□ 프라이버시보호네트워크 제1차 정기토론회
□ 함께하는시민행동 정보사회의제만들기 제4차 토론회

프라이버시 보호를 위한 사회적 과제

일시 : 2001년 5월 24일(목) 오후 2시
장소 : 참여연대 2층 강당
주관 : 함께하는시민행동
주최 : 프라이버시보호네트워크
후원 : 벤처나눔

프라이버시보호네트워크 참여단체 : 민주사회를위한변호사모임 · 서울대지문날인거부자모임 · 서울대S카드모임 · 인권실천시민연대 · 인권운동사랑방 · 주민등록법개정행동연대 · 진보네트워크센터 · 참여연대 · 한국여성단체연합 · 함께하는시민행동

□ 프라이버시보호네트워크 제1차 정기토론회
□ 함께하는시민행동 정보사회의제만들기 제4차 토론회

프라이버시 보호를 위한 사회적 과제

일시 : 2001년 5월 24일(목) 오후 2시
장소 : 참여연대 2층 강당
주관 : 함께하는시민행동
주최 : 프라이버시보호네트워크
후원 : 벤처나눔

프라이버시보호네트워크 참여단체 : 민주사회를위한변호사모임 · 서울대지문날인거부자모임 · 서울대S카드모임 · 인권실천시민연대 · 인권운동사랑방 · 주민등록법개정행동연대 · 진보네트워크센터 · 참여연대 · 한국여성단체연합 · 함께하는시민행동

---- 목 차 ----

[기조발제-1]

정보사회의 프라이버시 보호를 위한 정책과제
- 개인정보보호법률(Privacy Act)의 실현을 중심으로-

정영화 (서경대 법학과 교수)

Ⅰ. 기본권의 본질로서 프라이버시

후기산업사회에서 정보의 대부분은 전자정보의 형태로 존재한다. 직접 대화와 수기의 메시지 이외의 어떤 통신도 전자정보의 형태를 초월 할 수 없다. 인터넷은 국가와 전세계 네트워크, 컴퓨터 기업과 통신 시스템, 전자메일, 전자게시판, 이동전화, 디지털팩스, 음성메일, 세계적인 웹서비스, 쌍방향 TV, 화상통신 등 헤아릴 수 없는 기술을 포함하는 디지털 정보혁명의 실례이다.[1] 이러한 인터넷과 무선전화기의 보급으로 프라이버시의 보호범위가 확대되고 있다. 그런 반면에 프라이버시 권리는 다양하고 광범위하게 침해되면서 정보사회의 역기능을 초래하고 있다. 예컨대, 다른 미디어 매체와 달리 인터넷은 표현의 자유의 본질과 범위에 관해서 중요한 논쟁을 불러일으켰다. 이러한 점에서 인터넷은 기존의 다른 매체들이 제공한 것 이상으로 사회규범과 사람들의 의식구조에 대해서 훨씬 직접적이고, 실질적인 영향을 미치고 있다. 이러한 정보기술이 모든 생활에 급속히 응용된 결과로 불특정 다수가 과거에는 상상할 수 없는 대량의 정보를 훨씬 저렴하고, 정확하게 처리하면서 정보유통의 메커니즘은 시간 및 공간의 물리적 한계를 해소하게 되었다.[2]

최근 미국에서의 인터넷 규제에 관한 주된 논쟁은 포르노그라피(pornography)와 인종차별 및 개인정보의 불법이용에 집중되었다. 그러나 실제로 정보통신수단을 둘러싼 법적 문제는 개인과 집단 및 국가에 의한 정보의 사유화(privatization), 유해정보의 유포, ID 절취에 의한 전자사기, 통신 및 전자메일의 도청, 저작권의 침해 등 사회적 및 경제적 이익의 권리침해에 초점을 두고 있다. 특히 정보기술의 발전으로 유전자와 DNA의 분석이 본인의 동의에 의해서 임의로 행하고 있다. 이로써 인간의 수명과 특성 및 능력유무를 심사할 정도로 인간존엄성을 명백히 위배하는 행위들이 사회 전반적으로 발생하고 있다.

오늘날 데이터나 정보처리를 위해서 컴퓨터를 이용하면서 프라이버시의 정의가 국가마다 사회문화의 배경과 정치경제력의 차이로 인해서 입법과 판례의 태도가 상이하다. 그럼에도 불구하고 개인의 프라이버시 보호를 위해서 규제방법과 그 효과에 대한 논쟁은 정부규제와 자율규제 및 시장규제의 방식으로 제

1) Fred H. Cate, Privacy in the Information Age, Brookings Institution Press, 1997, p.7.
2)자세한 내용은 정영화, "정보법령의 법이론(The Jurisprudence of Information Codes)", 세계헌법연구 제5호, 국제헌법학회 한국학회, 2000. 10, p. 258 이하 참조,

시하고 있다.3)

그런데 대다수 프라이버시에 관한 논쟁에도 불구하고 견해가 통일되지 못한 이유는 프라이버시의 정의가 다르기 때문이다. 그럼에도 불구하고 프라이버시 개념이 카멜레온(Chameleon)과 같이 그 배경과 맥락에 따라서 매우 다양한 의미를 갖을지라도 놀라운 일이 아니다. 본래 프라이버시는 그 사회의 정치경제 및 법문화의 배경에 따라서 보호정도를 달리하기 때문이다. 예컨대 제1세계 국가에서는 타인의 프라이버시에 대한 관념이 일반적이고 보편적으로 존중되는데 반해서 제3세계의 국가에서의 프라이버시는 일종의 사치품과 같이 부유한 계층의 전유물과 같이 인식하는 경향이 있다는 점이다.4)
이하에서는 프라이버시의 정의에 관해서 살펴보기로 한다.

II. 프라이버시 권리의 해석구조

1. 프라이버시의 사인간의 직접적인 효력

인권의 국제적인 목록에서 프라이버시가 가장 정의하기 어려운 용어라고 본다. 프라이버시의 정의는 인간의 존엄과 가치, 표현의 자유, 결사의 자유, 통신의 자유, 거주의 자유 등 다수의 인권과 직접적으로 관련되므로 그 맥락에 따라서 다양한 의미를 갖는다. 인권에 대한 통일된 정의가 곤란할지라도 역으로 그의 중요성이 반감되는 것은 아니다.

헌법상 프라이버시 권리는 인간존엄과 가치의 실질적 보장인 일반적 행동자유와 일반적 인격권 중에서 후자에 해당한다. 프라이버시 권리는 정보자기결정권을 본질적인 내용으로 정하고 있다고 해석한다. 그런데 현행 헌법의 프라이버시 권리는 제10조의 인간의 존엄과 가치, 제17조의 사생활의 비밀과 자유, 제16조의 통신의 자유, 제18조 거주이전의 자유의 구조와 같이 각기 자유권의 방어적 권리로 이해하고 있다. 특히 정보자기결정권은 인간의 존엄권의 한 요소인 동시에 계약에 의한 임의의 개인정보의 처분과 수집 및 이용 그리고 사용등을 결정한다는 점에서 중요하누 의의를 갖는다.

한편, 오늘날의 프라이버시 권리는 모든 인권의 공통요소를 갖는 인권의 본질적인 특성을 보이고 있다.5) 통신기술의 발전으로 종래 전화, 팩스가 인터넷과 결합되면서 정보 프라이버시로 확대되고, 더구나 인터넷은 무선방송이나 TV(위성방송)와 통합되어서 종래의 통신비밀은 그 실체를 이해하는데 통신 프라이버시의 문제를 제기하기 때문이다. 여기서 프라이버시 개념은 개인정보의 취급과 관련하여 해석되는 데이

3) 이는 인권보호와 정보시장의 활성화의 상충관계(trade-off)에 있다(정영화, 전자정부에서의 공공정보의 접근 및 유통에 관한 법정책연구, 공법연구 제26권 제2호, p.308-310 참조). 때문에 그 국가나 사회의 법문화와 웹이용자의 규범의식 등에 관해서 실증연구를 요하는 중요한 문제이다. 이에 대한 선행연구로서는 Lorrie Faith Cranor and Joseph Reagle and Mark S. Ackerman, Beyond Concern: Understanding Net' Users' Attitudes about Online Privacy(AT&T Labs-Research Technical Report Tr 99.4.3) 등이 있다.
4) 정영화, 현대 헌법학에서 프라이버시법리의 재검토, 사이버커뮤니케이션 제7호, 사이버커뮤니케이션학회, 2001.5, 참조
5) Volio Fernando, "Legal Personality, Privacy and Family" in Henkin(ed), The International Bill of Rights, Comlombia University Press, 1981

터 보호와 결합되고, 엄격한 의미의 프라이버시 보호는 사회가 개인적 비밀을 어디까지 관여할 수 있는가? 문제로 해석된다.

다른 한편, 종래 프라이버시에 대한 효력은 국가의 공권력에 의한 침해가 주된 형태였으나, 오늘날에는 사인과 민간단체 등에 의한 침해가 보다 심각한 상황에 놓여있다. 예컨대 정치적 목적이나 반정부 인권운동단체 등에 대한 도청과 비밀 감시행위는 정부기관에 의해서 행하는 것이 아니라, 민간정보조사업체에게 자금을 제공하여 업무의 외주형태가 일반적인 현상이다. 더구나 제1세계의 비약적인 정보통신기술을 제3세계의 정부들에 의해서 기술이전이 급속히 이루어지기 때문에 광범위하고 다양한 형태의 개인정보침해가 용이한 실정인 것이다. 따라서 프라이버시의 침해는 국가 공권력과 사인에 의한 직접 침해가 일반적으로 발생하고 있기 때문에 프라이버시 권리에 대한 사인간의 직접적인 효력문제의 해결방안이 논의의 초점인 것이다.

2. 프라이버시의 정의와 패러다임

오늘날 전세계적으로 법집행 기관과 기업들이 인체의 유전정보, 사적 개인정보, 인터넷에 의한 통신정보 및 위성을 통한 불법검열과 감시가 행해지면서 개인의 프라이버시에 대한 사망선고를 예고하고 있다. 이러한 프라이버시의 사망은 결국 민주주의를 포기하는 사태와 기술에 의한 인권침해를 당연한 결과로 수용하는 위험사회로의 종말을 초래할지도 모른다. 여기서 프라이버시 개념의 정의에 대해서는 다음과 같이 다양한 입장을 검토할 수 있다.

첫째, L. Brandeis는 개인의 "혼자 있을 권리"(right to be left alone)로 이해하여, 민주주의에서 가장 중요한 자유로서 헌법에 반영되어야 한다고 주장하였다.6)

둘째, Alan Westin는 프라이버시는 어떠한 환경에서든지 자신의 신체, 태도와 행위를 타인에게 얼만큼 노출실 수 있는가는 자신의 자유롭게 선택할 수 있는 자유라고 파악하였다.7)

셋째, Edward Bloustine는 프라이버시란 인간의 인격권의 법익이므로 인격의 침해, 개인의 자주성, 존엄과 완전성을 보호하는 것이라고 한다.8)

넷째, Ruth Gavison는 프라이버시의 세 가지 요소로서 비밀(secrecy), 익명성(anonymity), 고독(solitude)을 갖으며, 그것이 자신의 선택에 의해서 또는 타인의 행위에 의해서 상실할 수 있는 상태를 말한다고 한다.9)

다섯째, 영국의 Calcutt Committee에서는 프라이버시의 만족할 수 있는 법률 규정은 찾아보기 어렵기

6) Samuel Warren and Louise Brandeis, "The Right to Privacy," Harvard Law Review 4, 1890, pp.193-220
7) Alan F. Westin, Privacy and Freedom, Atheneum(N.Y.), 1967, p.7
8) Edward Bloustine, "Privacy as an Aspect of Human Dignity," 39 New York Univ. Law Review, p.971(1964).
9) Ruth Gavison, " Privacy and the Limits of Law," Yale Law Journal 421, 1980, p.428.

