정보통제자는 수집된 정보의 정확성, 완전성, 그리고 최신성을 유지해야 하며 수집목적과 관련되고 고지와 선택권 원칙에 부합하는 개인정보만을 유지해야 한다. 즉 미국의 정보통제자는 정보의 무결성(Data Integration)을 위해 노력하여야 한다. 여섯째, 정보주체는 자신의 개인정보에 접근 (Access)할 수 있어야 하며, 정보통제자가 보유한 자신에 관한 정보가 부정확하다면, 그 비용이나 부담이 개인의 프라이버시에 비해 그리 크지 않고, 다른 사람의 프라이버시가 손상되지 않을 경우, 이를 수정하거나 삭제할 권리를 제공받아야 한다. 일곱째, 개인정보의 보호를 효과적으로 이행(Implementation)

27) 첫 번째 초안은 1998년 11월에 만들어졌고 두 번째는 1999년 4월에 세 번째는 1999년 11월에 만들어졌다. 그리고 마지막 안은 2000년 3월에 만들어 졌고 이 안이 개정되어 유럽위원회에 의해 최종적으로 채택되었다.

28) 미국 상무부는 웹사이트(WWW.export.gov/safeharbor)에 safe harbor 원칙을 준수하겠다고 신청한 기업들의 명단을 작성해 두었다. 그러므로 유럽연합의 기업들은 이 명단을 확인함으로써 개인정보를 미국기업에 제공할 수 있다.

하기 위해서는 원칙의 준수로 인해 영향을 받는 이해당사자를 위한 청구권과 원칙을 준수하지 않은 미국의 기업들에 제재를 가할 수 있는 메카니즘이 필요하다. 본 메카니즘은 최소한 다음의 사항들을 포함하여야 한다. a)개인의 불만과 분쟁을 해결하기에 편리한 배상청구 메커니즘 b) 정보통제자의 개인정보 처리 업무의 성실성 및 개인정보보호원칙에 부합하는 개인정보 처리업무의 이행 검증체계 c) 프라이버시보호원칙의 준수를 표명하였던 정보통제자가 이를 이행하지 않았을 때 발생하는 문제를 구제하기 위한 의무 및 그러한 정보통제자들의 원칙 준수를 보장할 수 있을 정도의 엄격한 제제 조치 등이 그것이다.

지침 26조는 정보 전송작업에 관련한 모든 상황에서 평가되어진 적절한 보안수준을 갖추지 않은 제3국으로의 정보 이전에 대한 예외조항을 다음과 같이 열거하고 있다. 첫째, 정보주체가 자신의 정보 이전에 명백히 동의하였을 때 둘째, 정보주체의 요청에 따라 채택된 계약전의 조치를 이행하기 위하여 필요한 정보이전의 경우 셋째, 정보통제자와 제3자 사이에 정보주체의 이익을 위한 계약의 체결을 위해 정보이전이 필요하거나 그 계약이행을 위하여 정보이전이 필요한 경우 넷째, 중요한 공공이익을 위하여 법적으로 요구되거나 필요할 때, 혹은 소송제기, 수행, 방어를 위해 필요할 때 다섯째, 정보주체의 중대한 이익을 보호하기 위해서 정보이전이 필요할 때 등이다. 그러므로 safe harbor 조항에 가입하지 않은 미국의 기업이라도 위의 예외조항중 한가지에 해당된다면 그 기업은 EU로부터 개인정보를 이전해 올 수 있다.

IV. 결론

EU의 개인정보보호지침은 국제적으로 많은 논란의 대상이 되고 있다. 지침은 제3국의 기업들이 EU의 소비자들에 대한 정보 이용을 금지시킴으로써 국제무역에 장애를 가져올 수 있기 때문이다. WTO에서도 아직 인터넷 프라이버시의 보호에 관한 공식적인 논의를 진행시키지 않고 있는데 그 주된 이유는 각 국가별로 이루어지는 프라이보시보호행위가 국제무역을 저해하는 요인이라고 생각하기 때문이다.