때문에 "개인의 생활과 일거리 또는 그의 가족의 생활과 일들을 직접 물리적인 수단이나 정보공개에 의해서 침해되는 것을 방지하는 권리로 선언하였다. 호주의 프라이버시 헌장의 서문에는 "자유로운 민주사회는 개인의 자주성을 존중하며, 그러한 자주성을 침해하는 국가나 사적 단체의 권한을 제한하며, 프라이버시는 인간존엄의 본질과 결사 및 표현의 자유의 핵심 가치이다. 이는 기본적인 인권으로서 모든 인간의 합리적인 기대이다.

여섯째, 프라이버시의 주체를 식별할 수 있는 개인정보를 대상으로 한다. 이러한 개인정보가 그 주체에게 사적으로 특별히 민감하고, 당혹감을 줄 수 있는 경우는 말할 필요가 없고, 비록 그 정보가 평범하거나 사소한 것이라도 그 주체의 의사에 반한 것으로 추정되는 경우에는 프라이버시의 보호대상에 해당한다.[10]

III. 국제 프라이버시조약

1. OECD

Privacy Guideline(1980)의 적용에 관한 8 원칙을 정하였다.

① 데이터 수집제한의 원칙- 개인 데이터는 적법하고, 공정한 방법으로 필요한 경우에 당사자의 동의를 얻어서 수집이 제한되어야 한다.
② 데이터 특성의 원칙-개인 데이터는 사용목적과 그 목적에 필요한 범위 안에서 정확하고, 최신의 정보에 부합하여야 한다. 즉 데이터가 사용되는 목적에 관련되어야 한다는 점이다.
③ 목적 특정화 원칙- 이는 데이터의 특성과 데이터 사용제한의 원칙과 긴밀하게 관련된다. 수집되는 개인 데이터는 수집 당시에 특정되어야 하고, 목적 실현에 제한되어야 한다. ④ 사용제한 원칙- 개인 데이터는 주체의 동의와 법령에 의한 경우를 제외하고, 공개되거나, 특정한 목적이외 다른 용도로 사용되지 아니한다.
⑤ 비밀보호의 원칙- 개인 데이터는 불법적인 접근이나 파괴, 사용, 데이터 수정과 공개의 위험에 대비하여 합리적인 비밀보호의 조치가 적용되어야 한다.
⑥ 공개의 원칙- 개인 데이터에 대한 발전이나 관행 및 정책에 관해서 일반적 공개정책이 확립되어야 한다.
⑦ 개인참여원칙- 개인은 다음과 같이 데이터 관리자에게 자신에 관한 데이터를 보유하고 있는지 여부를 확인할 권리를 갖는다. 그에게 상당한 기간안에 그가 즉시 알 수 있고 또한 타당한 방식으로 과도한 비용부담이 없이 그에 관한 데이터를 통지받는다. 상기의 요청을 거부하는 이유와 그러한 거부에 이의를 제기할 수 있는 권리를 갖는다. 그러한 이의가 정당한 경우에는 그에 관한 데이터의 삭제, 수정, 종료하는 권리를 갖는다.
⑧ 책임성 원칙- 데이터 관리자는 상기의 원칙이 적용되는 조치에 부합하도록 책임을 진다.
이러한 개인데이터의 보호원칙은 국가적으로 해결되기 어려운 문제이므로 국제적인 데이터 이동의 증대를 고려하여 국제적인 데이터 은행의 창설에 초점을 두었다.

10) 정영화, "사이버스페이스와 프라이버시" 헌법학연구(제6권제3호), 한국헌법학회, 2000.10, 51-53면.

2. EU 조약

오늘날 개인정보는 정부보유의 개인정보와 민간기업이나 단체 보유의 개인정보, 자동처리의 데이터와 수동처리의 데이터, 개인정보(personal information)와 비개인정보(non-personal information), 상업목적의 데이터와 비상업목적의 데이터 등의 구분기준에 따라서 다양한 유형이 존재하고 있다. 그리고 프라이버시의 구조는 개인의 데이터의 수집과 보관하는가에 의해서 공적부문과 민간부문으로 이분할 수 있으며, 또한 그 데이터가 디지털 또는 아날로그 형태이냐 여부와 데이터의 접근과 이용이 On-Line 또는 Off-Line 중 어디에서 이동하는가에 따라서 법적 보호범위와 한계가 각기 구분될 수밖에 없는 것이다. 그런데 유럽이사회가 1981년에 제정한 Council of Europe Convention on Privacy 협약은 데이터보호의 기본원칙을 다음과 같이 제시하였다. ① 회원국의 의무- 국내법의 시행의무, ② 데이터의 성질- 자동처리의 개인데이터는 적법하고 공정하게 수집, 처리되고, 특정하고 적법한 목적으로 저장되며, 그 목적에 부합하지 않는 방법으로 사용하지 못한다. 저장목적이 비례원칙에 부합하여야 한다. 저장목적을 초과하는 기간동안 보유할 수 없다. ③ 데이터의 특별한 분류원칙은 인종과 정치신념, 성생활이나 형벌기록과 같은 민감한 개인데이터를 국내의 적절한 보호장치가 없이 자동처리를 금한다. ④ 데이터 주체를 위한 추가적인 보호장치로서 자신의 개인데이터에 관해서 과도한 지연이나 비용을 부담하지 않고 용이하게 확인할 수 있어야 한다. ⑤ 예외와 제한 원칙은 국가안보, 공공보호, 국가의 금융상 이익, 범죄예방을 예시하고 있다. ⑥ 제재와 구제원칙은 이러한 기본원칙을 시행하는 국내법의 위반행위에 대해서 적합한 제재와 권리구제를 마련하여야 한다. ⑦ 보호의 확대로서 이 협약이 정한 보호조치보다 회원국의 보호조치가 데이터 주체에게 제한하여 해석하거나 시행할 수 없다.

더구나 유럽연합은 1995년에 European Union Data Protection Directive에 의해서 1998년까지 회원국의 프라이버시에 관한 국내입법을 동 협약의 수준으로 상향조정을 결정하여 오늘날 유럽연합의 전체 회원국은 프라이버시보호입법을 시행하고 있다.[11] 따라서 동 협약의 개인데이터 처리의 적법성의 일반규칙(General Rules on the lawfulness of the processing of personal data)은 다음과 같다.

① 데이터 특성에 관한 원칙(principles relating to data quality)
② 적법한 마케팅 데이터처리의 근거에 관한 원칙(Principle relating to the reasons for marketing data processing legitimate)
③ 데이터 처리의 특별한 분류(Special Categories of processing)
④ 데이터주체에게 통지할 정보(Information to be given the data subject)
⑤ 데이터 주체의 데이터접근의 권리(The data subject's right of Access to data)
⑥ 면제와 제한(Exemption and Restrictions)
⑦ 데이터주체의 반대할 권리(The data subject's right to object)
⑧ 데이터처리의 비밀과 안전성(Confidentiality and Security of Processing)
⑨ 통지(Notification)
⑩ 법적 구제, 책임과 형벌(Judicial Remedies, liability and Penalties)

11) 자세한 내용은 당므 문헌을 참조. 정영화 외, 개인정보감독기구의 도입을 위한 법제개선방안 연구, 한국정보보호센터, 2000.11(연구과제보고서).

⑪ 제3국으로 개인데이터의 이전(Transfer of Personal data to third Countries)
이상과 같은 기본원칙을 유럽연합의 회원국에서 프라이버시법제는 국내법의 차원에서도 독립국가기구로서 개인정보감독기구를 축으로 운용하고 있다.

3. 소 결

대다수 국가의 프라이버시 보호의 법제의 형태를 보면, 공적부문에 있어서는 정보공개법(Freedom of Information Act)에 의해서 규율되는 반면에, 민간부문의 법제는 공공부문의 법제에 비해서 다소 늦게 최근에 입법화되고 있다. 그 이유는 인터넷 이용의 보편화와 전자상거래의 활성화를 위해서 선결조건이 되기 때문이다.[12] 즉 민간부문의 개인정보보호의 법제는 종래의 법질서하에서 헌법과 민법 및 형법 등에 의해서 사후구제를 위한 명예훼손과 불법행위책임을 통해서 제한적으로 보호되어서 일반적인 규제를 위해서는 별도의 입법이 필요하게 되었다. 적어도 그 원인은 프라이버시의 보호법익이 국가에 대한 개인의 주관적인 공권에 한정되지 않고, 사인간의 침해로 인해서 프라이버시의 직접 효력을 인정하지 않을 수 없기 때문이다. 따라서 민간부문에 있어서 프라이버시의 보호법제는 공적부문과 별도로 제정되었다가 점차 양자의 법제가 통합되고 있다는 점을 이해할 수 있다. 최근의 각국의 프라이버시의 보호법제의 특색은 공적부문과 민간부문의 개인정보보호를 위한 법집행기관이 통일되거나 또는 프라이버시의 침해에 따른 권리구제의 방식도 전통적인 법원재판의 보충하여 당사자주의에 의한 분쟁조정과 화해방식을 널리 채택하는 추세로 나타나고 있다.

Ⅳ. 프라이버시 보호입법의 동향

국내에 소개된 프라이버시 보호입법에 관한 연혁은 대부분 미국 브랜다이스 대법관의 1890년에 발표된 프라이버시 논문이 주요한 문헌으로 소개되었으나, 사실 세계 최초의 프라이버시 입법은 1361년 영국의 입법으로 알려져 있다. 특히 서구의 중요한 프라이버시 보호입법의 사례를 아래와 같이 살펴 볼 수 있다.

1. 세계 각국의 입법례

ⓐ 영국: law against peeping toms and eavesdroppers(1361년 입법), 판례; Entick v. Landmark(1765)
ⓑ 스웨덴(Sweden): Access to Public Records Act(1776)
ⓒ 프랑스(France): Trot of Privacy(1858)
ⓓ 미국(USA): Louis Brandeis(1890) The right of privacy–as the right to be let alone(Olmstead v. U.S. 277U.S. 438,478(1928)이 관련 판례가 있다. 이후에 컴퓨터에 의한 정보처리와 개인정보의 보관이 가능하게 되면서 수시로 개인정보보호에 관련한 법률 등이 아래와 같이 시행되고 있다. "Fair Credit Reporting Act"(1970), "Privacy Act"(1974), "Freedom of Information Act"(1974), "Family Educational rights and Privacy Act"(1974), "Right to financial Privacy Act"(1978), "Privacy Protection Act"(1980), "Cable Communications Policy Act"(1984), "Electronic Communications Privacy Act"(1986), "Video Privacy

12) 정영화, 전자상거래법, 다산출판사, 2000.9, 참조.

Protection Act"(1988), "Employee Polygraph Protection Act"(1988), "Telephone Consumer Protection Act"(1991), "Driver's Privacy Protection Act"(1994), "Telecommunications Act"(1996,Excerpt), "Children's On-Line Privacy Protection Act"(1999), "과 같이 다양한 프라이버시 법률을 시행하고 있다.

2. 국제사회의 법제동향

개인의 프라이버시 보호에 관한 국제입법동향은 개별국가의 관련 입법에 직접적인 영향을 미치고 있는데, 그 중에서 중요한 국제사회의 법제만을 살펴보면 다음과 같다.

첫째, 세계인권선언(1948년, Universal Declaration of Human Rights)에서 프라이버시의 권리의 보호를 선언하고 있다. 유엔은 1990년 컴퓨터 처리의 개인화일 규율의 가이드라인(UN Guideline for the Regulation of Computerized Personal files,1990)을 제시하였다.

둘째,OECD는 프라이버시 가이드라인(OECD Privacy Guideline,1980)과 자동처리의 개인정보보호에 관한 협약(Convention for the Protection of Individuals with regard to the automatic processing of personal data,1981), OECD Guidelines governing the Protection of Privacy and transborder Data Flows of Personal Data(1981), 암호가이드라인(OECD Cryptography Guideline,1997), 글로벌네트워크에서 프라이버시보호의 정부간 선언(Ministrial Declaration on the Protection of Privacy on Global Networks,1998)이 있다.

셋째, 유럽연합은 프라이버시 협약(Council of Europe Convention on Privacy, 1981), 유럽 데이터보호지침(European Union Data Protection Directive, 1995), 유럽연합 전화통신부문의 프라이버시 보호지침(European Union Directive for the Protection of Privacy in the Telecommunications Sector, 1997), 인터넷의 익명성(Anonymity on the Internet, 1997), Recommendation on the Respect of Privacy in the Context of Interception of Telecommunications(1999) 등이 있다.

한편, 이러한 미국과 유럽연합의 프라이버시 입법동향에 따라서 다수의 국가들은 헌법상의 프라이버시의 법적 해결을 위해서는 전통적인 사법상의 불법행위 및 명예훼손의 법리만을 의존하는 경우에 직면하는 법집행의 과정과 적용법률의 한계로 인해서 근본적인 권리구제의 수단과 절차가 필요하다는 점을 인식하고 있다. 왜냐하면 기존의 법집행 방식은 가해자와 피해자간의 정보의 비대칭성으로 인해서 당사자간의 입증책임분배와 피해의 원상회복을 기대할 수 없음에도 불구하고 정신적 피해에 대한 위자료산정의 기준이 지극히 낮다는 점을 들 수 있다.

다른 한편, 재판상의 권리구제방식은 피해사실의 공표와 소송경제상의 비용과 시간등의 과도한 거래비용을 수반한다는 점이다. 신기술에 의해서 개인의 유전자 정보에서 공개적인 표현 등에 걸쳐서 다양한 사적 사항이 완전히 침해될 수 있다는 사실에서 익명성을 보장하고, 신속하고 편리한 권리구제방식이 재판구제방식을 대체할 수 없는지의 문제가 제기되고 있다. 이제는 개인의 정보를 컴퓨터나 전자기기에 의해서 대량으로 신속하게 수집과 분석 및 가공 그리고 이전할 수 있다는 점에서 첨단의 기술력을 가진 공권력과 사회단체에 비해서 상대적으로 열등한 정보역량을 가진 개인의 법적 지위를 강화하는 것이 당연한 법리로서 요청되었다. 따라서 현재 PC에 의한 정보처리나 가상공간의 폭발적인 이용사태는 개인정

보의 이슈가 단순히 개인의 권리구제의 차원을 넘어서 국가와 사회의 공동의 공적문제로 논의되었고, 더구나 전자상거래와 관련해서는 국가간의 정치경제와 외교상의 쟁점사항으로 대두되고 있다는 점이다.

Ⅴ. 프라이버시의 유형과 보호영역

1999년 12월 21일 AOL과 Time Warner사간의 합병계약으로 약 1조6600억$로 기업의 경제적인 규모가 확대되었다. 이는 온라인의 기업과 오프라인의 기업간의 상호간의 정보결합에 의한 시장창출의 가능성을 시사하는데 실제는 Time Warner사가 AOL이 가진 온라인상의 개인정보를 활용하여 시장과 상품의 개발에 따른 시너지 효과를 기대한 것이다. 그런데 이러한 온라인 기업과 오프라인의 미디어 기업간의 결합효과를 반감시키는데 충격을 준 사건이 같은 날 Maxus라는 해커(Hacker)가 CD Universe사의 웹사이트(WebSite)에 침입하여 그의 고객 300,000명의 신용카드의 번호와 패스워드 파일을 절취한 사건이 발생하였다.,

한편, 오늘날 전자상거래의 활성화를 주도하고 있는 미국과 유럽국가 등은 2003년에 전자상거래의 세계시장규모를 3조 2천억US$(미국시장규모는 1조$) 추산하고 있다. 이는 1998년의 세계 시장규모인 810억$의 약 40배 증대할 것으로 예상한다. 그런데 전자상거래에서는 소비자들이 온라인 구매를 거부하는 이유를 보면, 네트워크의 안전성의 장해에 대해서(68%), 물품의 배송상의 문제를 이유(58%), 타인의 개인정보 침해(55%), 판매자의 신용문제(54%), 물품의 차이(49%), 기타 이유(20%)로 응답하였다.[13] 물론 선진국들은 전자상거래를 활성화하여 새로운 시장확대와 고용창출을 위한 최대 이점으로 인식하기 때문이다.

1. 프라이버시의 유형

오늘날 개인의 프라이버시는 신문과 유선 및 무선방송 또한 인터넷과 위성 TV의 통합과정에 있기 때문에 종래의 매체를 중심으로 개별적인 프라이버시의 보호법제와 달리 점차 통합되는 특성을 보이고 있다. 부연하면, 전통적인 송신자와 수신자 모델은 정보의 유통경로에 초점을 두기 때문에 미디어의 제도적 기능과 역할을 강조하게 되었다. 또한 정보와 수신자 모델은 수신자가 정보의 내용에 대한 인지와 해독이 중요하기 때문에 인격권 및 재산권의 이원적인 속성에서 데이터의 지적재산의 특성을 강조한다. 그리고 통신행위 모델은 통신행위와 관련되는 행위자의 목적과 의사에 따라서 정보의 가치와 속성이 결정되므로 사적 법익과 기업비밀 및 국가이익의 경합과 우열로 인해서 개인정보의 프라이버시 보호의 한계에 직면할 수 있다.[14]

우선 개인적 보호법익으로서 프라이버시의 유형은 개인정보(personal information)와 비개인정보(nonpersonal information)로 구별할 수 있다. 즉 개인정보는 프라이버시의 주체를 식별할 수 있는 정보를 의미한다. 이는 특정인의 정보를 제3자에게 전송하기 위한 의도적으로 창출하는 작성자가 존재하여야 한다. 또 프라이버시의 데이터는 그 개인의 경제사회 및 생물학 등의 다양한 측면에서 사회적으로

13) 정영화, 전자상거래법, 다산출판사, 2000, p.108 참조.
14) 정영화, "정보법령에 관한 법이론," 세계헌법연구(제5권), 국제헌법학회 한국학회, 2000.10, p.285 이하 참조.

지속되는 지위를 설명하는 요소를 포함한다. 예컨대 생리적 특성으로서 성별, 신장, 체중, 혈액형, 지문, 홍채의 형태, 건강진단의 내용, 유전자와 DNA 등, 또 사적 사항으로서 혼인여부, 생일, 성적 취향, 가족관계, 학력과 전과기록, 병력사항, 납세 및 소유재산의 내역, 종교유무와 거주지의 주소 등, 정치 및 사회단체의 참여여부, 등이다. 그리고 그 사회의 제도적인 개인식별의 증명수단으로서 주민등록증 및 그 번호, 사회보장카드와 그 번호, 생활보호대상자 카드, 의료보호대상자 카드, 특정직업종사자의 건강증명과 같은 각종 개인식별의 수단이 제도적인 신원증명에 해당한다.

그런데 문제는 이러한 개인신원의 증명수단을 제한된 이용목적에 한하여 적용되어야 함에도 하나의 증명수단이 다양한 행정목적과 필요성에 의해서 광범위하게 적용하는 경우에는 최소한의 이용목적에 반하는 결과로 인해서 모호하게 되어서 프라이버시의 보호목적에 반하는 결과를 초래함으로 위법하거나 위헌성의 문제를 야기하게 된다. 예컨대 현행 주민등록증 제도는 개인의 모든 공적 및 민간 부문의 생활영역에 걸쳐서 개인의 프라이버시가 침해되는 결과를 초래하고 있다. 즉 주민등록증은 위(변)조가 가능하고, 이는 행정과 금융 및 모든 거래에서 개인의 동일성을 광범위하게 식별하는 수단으로서 개인의 출생과 사망시점까지 불변하고, 고유성을 내포하고 있다. 이를 제3자가 도용하거나 모용하는 경우에 거의 모든 생활영역에 걸쳐서 공적 및 사적인 신용과 신뢰를 회복하기가 거의 불가능한 상태에 처하게 됨에도 여전히 제도적 모순을 개선하지 못하고 있음은 매우 유감스러운 일이다. 부연하면 현행 주민등록제도는 데이터의 고유성과 불변성 및 적용의 무제한성으로 인해서 개인의 식별수단으로서 지나치게 광범위하고 또한 일회적인 침해로써 원상회복이 불가능한 인격권의 본질적 침해를 우려하지 않을 수 없다. 따라서 프라이버시 인권에 대한 광범위하고 과잉침해 가능성은 법치주의 비례원칙에 위배되기 때문에 시급히 개선이 요망된다. 특히 우리 나라의 가상공간의 대부분은 이용자의 개인정보로서 주민등록번호와 주소 등에 관해서 공개를 요구하는 현실에서는 매우 위험한 사태가 계속 발생할 수밖에 없다. 최근 은행 내부자가 예금자의 개인정보를 무제한적으로 침해할 수 있는 상황과 마찬가지로 언제나 해킹 가능한 상황에서 대규모의 은행예금의 불법적인 이체가 내부자 및 외부자에 의해서 발생할 수 있음을 시사하였다. 왜냐하면 예금자의 주민등록번호를 불법으로 이용해서 금융전산망에서 그의 예금자산을 확인하면, 그의 비밀번호와 예금계좌번호를 절취해서 불법적인 예금이체가 가능하다. 결국 인터넷의 이용자의 개인정보인 주민등록번호의 공개는 법적으로 제한하여야 할 것이다. 적어도 네트워크 접속에 필요한 이용자의 ID나 패스워드(password) 또는 CD기의 자동처리를 위한 패스워드는 중요한 개인정보로서 특별한 법적 보호조치가 필요하다. 따라서 이러한 정보는 은행과 증권 및 보험회사 또는 행정청 등 개인정보의 관리조직의 내부에서도 접근제한을 위한 법적 제한조치가 수반되지 않으면 정보사회의 신뢰성이 붕괴되고 말 것이다.