그러나 개인정보보호법은 전자상거래를 촉진시킬 수 있고 민주주의를 발전시킬 수 있다는 점에서 매우 중요하다. 그러므로 각 국가는 국제무역을 저해하지 않으면서 각 국민의 프라이버시를 보호해줄 수 있는 방안을 찾아야 할 의무가 있다고 볼 수 있으며, 이를 위해서는 첫째, 인터넷 상에서 정보주체가 알지 못하는 사이에 cookie나 log file을 이용하여 정보를 수집하는 행위를 금지시킬 수 있는 기술을 개발하는 것인데 그 한가지 방법이 기술개발을 위한 투자를 늘리는 것이다. 둘째 모든 국가가 OECD에서 제정한 프라이버시보호와 개인정보의 국제유통에 대한 8가지 지침을 근거로 국가별로 개인정보보호법을 제정하되 국가별 차이를 가능한 근소하게 하는 것이다. 셋째는 WTO와 같은 국제기구가 통일된 개인정보보호협정을 체결하여 모든 국가가 이용하도록 하는 것이다.

국가에게는 국민의 프라이버시를 보호해야 할 의무가 있으며 동시에 자유무역을 촉진시킴으로써 개별국가차원에서는 물론 세계 전체적인 후생을 증대시키기 위한 효과적인 프라이버시보호방안을 찾아야 할 의무가 있다.

참고문헌

김진아, 전자상거래의 소비자보호에 관한 법적 고찰, 전남대학교, 2000

_____, 전자상거래상의 개인정보보호에 관한 법제검토, 2000

김주환, 디지털 정보와 프라이버시 권리, http://www.privacy.or.kr/privacy_text.htm

신종철, http://www.goodcitizen.or.kr/lecture/pastlist.asp?b_code=text0014

임영형, 미국의 個人情報保護法制에 관한 硏究, http://my.netian.com/~anilink/non1.htm

정영화 전자상거래법 (제1판), 다산출판사, 2000

———외, 개인정보보호 감독기구 도입을 위한 법제개선방안연구, 한국정보보호센터, 2000

——— 전자상거래법 (제2판), 다산출판사, 2001

_____ 정보사회의 프라이버시 보호를 위한 정책과제 - 개인정보보호법률의 실현을 중심으로, http://www.privacy.or.kr/privacy_text.htm

Alan F. Westine, Privacy and Freedom, Atheneum(N.Y.), 1967

Bejot, Michel, European Treatemnt of Internet Pri acy Issues, Journal of Internet Law, 2001

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html

EC 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, http://austlii.edu.au/~graham/PLPR_EU_1.html, 1995

Edward Bloustine(1964). "Privacy As an Aspect of Human dignity," 39 New York University Law Review

EU Working party Document, "Judging industry self-regulation; When does it make a meaningful contribution to the level of a data protection in a third country?", http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp7en.html

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

Graham Pearce and Nicholas Platten, "Achiving Personal Data Protection in the European Union", Journal of Common Market Studies, Blackwell Publishers Ltd, 1998

Marc Rotenberg, The Privacy Law Source Book 1999, EPIC(Washington DC), 1999

Michael, J. Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology. Brookfield, VT: Dartmouth Publising Co., 1994

Regan, P. M., Ideas or interests: Privacy in electronic communication. Policy Studies Jouranl, 21(3, 450), 450, 1993

US Department of Commerce, The Emerging Digital EconomyII, 1999

_____, The Emerging Digital Economy, 2000

_____, Safe Harbor Overview,
http://www.export.gov/safeharbor/sh_overview.html
_____, Safe Harbor DOCUMENTS 2000,
www.export.gov/safeharbor/sh_documents.html, 2000
WTO, The WTO and Internet Privacy, GATS: Fact and Fiction, 2001
http://www.privacy.org/pi/
http://www.eco.utexas.edu/Homepages/Faculty/Norman/long.extra/information/infopolindex.html
http://freespeech.jinbo.net/white/98-2/98-2.htm#2.1