다음으로 비개인정보(nonpersonal information)는 그 개인의 데이터의 익명성으로 인해서 특정한 개인을 식별하기 어렵고 또는 추적이 곤란한 정보를 의미한다. 물론 비개인적 정보는 외견상으로 프라이버시의 침해의 우려가 없을지라도 법집행 과정이나 미디어에 의해서 익명성이 보장된 피의자나 피고인 등의 진술도 전체적으로 식별이 가능하다는 점이다. 또한 정신과 치료의사가 자신의 특정한 환자의 임상치료과정과 그 결과에 관해서 익명으로 출간할 경우에도 개인정보의 보호대상에서 제외되는 것이 아니라는 점을 분명히 인식하여야 한다. 오늘날 가상공간의 이용이 급증하면서 이러한 비개인정보는 그 범위가 훨씬 제한되고 있기 때문에 단순히 개인정보만으로 식별이 곤란할지라도 다른 관련 정보와 결합됨으로써 식별될 수 있다는 점을 유의하여야 한다. 따라서 단체에 관련되는 정보에 있어서는 그의 비중이 조직의 규모나 특성 및 하위조직에 있을 경우에는 개인정보와 유사한 것으로 이해함이 타당하다고 본다.

2. 프라이버시의 보호영역과 한계

인터넷 이용은 대량 정보의 처리와 유통이 신속하고, 공간의 장애를 해소하여 쌍방향으로 증대되고 있다. 오늘날 각국은 개인정보의 보호대상에 관해서 공통적인 대상을 설정하고 있는 추세를 보이고 있다. 이는 개인정보의 보호객체가 정보기술의 적용에 따라서 동일한 범위로 점점 보편화되고 있는 현상을 나타내고 있음을 알 수 있다. 그러한 프라이버시의 보호대상을 다음의 네 영역을 중심으로 해당하는 문제를 검토하고자 한다. 물론 이러한 프라이버시의 보호영역은 개인의 인권을 보호하는데 기준을 두고 있지만, 경우에 따라서는 기업의 비밀과 국가이익과 충돌하는 까닭으로 공권력의 제한이 어떤 요건과 절차에 의해서 허용할 것인가의 프라이버시의 보호의 한계와 직접적으로 관련하여 검토하여야 할 것이다.

(1) 정보 프라이버시(Information Privacy)

이는 종래의 공적부문과 민간부문에서 개인정보의 데이터의 수집과 취급에 관련하여 법령을 근거해서 운용하는 개인정보를 포함한다. 우선 공공기관이 수작업이나 컴퓨터에 의해서 수집과 관리 및 이용하는 개인정보가 주요 대상이다. 먼저 행정기관이 시민의 개인정보를 수집하고, 관리하는 경우에는 디지털 형태이든지 아날로그 형태이든지 관계없이 모든 개인정보에 대한 접근과 이용에 대한 법적 규율이 전제되어 있다. 예컨대 현행 주민등록법에서 정하는 일반적인 행정정보에 관련되는 성명, 주민번호, 주소, 전화번호, 생년월일, 출생지, 본관, 취미와 특기, 국적, 가족관계, 교육과 직업훈련에 관한 정보로서 최종학력과 학적사항, 자격증, 상벌관계, 병역정보로서 계급, 병과와 병종, 특기부여, 군번 등이 있다. 재산사항에 관한 등기내역으로서 동산과 부동산의 내용과 채권 및 지적재산권의 내역, 과세목록과 내역에 관한 내용, 각종 소득정보로서 연봉, 소득세의 징수내역과 납세실적 등, 보험가입과 부대수입 등 그리고 고용정보로서 사업주나 고용관계 및 근무평가기록 등이 있다. 특히 중요한 개인정보는 금융신용기관의 신용정보로서 은행예금과 거래내역, 증권회사 고객의 증권계좌와 주식거래 내역 등, 신용카드회사의 고객의 신용정보와 결제내역 등이다. 또한 병원이나 의료기관의 환자의 병력과 진료내역 등의 개인정보와 의료기관이나 의료보험공단 등이 관리하는 병력과 진료기록 및 치료과정의 자료 등이다. 또한 정부가 기록하고 보관하는 범죄인의 개인기록으로서 전과자료, 범죄특성의 기록, 그리고 혼인관계와 성적 취향에 관한 기록이나 경력의 자료 등이 이에 해당하는 개인정보로서 민감한 사안에 관련된다고 본다. 이러한 개인정보는 관리주체에의 접근과 열람에 위해서 침해될 수 있으므로 객관적인 물건의 형태로 존재할 뿐이고, 가해자의 의사와 동작에 의해서 구체적인 행위를 매개하여서 침해되며 또한 외부자의 침입보다는 내부자의 불법적인 유출에 의하여 침해되는 까닭에 조직내부의 개인정보에의 접근을 엄격하게 법적으로 규율하는 것이 무엇보다도 중요한 관건이다.

(2) 통신 프라이버시(Communication Privacy)

통신 프라이버시는 오늘날 통신기술의 발전에 따른 부작용으로서 빈번하게 발생하는 문제이다. 이는 우편·유선전화·이동전화(mobile phone), E-mail 및 인터넷의 통신수단을 매개하여 수집과 분석 및 가공되는 개인정보로서 새로운 기술을 이용하기 때문에 데이터의 움직임을 전제한다. 따라서 가해자는 개인정보의 침해의사를 가지고 이동하는 데이터에 대한 접근에 의해서 개인정보를 도청하거나 검열하는 까닭에 그 기술력에 의해서 침해범위가 결정되는 특성을 나타낸다. 현재 가장 치열한 논쟁의 대상이 되고

있는 통신 프라이버시는 국가이익이나 군사기밀 또는 기업비밀을 보호하기 위해서 정보기관이나 대기업에 의해서 E-mail의 검열과 voice-phone의 도청이 일반적으로 행해지고 있는 형편에 있어서 이에 대한 거부감이 가장 높게 나타나고 있다. 이러한 통신 프라이버시의 침해도 당해 개인의 동의가 필요하기보다는 적법절차에 의한 절차적 정의의 문제가 중요한 이슈가 될 수 있다.[15] 부연하면, 전통적인 서류의 기록, 전화통화, 하드디스크(hard disk) 또는 디스켓에 저장한 데이터에 대한 강제수사가 필요할지라도 법원의 영장발부가 필요하다. 반면에, 공권력에 의한 전자메일의 제한은 인터넷 시스템 운영자인 웹마스터(web-master), 시삽(sysops)에게 규제권한이 행사되기 때문에 정보관리자로서 정보나 자료의 제출영장이나 명령에 대응하여 합리적인 정책이 필요하다. 대개 운영자들은 실제 접근가능한 정보만을 전자게시판을 통해서 다수인에게 공개하고 있으며, 이용자와의 계약조건에 의해서 이행하되, 본인의 동의나 법원의 영장에 의해서 데이터의 공개가 가능하기 때문에 엄격한 적법절차의 요건이 부과된다고 해석한다. 그러나 기업들은 자산의 관리주체로서 고용인들의 전자메일에 대해서 검열하고 있으나, 이는 표현의 자유에 대한 중대한 침해라고 하지 않을 수 없다. 적어도 이를 위해서는 내부의 규약과 적법한 절차적인 요건에 의해서 사업주의 임의의 검열이나 열람이 제한되어야 한다.

(3) 신체상의 프라이버시(Biometrics Privacy)

유전자 정보(genetic tests), DNA tests, Drug testing, Cavity searches 등은 일반적으로 행해지는 인체상의 중요한 정보를 수집하는 작용임에 없다. 이 인체의 본질에 접근한 개인의 유전적인 특성과 비밀은 종래의 공권력만이 아니라 민간세력에 의해서도 요청되고 있다. 이는 DNA나 유전자 데이터베이스가 훨씬 일반화되면서 사업주가 시험을 위해서 널리 사용하는 공통수단이 되고 있다. 유전자 테스트가 비록 직업병의 예방을 위해서 합법적일지라도, 고용주가 현재 또는 장래의 종업원을 차별하기 위해서 이러한 유전자 테스트를 이용하는 것은 심각한 위험을 야기할 수 있다. 법적 개입이 없이 고용주가 종업원의 질병이나 직무태만 등의 경향이 있는지 여부를 식별하는 정보가 종업원을 차별하는데 이용될 수 있다. 유전자 테스트는 개인의 인격을 구성하는 핵심요소(hard core)에 관련되는 프라이버시의 외적 침해이다. 더구나 이 테스트는 당해 개인만이 아니라 그의 가족이나 집단 및 인종 차별을 초래할 수 있다. 일정한 유전 조건은 특정한 인종이나 혈족집단을 시사하고 있다. 예컨대 적혈구 빈혈증은 미국의 아프리카인들에게는 유전병이고, 유방암의 발병은 동유럽 거주의 유태인의 유전병으로 나타내고 있다.[16] 최근 미국의 경영학회지에 의하면, 기업들의 15%가 종업원의 직무태만의 의심을 테스트하거나 유전자 테스트를 수행하고 있는 것으로 보고되고 있다. 이러한 유전자 테스트의 위험성을 인식하여 다수의 국제적인 단체들이 직장에서의 유전자 테스트의 시행을 법으로 제한할 것을 권장하고 있다. 1989년 유럽의회는 종업원의 동의를 받지 아니하고 고용인의 선발이나 시험할 목적의 유전자 테스트를 금지하는 법제정을 권장하는 결의를 하였다. 2000년 5월에 세계의학협회는 건강정보의 데이터베이스의 개발에 관한 가이드라인을 채택하여서 프라이버시, 동의, 개인의 이용접근 및 책임의 이슈를 발표하였다. 아직 세계적으로 유전자 테스트에 관한 근거법률을 제정한 국가는 거의 없다. 대부분 이러한 유전자 테스트의 경우에는 기존의 노동법령에 의해서 간접적으로 금지되어 있다.

한편, 대다수 국가에서 유전자 테스트보다는 약물 테스트는 보편적으로 행하고 있다. 많은 종업원들에게

15) 전통적인 통신 데이터와 Email 등의 새로운 데이터에 대한 적법절차의 차이점에 관한 상세한 논의는 정영화, 앞의 논문(주.1), 81-83 면 참조.
16). ACLU: Genetic Discrimination in the Workplace Fact Sheet.

있어서 약물 테스트는 정형화된 직장생활의 일부가 되고 있다. 오늘날 직장에서 소변이나 머리카락의 검사를 통해서 종업원이 마약이나 중독성 항정신성 약품의 흡입을 추적할 수 있다. 이러한 예방적인 약물 테스트의 시행에 따른 문제는 프라이버시, 신체상의 안전성, 자유 및 무죄추정의 전반적인 문제를 야기한다는 점이다. 테스트 과정 자체가 매우 비인간적이고, 감시자들이 현장에서 샘플을 파손하지 못하게 상주해야 한다. 특히 소변검사의 경우는 매우 침해적인 것이다. 이 약물검사는 협박과 위협으로 생명과 명성을 구하는데 필요악이라고 판명되지만, 사업주의 이익이 종업원의 존엄성과 인권을 압도하는지는 분명하지 않다. 제조기업들은 약물 테스트의 유익함을 강조하는데, 그들 수 천명의 종업원들이 직무태만에 의한 사고감소, 저생산성, 산업재해보상 및 의료보호의 청구로부터 많은 고용주들을 구제할 수 있었다고 한다. 각국 정부들도 약물과의 전쟁의 일부로서 약물테스트를 권장하고 있다. 그러나 약물 테스트도 약 40% 정도까지 부정확하다는 점을 상기하여야 할 것이다.[17] 특히 약물에 대한 양성반응이 모두 약물이 체내에 흡입되었다고 단정할 수 없다.

(4) 공간검색 프라이버시(Territorial Privacy)

일정공간의 외부 침입을 방지하고자 설치하는 전자기 장치나 비디오 감시장치, ID 카드 등이 있다. 우리나라에서는 백화점이나 중요 시설물에 설치되어 있는 CCTV나 감시카메라의 형태가 일반적인 형태로 인식되고 있다. 최근 ID 카드제도는 점차적으로 확산되고 있는 실정에 있는데, 이는 원래 인종 및 종교차별, 정치적 극단주의로부터 위협을 피하기 위해서 고안된 것이다. 이제 다른 국가에서 ID카드는 행정민원 신청의 수단으로 활용되고 있다. 대다수 국가에서 ID카드제도는 헌법상 프라이버시 침해의 우려를 이유로 심각한 문제가 제기되고 있다. 1991년 헝가리 헌법재판소는 다목적(multi-use)의 개인 ID번호 부여는 헌법상의 프라이버시 권리를 침해한다고 판결하였고,[18] 1997년 포르투갈 헌법은 "시민은 모든 목적의 국민 ID번호를 부여받을 않는다"고 규정하고 있다. 또한 1998년 필리핀 대법원은 국민 ID제도는 헌법상 프라이버시 권리를 침해한다고 판결하였다.[19] 또한 미국에서는 전체 연방에서 적용되는 통일적인 ID부여의 운전면허증의 법제화에 대한 저항에 직면한 바 있다.

Ⅵ. 프라이버시의 보호방안[20]

오늘날 프라이버시의 보호방안은 정보기술의 발전에 상응하여 프라이버시의 침해가 급속하게 대두하면서 시급한 국가 및 국간의 중요한 과제가 되었다. 특히 프라이버시의 침해를 촉진하는 몇 가지 경향이 있는데, 이는 정보기술의 이전에 따른 정보공유체제가 등장하면서 데이터 이동에 따른 지리적 장애를 제거한 세계화와 국가간의 기술적인 장애를 제거하면서 체제수렴의 현상 그리고 다양한 데이터를 수집한 것을 다른 형태로 전환하여 이용할 수 있는 멀티미디어의 통합에 따른 결과라고 지적할 수 있다. 정

17), .Ethan A. Nadelman, "Drawing the Line on Drug Testing," http://www.lindesmith.org/library/ethan-drugtesting2.html.

18) Constitutional Court Decision No. 15-AB of 13 April 1991, Abailable [http://www.privacy.org/picountries/hungary/hungarian-id-decision-1991.html].

19) Philippine Supreme Court Decision of the National ID System, july 23 1998, G.R. 127685. [http://www.bknet.org/laws/nationalid.html]

20) 이에 관한 상세한 논의는 정영화, 세계의 정보프라이버시와 개인정보보호법, 근간(2001).

보통신 기술분야에서의 감시장치의 스팩트럼은 도청, 개인ID제도, 데이터 개발, 검열, 암호통제 등이 적절한 보호장치 없이 제 1세계에서 제 3세계로 수출되고 있다는 점을 지적할 수 있다.

여기서 각국의 프라이버시 보호모델로서는 OECD 국가를 포함하여 34개 국가에서 공적부문의 프라이버시 법제와 민간부문의 프라이버시 법제가 이원화되거나 통합되는 경향을 보이고 있다. 이러한 입법모델은 유럽연합 등을 중심으로 하는 OECD국가에서의 일반적인 입법유형으로 나타나고 있다. 현재 이러한 모델은 OECD 국가를 포함한 약 34개 국가에서 통합법제를 시행하고 있다. 이와 달리 미국과 멕시코, 일본 및 한국 등 6개 국가는 아직 부분적인 입법에 의해서 해당 분야의 프라이버시 입법을 개별적인 부분 법제의 모델을 시행하고 있다. 특히 미국을 제외한 기타 국가들은 프라이버시 입법동향이 매우 부진한 실정에 놓여 있다.

1. EU model(포괄적인 법률)

공공부문의 개인정보, 민간부분의 개인정보, Online 및 Offline 정보의 통합방안이다. 이러한 EU모델의 논거는 과거의 프라이버시의 침해에 대한 철저한 권리구제, 전자상거래(E-commerce)를 촉진하기 위해서, 또 EU 법체계의 통일을 기하고자 단일한 개인정보감독기구의 설치를 전제하고 있다. 권리구제 방식도 법원에 의한 구제가 아니라, 옴부즈맨과 같은 독립기구에 의해서 신속하고 사법비용이 적게 들기 때문에 매우 유리한 구제방안 이다.

2. 미국 모델(분야별 입법)

미국과 일본 및 한국의 경우가 이에 해당한다. 이는 새로운 입법이 새로운 기술에 뒤따라서 시도되기 때문에 개인정보의 보호가 취약한 약점을 갖는다. 이는 통일적인 감시기구를 설치하지 않고, 일반 법원 재판의 권리구제에 의존하기 때문에 사법거래비용이 증대된다는 비판이 있다.

3. 자율 규제 모델

이는 이론상 이상적인 방안이지만, 사업자의 이익담합이나 그들의 도덕적 해이 현상으로 인해서 규제의 효과를 기대할 수 없음이 증명되고 있다. 규제에 수반되는 조사나 결정의 집행력이 미약하다는 약점 때문에 점차 회피하는 방안이다. 물론 공통접근은 암호프로그램, Proxy Server 등의 기술개선에 의한 프라이버시 보호방안이 있다.

Ⅶ. 우리나라의 개인정보 보호법제의 현황

1. 개인정보의 침해유형

개인정보의 침해유형을 구분하는 기준은 침해주체가 공공기관 또는 민간단체 및 사인에 의한 형식적 기준과, 또 침해내용에 따른 실질적 기준으로 대별할 수 있다.

첫째, 침해주체는 공공기관이든 민간조직이든 간에 공공기관의 개인정보보호법 또는 정보통신망이용 및 정보보호법의 적용에 따른다.[21] 또는 공공기관이 자체의 개인정보를 침해한 경우에는 전자의 법률에 의해서, 또는 그가 정보제공사업자의 보유정보를 수집하는 경우에는 정보통신망이용 및 정보보호법이 적용된다.[22] 실제로 정보통신서비스제공자[23]로서 전기통신사업자, 웹캐스팅(webcasting), 가상몰사업자 등, 또 서비스사업자인 금융기관, 백화점, 항공사, 호텔사업자, 의료기관 등, 개인정보 처리 및 관리 수탁자로 분류할 수 있다.

둘째, 침해행위의 내용은 다음과 같은 유형으로 분류될 수 있다.
① 정보의 수집단계에서 정보주체의 의사에 반한 수집행위로서 동의없는 개인정보수집, 동의하에서 과다한 정보수집, 목적달성 후에 개인정보 미파기, 동의철회에 대한 거부 및 아동으로부터 개인정보수집을 들 수 있다.
② 정보의 관리나 저장 및 이용단계에서 개인정보의 프로파일링(profiling), 목적달성 후에 개인정보의 파기거부나 계약불이행의 문제를 들 수 있다.
③ 개인정보의 이전단계에서 부정한 방법에 의한 위법한 거래로서 정보주체의 동의나 통지없이 제3자에게 임의제공 또는 판매, 또는 개인정보의 불법적인 유출이나 공개행위를 들 수 있다.[24] 이와 같이 상업적 목적으로 기존의 오프라인의 기업에서 보유하는 개인정보를 불법적으로 거래하고 있다,

셋째, 정보저장이나 검색단계의 침해행위의 유형은 수집목적의 남용, 비밀리에 정보수집, 오류의 개인정보의 저장 등으로 분류될 수 있다. 즉 기업체의 전산담당자가 외부인에게 다수의 개인정보를 제공한 사례를 들 수 있다. 요컨대, 개인정보의 남용과 관련한 이러한 분류는 인터넷 이용자들의 개인정보의 침해를 우려하는 유형을 분류하고 있다. 정보수집자가 다른 기업체나 공공기관 및 수사기관 등에게 그들 의 개인정보를 유출하거나 또는 판매하는 등을 가입자의 개인정보 침해라고 본다.[25]

2. 개인정보보호의 법제 현황

개인정보는 인격권의 보호법익과 프라이버시 권리의 보호대상에 한정한다. 국가비밀에 관한 법익은 개인정보와 직접 관계없이 개인의 프라이버시를 제한하는 사유가 될 수 있기 때문에 프라이버시 권리의

21) 부산여대는 부산여대는 학생들의 개별 동의없이 재학생 5,200 여명의 이름과 주민번호, 주소를 (주)L인터넷사에 제공하고 온라인 강의용 기자재 3,600만원의 무상증여 받아서 법위반으로 처벌을 받았다.(중앙일보, 1999.11.2자 기사)
22) 정보기관이 1999년 4월 유니텔, 하이텔, 천리안 등 PC통신 고객지원센터에 PC통신 가입한 모든 주한외국인의 이름, 통신ID, 직업, 주소, 여권번호 등의 협조공문을 발송하였다. 이에 따라 통신사업자들이 그 기관에 제공한 외국인 가입자 수는 전체적으로 1,000명이 넘는 것으로 추정된다.(동아일보, 1999.9.10자 기사)
23) 한국통신 직원 K씨는 전화가입자의 개인정보를 사채업자에게 대가를 받고 제공하여 채무자들을 추적한 사채업자와 함께 구속되었다. K씨는 96년 1월부터 올 3월까지 P씨 등의 부탁을 받고 모두 1백여 차례에 걸쳐 전화가입자들의 주소와 통화내역서 등 개인정보를 유출시켜온 혐의다. 이는 통신비밀보호법 위반의 책임도 물었다.
24) 국민연금관리공단 직원이 연금가입자의 개인정보가 수록된 자기테이프를 민간사기업에게 이전한 사건이다. 유출된 데이터는 1991년 11월 당시 국민연금 가입자 10만 명의 이름, 직장명, 전화번화, 우편번호 등이 수록되었다.(한국전산원, 정보사회의 정보이용자 권익향상 방안,1997.12.)
25) 정보화 역기능 실태조사, 한국정보보호센터, 1999. 12, p.51.

한계에 해당한다. 특히 공공기관이 행정목적의 개인정보를 컴퓨터에 의한 수집과 처리 및 이용이 광범위한 범위에 걸쳐서 행해지면서 개인정보의 보호방안이 중요한 사회적 이슈로 제기되었다. 이는 국민들의 알권리를 구현하기 위한 정보공개와 함께 근거법률을 법제화하기도 하였다. 이제 개인정보가 단순한 인격권의 보호법익의 범주에 국한되지 않고, 경제적 재화와 공공재로서 다목적 용도로 이용되면서 개인의 동일성을 식별할 수 있는 개인정보는 헌법과 형법 및 공법적 규율의 정도가 강하게 제기되고 있다.

문제는 사인이 특정인의 개인정보를 직접 침해한 경우에 법적 권리구제의 수단과 절차는 아날로그 형태의 데이터와 오프라인(Off-line)의 현실세계를 전제하였기 때문에 온라인(On-line)에서 디지털형태의 개인정보의 침해에 대한 구제가 취약하다는 문제가 있다. 왜냐하면 온라인에서는 이용하는 형식의 데이터와 호환성을 전제로 하기 때문에 기존의 불법행위 법리에 의한 해결로 역부족의 결과를 초래할 수밖에 없다. 즉 가상공간은 국경의 물리적 공간을 해소하고, 실시간으로 쌍방향에 의한 의사소통을 전제함으로 현실세계에 비해서 거래비용과 침해의 다양성을 고려하여 입증방법 및 책임범위의 명확한 구분이 쉽지 않기 때문이다. 특히 가상공간에서는 개인정보의 수집자와 피해자간의 현저한 정보의 비대칭성(asymmetry)으로 인해서 정보량과 정보접근의 격차 때문에 피해자의 입증책임의 완화 등의 보완이 절실하게 요청된다. 그럼에도 불구하고 현실세계의 기존의 법제는 피해자의 입증책임을 종래의 비경제적이고 과도한 거래비용을 수반하는 소송방식에 의해서 책임을 부담함으로 피해자의 권리구제는 정보량의 격차와 정보접근의 차별화에 의해서 수집자와 이용자가 일방적으로 유리한 상황에 있다. 따라서 이러한 근본적인 문제점의 해결방안을 제시하기 위해서는 현행 개인정보 및 프라이버시의 보호법제의 구조와 특성을 검토함이 선결과제이다.

3. 개인정보보호법제의 특성

인터넷을 통한 전자상거래가 활성화되고 있는 가운데, 네트워크를 통해 개인정보가 쉽게 유출되고, 한번 유출되면 쉽게 다수에게 이용될 수 있다. 그러한 개인정보가 국경을 넘어 유통됨에 따라서 개인정보의 보호는 온라인 환경에 있어서 매우 중요한 과제로 부각되고 있다. 우리 나라에서도 개인정보의 유출, 이전 등의 개인정보 침해는 심각한 수준이다. 개인정보의 문제는 비단 전자상거래만이 아니라, 치안 및 범죄 등의 정보, 공공 및 민간 정보망의 상호접속, 항공 및 여행사에서 보유한 개인정보, 의료기관이 수집하는 개인정보 등 폭넓은 관점에서 개인정보의 보호문제를 검토할 필요가 있다.

무엇보다도 전자상거래가 활성화되면서 영리목적으로 개인정보가 네트워크를 통해 유통되는 경우 폐해의 위험성이 훨씬 커졌다. 더구나 정보주체는 개인정보가 누설되는 것조차 인식할 수 없으며, 그것도 피해발생 이후에 비로소 인식할 수 있기 때문이다. 따라서 종래의 프라이버시의 피해에 대한 사후구제보다는 사전예방의 조치로서 개인정보보호의 기본원칙을 준수하도록 하는 것은 중요한 과제가 되었다.

(1) 개인정보보호의 법적 근거

현행 헌법의 개인정보 보호는 외국의 입법 유형과 다소 비교되는 성질을 보이고 있다. 즉 헌법은 개인정보(privacy) 보호에 관해서 주거의 평온을 보장하는 주거의 자유(제16조)와 통신비밀을 위한 통신의 자유(제18조) 그리고 일반적인 사생활의 비밀과 자유(제17조)를 규정하고 있다. 사생활의 비밀과 자유는 헌법의 주거와 통신의 자유를 제외하는 인격권을 비롯한 내밀영역과 비밀영역 및 사적영역 그리고 사회적

영역에 관한 기본권과 자유의 보호로 이해할 것이다. 이제 헌법 제17조의 사생활의 비밀과 자유를 협의의 개별 기본권으로 이해하면 그 보호법익은 인격권에 한정하게 된다.[26]

그러나 이러한 해석은 개인정보의 사적 재화 내지 재산권의 객체로서 당사자의 동의나 그에게 통지도 없이 수집되고 거래되는 행위에 대해서는 보호범위를 벗어나는 까닭으로 인격권의 보호한계를 극복하지 못한다는 점이 문제이다. 그래서 주거비밀의 보호법익은 헌법 제16조 및 형법의 주거침해규정(형법 제319-321조), 또 통신의 자유는 헌법 제18조와 통신비밀보호법과 형법 및 형사소송법 그리고 명예훼손(형법 제308조) 및 불법행위(민법 제750조)의 손해배상에 의한 해결이 기본 방도이다. 따라서 이러한 헌법의 프라이버시 권리는 좁은 의미의 알권리와 다르게 자신의 개인정보에 대한 자기결정권과 구분하여야 한다. 즉 알권리로서 개인정보의 자기결정권은 헌법 제10조의 인간존엄 및 행복추구권의 인격권을 원용하지 않을 수 없다.

그런데 정보혁명의 결과로 개방형 네트워크인 가상공간(cyberspace)과 무선전화(mobile phone)의 폭발적인 이용은 개인정보와 관련하여 기존의 헌법조항의 해석을 확장하지 않을 수 없다. 즉 제17조 헌법규정은 개인의 프라이버시 보호의 기본규범으로 이해할 것이다. 현재 개인정보의 보호영역은 가상공간이란 매체를 기준으로 온라인(On-line)과 오프라인(Off-line)으로 구분되고 있다. 온라인의 개인정보는 컴퓨터로 수집, 가공, 이용 또는 실시간으로 이동하는 정보를 포함하는 반면에, 오프라인의 개인정보는 종래의 수작업에 의한 수집과 이용 및 유통하는 문서와 기록 등의 데이터이다.

요컨대 개인정보는 공공기관에 의해서 수집과 저장 및 이용하는 형태, 개인과 사기업 및 민간조직에서 수집과 관리 및 이용하는 개인정보로 구분된다. 그러면 이하에서 현행 개인정보보호법제의 구조를 개관하기로 한다.

(2) 개인정보보호의 법제현황

현행의 개인정보보호 법제는 형법의 '비밀침해죄', 전기통신의 도청금지를 위한 '통신비밀보호법' 등의 보호규정과 달리 '공공기관의개인정보보호에관한법률'과 '정보통신망이용촉진및정보보호등에관한 법률'(2001.7.1시행) 등이 있다. 동법은 공공 및 민간부문에서 취급하는 개인정보의 보호를 대상으로 한다. 국내의 개인정보보호에 관한 법률을 개관하면 다음과 같다.

(3) 정보공개의 법적 근거

현대사회의 다양성을 반영시킬 개인의 알권리는 적극적인 의미로서 직접민주제의 구현에 부합되는 헌법적 의의를 갖는다. 알권리(right to know)는 헌법상 명문의 규정을 두고 있지 않지만, 세계인권선언 제19조에서 명시하고 있다. 알권리의 헌법적 근거에 대한 논의와 관련하여 표현의 자유의 내용으로 이해하거나, 또는 일반적으로 인격의 형성 및 발현의 인격권으로 이해하는 입장이 대별된다. 이와 같이 현대 헌법학에서 알권리는 규범적인 측면에서는 참여적인 권리의 인권인 동시에 정치과정에서 주권자로서 시민의 지위를 강화하는 의의를 가진다. 이와 관련하여 헌법판례도 알권리의 헌법적 가치를 인정하는 관행을 확립하였다.[27]

26) 김철수, 헌법학 신론, 박영사, 2000, 260면 이하 참조

<표 2> 국내의 개인정보보호 관련법령

입법연도	입법 명칭
1983년	전기통신기본법, 전기통신사업법
1986년	전산망보급확장과이용촉진에관한법률(99,2000개정)
1989년	전파법 개정(61년 제정)
1991년	무역업무자동화에관한법률
1993년	통신비밀보호법, 금융실명거래및비밀보장에관한긴급재정경제명령
1994년	공공기관의개인정보보호에관한법률, 정보통신설비에관한안전신뢰성기준, 공업및에너지기반조성에관한법률
1995년	컴퓨터범죄대응규정에관한 형법개정
1997년	금융실명거래및비밀보장에관한법률, 공공기관의정보공개법
1999년	정보통신망이용촉진등에관한법률(제정)
2000년	정보통신망이용촉진및정보보호등에관한법률(제정) 정보통신망기반보호법(2000.12 제정)

출처: 정영화, 전자상거래법(2판), 다산출판사, p.320

즉 알권리는 민주국가에서 국정의 공개와도 밀접한 관련이 있다. 헌법에서는 입법의 공개(제50조 제1항), 재판의 공개(제109조)와 같은 명문의 규정을 두고 있지만, 법치행정의 원리에 입각하여 행정효과의 공개와 함께 행정과정의 공개에 대해서는 명문의 규정이 없다. 알권리의 연혁을 고찰할 때에 정부기관이 보유하는 정보에 대한 시민의 접근과 공개 등의 청구권을 인정할 수 있다.

알권리의 내용은 소극적인 정보수령권과 적극적인 정보청구권으로 구성된다. 전자는 종래 시민을 정부나 언론매체의 정보독점에 대해서 소극적인 정보수령자의 지위로 보는 입장으로 표현의 자유와 상호보완적 관계에 있다. 특히 언론매체도 신문보다 늦게 나타난 공중파 방송은 정부의 독점적 지위를 갖기 때문에 공적 책무와 과업을 부과하는 것이 일반적이었다. 반면에 후자는 정보의 매체중립성의 특성을 강조하면서 시민의 적극적인 지위로서 정보의 접근과 공개청구권을 인정하게 되었다. 문제는 언론기관이 민간기업의 형태로 운영되는 경우에 사인이 특별한 계약의무나 법적 의무를 전제하지 않은 상태에서 주관적 공권으로서의 알권리를 청구할 수 있는지 여부이다. 왜냐하면 전통적으로 기본권은 대국가적 공권으로서의 지위를 인정하고 있으며, 예외적으로 사인간에 있어서 직접 적용될 수 있는 인권목록을 상정하기 곤란하다. 이러한 까닭으로 알권리가 사인에게 직접 적용되는 경우도 언론의 공공성을 전제하여 반대 당사자로서 접근권(access right)과 반론권을 인정할 수 있다.

27) 헌법재판소는 1989년부터 알권리를 근거로 제기한 헌법사건에서 구체적으로 인용하고 있다. 공권력에 의한 재산권 침해와 헌법소원(헌재 1989. 9.4, 88헌마 22, 헌재판례집 제1권 176면): 기록등사신청에 대한 헌법소원(헌재 1991. 5.13, 90헌마133. 헌재판례집 제3권, 234면): 지세명기장 열람거부 등 위헌확인(헌재 1994.8.31. 93헌마 174, 헌재판례집 제6권 2집 324면): 군사기밀보호법 제6조 등에 대한 헌법소원(헌재 1992.2.25, 89헌가104, 헌재판례집 제4권, 64면): 형사소송법 제55조 제1항 등 위헌확인(헌재 1994.12.29, 92헌바31, 헌재판례집 제6권 2집, 376면): 대통령선거법 제65조 위헌확인(헌재 1995.7.21, 헌마177, 199병합, 헌재판례집 제7권 2집, 112면) 등의 판례가 있다.

여기서 알권리는 공공기관이 보유하는 정보에 대한 공개청구권을 인정하는 헌법적 근거로서 기능하고 또한 공공기관이 수집 및 보유하는 정보의 접근과 공개 및 이용의 목적으로 청구할 수 있는 공권으로 이해된다. 그런데 적용대상은 공공기관으로 한정하기 때문에 개인의 이익과 권리에 직접 또는 간접적으로 영향을 미치게 된다. 따라서 개인은 직접 공공기관에 대해서 자신의 개인정보에 대한 접근과 열람 및 잘못된 내용에 대한 삭제 또는 정정을 청구할 수 있다. 왜냐하면 정부기관 및 공공단체는 공공서비스를 제공하는 공익 실현을 위한 기능으로서 행정정보 및 경제정보를 수집한다. 예컨대 개인이 일정한 사업을 수행하기 위해서 기업등록 및 등기 또는 일정한 수익처분의 행정처분을 청구할 경우에 행정청에 대해서 당해 사업자 또는 기업정보를 제공하게 된다. 우리들은 사업주체인 기업의 과학기술, 경영정보, 또는 노사관계 및 영업비밀을 포함하는 정부기록에 접근하고자 한다. 만약 누가 정보공개법에 의하여 공공기관이 보유·관리하는 정보를 법률에 의하여 공개를 청구하면 이를 수용하여야 하기 때문에 그러한 법적 실체를 "이해관계인"(affected person) 또는 제3자(third party)의 정보형태라고 한다. 설령 누가 동법에 의해서 어느 기관이 보유한 정보에 접근할 경우에 그 기관에 공개청구를 하여야 하고, 당해 기관은 그 정보를 공개할 수 있는지 여부를 결정하여야 한다. 제 3자 정보가 문제로 되는 경우에 빈번히 제기되는 아래의 문제에 대한 대답이 가능하다. 왜 사람들은 타인의 정보에 접근하는 것인가? 그 이유는 다양하지만, 그에 대한 설명으로서 다음과 같은 예들을 들 수 있다. 첫째, 과거에 정부의 경쟁계약을 수주하였던 사람이라면, 다른 사람들이 입찰과정을 알아보고자 할 것이다. 둘째, 만약 당신이 정부의 기금을 받았다면, 사람들은 그의 구체적인 내용이나 기금의 액수를 알고자 한다. 셋째, 어느 기업이 정부기관과 공동사업을 착수하였다면, 사람들은 그 사업의 조건을 정한 계약서의 내용을 확인하고자 한다.

그런데 3자로부터 정보에 대한 접근 청구를 받은 기관이 그 정보의 비공개를 결정할 경우에 제3자에게는 대개 공개하지 아니한다. 즉 당해 행정청이 제3자에게 정보 공개를 않기로 결정하면, 정보공개법에 의해서 3자가 이의를 제기할 경우에 이를 누가 담당하는가의 문제가 있다. 이 경우에 제3자가 그 정보의 공개여부를 평가할 권리를 법률에 의해서 인정한다. 이러한 심리에서 심판자는 당사자와 제3자에게 서면에 의한 주장을 진술하도록 조사와 절차적 권리를 보장하여야 한다. 이하에서는 개인정보보호법제는 대개 정보공개법과 이론적 및 실무상의 긴밀한 관련을 갖기 때문에 먼저 정보공개법률의 체계와 문제점을 개별적으로 검토하기로 한다.

4.「공공기관의정보공개에관한법률」

현행 정보공개법은 공공기관이 보유·관리하는 정보로서 알권리를 보장하고 국정에 대한 국민의 참여와 국정의 투명성을 확보하여 실질적 국민주권을 실현한다.

(1) 적용범위의 제한성

동법의 적용범위는 특별히 다른 법률에 규정하는 경우이외에 공공기관의 정보공개에 관하여 정한다. 정보공개의무를 지는 공공기관은 모든 행정부, 입법부, 사법부, 헌법재판소, 중앙선거관리위원회, 지방자치단체 등 전체 공공기관이다. 또 정부투자기관관리기본법의 투자기관은 정부가 납입자본금의 5할 이상을 투자하여 설립된 기업체로서 정보공개의무를 부담한다. 그리고 대통령령에 의해서 정보공개대상기관은 교육법에 의해 설립된 각급학교, 특별법에 의해 설립된 특수법인, 공무원연금법의 적용에 의한 기관이 정보공개의무를 진다. 우리 나라의 정보공개의무의 적용기관은 조직법의 근거에 의한 접근을 채택하고

있기 때문에 미국이나 유럽 등의 각국의 정보공개법제에 비해서 좁게 되어있다고 본다. 그들 국가는 조직법, 예산지원, 기능을 적용범위의 요소로 정하고 있어서 상당히 넓게 나타나기 때문이다. 특히 이들은 오랜 관행과 절차적인 완비를 통해서 정보공개제도의 내실을 기하고 있다.

(2) 정보공개의 내용

공개할 정보란 공공기관이 직무상 작성 또는 취득하여 관리하는 문서, 도면, 사진, 필름, 테이프, 슬라이드 및 컴퓨터로 처리한 매체의 기록 등을 의미한다(제2조). 공개란 동법에 의한 정보의 열람과 사본 또는 복제물의 교부하는 것을 의미한다. 또한 국민의 정보공개청구권을 원칙적으로 인정하고, 예외적으로 공개면제의 정보를 열거하고 있다. 청구권자는 자연인, 법인(단체 포함), 외국인에게도 허용한다. 특히 비공개 정보는 국가이익, 공공이익, 국민의 기본권에 관한 개인정보로 분류된다. 즉 다른 법률에 의해서 비밀유지나 비공개사항으로 정한 경우, 공개시에 국가의 중대한 이익을 해할 우려가 있는 정보나 공공안전과 이익을 현저히 해할 우려가 있는 정보, 또 진행중인 재판에 관련된 정보 등, 당해 정보에 포함되어 있는 이름·주민등록번호 등에 의하여 특정인을 식별할 수 있는 개인에 관한 정보, 법인·단체 또는 개인의 영업상 비밀에 관한 정보로서 공개시 그의 정당한 이익을 현저히 해할 우려가 있는 정보 등이다(법 제7조).

여기서 문제는 개인의 이름과 주민번호가 공개될 경우 그의 식별이 용이함으로 잠재적으로 그의 정당한 이익을 해할 개연성이 높다는 점을 고려할 것이다. 행정목적의 주민등록번호는 제한된 이용목적을 고려한 것이 아니라, 다목적의 용도로 공공 및 민간부문에서 이용되고 있다는 점에서 심각한 폐해를 야기하기 때문이다.

(3) 접근권의 보장과 절차법 개선

정보공개청구는 그 내용과 사용목적을 기재하여 서면으로 제출한다. 그 정보가 이미 공지사항이거나 과다 청구로 인해서 현저한 업무수행의 어려움을 초래하는 경우에는 교부가 제한될 수 있다(제8조). 이의 제도적인 개선은 컴퓨터의 이용에 의해서 다소 해소의 가능성이 있다고 본다. 현행 정보공개법은 정보공개절차와 불복구제절차가 분리되어 행정청이나 법원에 의한 심리를 구분하고 있다. 따라서 공개여부의 조사절차가 실질적인 적법절차에 부합하지 않는다는 문제점이 제기된다. 나아가 정보공개의 감독방안은 정보처리의 내부규제와 외부통제가 타당하다는 입장으로 대별된다. 외부통제의 방법도 음부즈맨(Ombusman) 제도, 독립위원회 및 행정기구의 설치방안으로 구분된다. 외국의 입법과 같이 정보공개 및 개인정보감독기구의 운영이 효과적인 공공정보의 공개제도의 성패를 결정할 수 있다고 본다.

5.「공공기관의개인정보보호에관한법률」

(1) 현행 개인정보보호의 일반법의 지위

공공기관이 보유한 정보는 헌법의 알권리에 의해서 공개를 청구할 수 있지만, 그 정보가 개인의 사생활에 관한 정보인 경우에 헌법 제17조를 근거로 공개가 면제될 수 있다. 이러한 점에서 공공기관 보유의 개인정보는 공개 및 비공개의 대상이 되므로 헌법의 보호범위와 한계에 관련하여 대립적인 해석론이 제

기될 수 있다. 이와 관련하여 판례는 1994년 국세청이 언론기업에 대해서 세무조사를 실시하였으나, 그 결과발표를 공표하지 않았던 사건에서 극명하게 보여주었다. 이 사건을 심리하였던 서울고등법원은 다음과 같이 비공개의 이유에 대한 판단을 제시하였다(서울고법 1995.8.20 선고, 94구39262). 여기서 고등법원은 알권리를 충족할 공익만으로 사생활의 비밀로서의 조세비밀을 침해할 명백하고 우월한 공익이 존재한다고 보기 어렵고, 또 기본권의 보호법익은 인격권이 가장 우선한다고 보여진다는 점에서 알권리보다는 개인의 사생활의 비밀과 자유가 더욱 보호해야 할 우선적인 가치라고 보아 그 범위 내에서는 국민의 알권리도 제한받지 아니할 수 없다고 판시하였다.

그런데 문제는 법인의 영업비밀이 과연 헌법상의 사생활의 비밀과 자유의 보호대상에 해당한가의 문제이다. 물론 헌법상의 프라이버시 권리의 주체로서 기업도 해당한다는 점을 일면 수긍할 수 있으나, 정보사회에서 개인의 프라이버시의 보호주체는 자연인만을 한정하는 것이 국제적인 통설이다. 그럼에도 불구하고 현행 헌법학계의 지배적인 통설에 의해서 법인의 영업비밀을 프라이버시의 범주로 보는 견해는 재고의 여지가 있다. 특히 기업비밀이 프라이버시의 보호대상이 아니라, 경쟁사와 관계에서 영업비밀은 부정경쟁방지법의 보호대상에 불과하기 대문에 알권리와 프라이버시의 법리를 오해한 해석이다. 국세청의 세무조사의 내용은 중대한 공익실현을 가늠할 수 있는 대상이란 점에서 언론사의 영업비밀을 프라이버시 보호법익으로 해석함은 당해 기업의 탈세혐의와 위법성에 대한 법치행정을 담보하여야 한다는 점에서 프라이버시 법리의 한계를 간과한 것이다.

(2) 주민등록제도와 개인정보보호의 법적 문제점

정부는 정보사회의 역기능방지를 위해서 제정한 개인정보보호의 법제인 「공공기관의개인정보보호에관한법률」은 개인정보를 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다) 정의하고 있다(제2조 2호). 특히 프라이버시의 보호주체는 법률에 의해서 구체적인 생존하는 자연인의 개인정보에 한정되는 것임이 명백하다. 공공기관이 컴퓨터에 의하여 처리하는 개인정보의 보호를 위하여 취급에 관하여 필요한 사항을 규정하기 위함이 목적이다.

그런데 주민등록법률은 1962년부터 실시한 주민등록제도를 통해서 인구동태의 파악을 통해서 행정편의를 도모하기 위함이다. 또한 행정기관은 주민등록법의 운용에서 긴밀한 관련성을 가진 개인정보를 행정정보로 활용함으로써 중대한 헌법적 문제를 내포하고 있다. 주민번호는 다양한 행정목적을 위해서 수집되고, 모든 국민에게 특유하게 부여된 ID번호로서 매우 민감한 개인정보로 이해되기 때문이다. 이는 특정한 개인의 신원을 식별할 수 있는 개인데이터로서 당해 개인정보의 검색이 가능한 프로파일은 개인정보의 집합물로서 컴퓨터의 자기테이프·지기디스크 기타 이와 유사한 매체에 기록된다.

그러나 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있도록 허용하고 있다. 현행 주민등록법(1962년 제정)이 약 30년간 운용과정에서 12회나 개정되면서 명백한 위헌성을 내포하고 있음을 알 수 있다. 주민등록제도는 모든 국민 개개인마다 고유한 주민번호를 부여하여 다양한 행정목적의 용도뿐만 아니라 민간부문에서도 마찬가지로 이용되고 있음을 유의할 것이다. 원래 행정목적의 주민등록제는 공공부문에만 한정되지 아니하고, 민간부문까지 전체 생활영역에서 특정한

개인정보가 광범위하게 활용되면서 주민번호의 오·악용 피해의 실태는 중대한 경제사회적 문제를 야기하고 있다.[28] 주민등록제도에 따른 기본권 침해의 개연성은 개인정보파일을 공공기관마다 분산·보유하는 형편이고, 또 개인정보에 대한 침해와 분쟁해결에 관한 제도도 정비되지 아니한 상황에 있다. 당연히 주민등록법에 의해서 모든 국민에게 고유하게 식별되는 다목적 용도의 주민등록번호를 부여함으로써 개인파일이 생성될 수밖에 없고 또한 개인별·세대별 주민등록표를 작성과 비치 및 기록하도록 한다(주민등록법 제7조). 이들 주민등록표파일은 전산정보처리로 기재하도록 한다는 점에서 온라인에 의한 개인정보의 보호범위에 속하는 것임을 알 수 있다.[29]

(3) 개인정보법제의 문제점

공공기관의정보공개에관한법률은 1997년 현재 약 29,000개의 기관에 적용되고 있다. 총무처는 법시행 이후 1995년 4월 30일까지 공공기관의 보유파일에 대해서 개인정보파일의 명칭, 보유목적, 보유근거, 기록대상자의 범위, 기록항목의 범위 등 처리현황을 통보하도록 요청하였다. 그 결과 전체 4,791개 기관에서 332종 10,579개의 보유 파일의 전체 데이터건수는 10억 2천만 건에 달한 것으로 나타났다.

① 수기정보의 보호대상 포함

개인정보는 컴퓨터에 의해 처리한 개인정보에 한정하고 있다. 여기서 수기파일의 데이터도 당연히 보호할 것임에도 제외한 것은 입법적 미비이다. 국가의 모든 행정이 전산화되었다고 할지라도 수기파일이 보호가치가 낮은 개인정보로 평가할 수 없다. 대다수 국가의 개인정보법제는 수기파일의 정보도 보호범위에 포함시키고 있다. 그 데이터의 유출이 용이한 반면에, 추적은 역으로 어려운 편이다.

② 사자(死者)의 개인정보 문제

법인과 사자(死者)의 개인정보는 제외된다. 법은 자연인의 개인정보만을 보호하기 때문이다. 법인의 개인정보는 보호대상에서 제외하는 것이 국제사회의 공통적인 입법 추세이다. 사자의 경우는 유족과의 관계에서 일정기간의 보호대상으로 포함하여 해석할 수 있다. 대개 개인정보의 보호기간은 사후 20년 동안 보호하고 있다. 현행 법제는 개인정보의 보호기간을 규정하고 있지 않기 때문에 유족의 개인정보와 관련하여 보호된다고 본다. 그러나 사자도 그가 생존 당시의 개인정보를 일정기간의 보호기간을 설정하는 입법개선이 요청된다.

③ 개인정보관리의 개선방안

개인정보파일의 명칭과 그 파일의 보유목적, 보유기관의 명칭, 개인정보파일에 기록되는 개인 및 항목의 범위, 개인정보의 수집과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭, 개인정보파일의 열람예정시기, 열람이 제한되는 처리정보의 범위 및 그 사유, 기타 대통령령이 정하는 사항(법 제6조)을 규정하고 있다. 개인정보의 보유기관의 장은 처리정보를 정보주체이외의 자에게 제공하는

28) 주민번호제도는 개인마다 특유한 고유번호가 부여되어 그 번호로 고유성을 식별한다는 점에서 비례원칙의 한계를 벗어났다. 개인의 ID로서 주민번호부여는 행정목적의 범위를 벗어나 민간부문에서 악용되는 실태를 파악하지 않을 수 없다.

29) 주민등록번호의 위헌성에 관한 상세한 고찰은 다음 문헌을 참조할 수 있다.
정영화, "현행 주민등록번호제도의 위헌성과 그 제도개선방안", 민주사회와 변호(2001.3/4), 민주사회를 위한 변호사모임.

때에는 그 수령자에 대하여 사용목적·사용방법 기타 필요한 사항에 대하여 제한하거나 처리정보의 안전성확보를 위하여 필요한 조치를 강구하도록 요청하여야 한다(제10조 2항). 또 개인정보취급자는 개인정보를 누설 또는 권한없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하는 것을 규제한다(제11조). 정보주체는 개인정보파일대장에 기재된 범위 안에서 서면으로 본인에 관한 정보열람을 청구할 수 있고, 정보를 보유하는 기관장은 15일 이내에 당해 처리정보를 열람하게 하여야 한다. 정보주체의 개인정보열람청구에 대한 거부 등에 대한 불복절차는 행정심판법에 의하여 다투도록 하고 있다(제15조). 물론 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의하기 위한 개인정보보호심의위원회의 권한은 분쟁의 해결에 직접 개입할 수 있는 것이 아니라, 간접적으로 정책개선을 위한 기능을 담당할 뿐이다.

④ 정보이용 목적의 제한과 파일링(profiling)의 규제
현행 공공기관이 보유하는 정보의 공개와 개인정보보호를 위한 법제의 운영현황은 개인의 프라이버시의 권리를 실체법 및 절차법의 차원에서 인권보장을 위한 제도정비가 미흡한 점을 인정하지 않을 수 없다. 즉 공개대상의 정보에 대한 과도하고 불명료한 사유에 의한 공개면제범위의 광범성과 개인정보보호의 절차법 보호가 시급히 개선되어야 할 내용으로 파악되고 있다. 특히 공공기관 내부의 정보관리자의 직무의 전문화와 권한과 책임의 명료성이 전제되며 또한 주민등록제도와 같이 만능의 행정편의와 행정목적을 위해서 개인에게 고유번호를 출생과 더불어 사망시까지 개인식별 수단의 오·남용과 함께 행정기관만이 아니라 민간부문에서도 이러한 개인의 주민번호를 토대로 공적부문에 비해서 더욱 방대한 개인정보파일이 생성되어 있음을 간과할 수 없다.

6. 민간부문 개인정보보호의 법적 근거

헌법 제17조의 사생활의 비밀과 자유는 공권력에 대해서는 직접 효력이 있지만, 프라이버시 권리는 사인(사기업등)간에 있어서 간접적인 효력을 인정하는 경우에는 민법의 불법행위나 형법의 명예훼손에 의한 해결이 전제되기 때문이다. 따라서 현재와 같이 사인에 의한 개인정보침해가 급증하는 사태에서는 민간부문의 개인정보보호를 위한 단행 법률이 존재하여야 한다. 그런데 2000년 12월에 개정되어 2001년 7월 1일부터 시행되는 「정보통신망이용촉진 및 정보보호등에 관한법률」(이하 '정보통신망법'이라 한다)은 다음과 같은 점을 강조하고 있다.

(1) 법적 규제의 의의

첫째, 정보통신망의 이용을 촉진하여 정보통신서비스이용자의 개인정보의 보호를 강화하고 유해정보로부터 청소년보호를 강화하였다.
둘째, 온라인서비스 이용자의 권익보호를 위하여 인터넷서비스 품질개선 시책을 강구하고, 그 서비스제공자는 서비스의 품질을 이용자에게 주지시키도록 한다.
셋째, 정보통신부장관이 인터넷도메인이름 등 인터넷주소자원의 확충과 적정한 활용, 그리고 도메인분쟁의 조정해결을 고려하고 있다.
넷째, 정보통신서비스제공자가 개인정보의 수집·처리·관리 등을 타인에게 위탁하는 경우에 그 타인의 개인정보보호 위반행위에 대하여 책임을 부과하고 있다. 이와 같이 온라인 환경의 급속한 발전에 의해서 이전보다 디지털 정보형태가 온라인 서비스의 중요한 거래객체로써의 의의를 강조하는 국제적인 추

세를 반영한 것으로 평가된다.

개인은 민간단체 또는 기업들이 자신에 관한 어떠한 개인정보를 언제, 어떻게 수집하여, 어떤 형태로 보유하고 또 이를 어떤 목적으로 이용할 것인가에 대해서 알권리를 인정할 수 있다. 왜냐하면 민간부문이 보유한 그러한 개인정보는 수집자인 기업이나 단체가 수시로 소비자로 혹은 마케팅의 기법을 이용해서 임의로 처리하여 데이터 베이스한 것이다. 이 때문에 그의 정보에 대한 정보주체의 소유권 주장에 대해서 사업자는 자신의 비용과 노력에 의한 결과로서의 소유권 주장을 하고 있다. 그러면 정보주체는 그러한 수집정보에 대해서 삭제나 수정을 요구할 권리가 있는지 문제이다. 민간조직들이 그들의 개인정보를 수집하는지, 그들이 어떤 정보를 보유하는지, 그 정보를 어떻게 이용할 것인지, 그밖에 누가 그 정보를 수집하는지에 대한 알권리는 계약 이외 어떠한 법률관계에서 허용될지 의문이다. 이해의 편의를 위해서 정보통신망법과 관련하여 정보프라이버시(information privacy)를 살펴본다.

(2) 정보주체의 법적 지위

현재 민간부문의 일반적인 개인정보법제가 부재한 현실에서 분야별 법제로 운용되고 있다. 정보통신 네트워크를 이용하여 타인의 개인정보를 수집과 저장 및 처리하여 그 데이터를 공개 또는 누설하는 경우에 통신비밀보호법 또는 정보통신망이용법의 규율이 예상된다. 예컨대 E-mail의 검열이나 무단 열람행위는 통신비밀보호법의 위반으로 처벌할 수 있다. 또한 정보통신망을 통하여 수집·저장·처리·보관·이전되는 개인정보의 오·남용에 대비하여 정보통신서비스제공자가 이용자의 동의하에 개인정보를 수집하고, 수집목적이외의 개인정보의 이용제한과 제3자에게 제공을 제한하며, 정보주체의 개인정보에 대한 열람 및 정정 권리를 부여함으로써 개인의 정보프라이버시 보호이다.

정보서비스사업자와 이용자의 법률관계는 정보매체를 매개로 서비스의 공급계약관계에 따른 소비자와 사업자간의 법률관계에 따른 권리의무를 고려할 수 있다. 이들 법률관계는 단순한 소비자의 권리보호에 한정되는 것이 아니다. 부연하면 이용자의 개인정보에 대한 권리는 그에게 전속되는 인격권 동시에 재산권이지만, 소비자의 권리는 서비스의 특성과 공급자의 채무불이행이나 불완전이행을 전제로 제기되는 청구권이다. 따라서 인격권 및 재산권은 권리자에게 그의 행사와 귀속이 전속되는 권리인 반면에, 청구권은 계약목적과 급부 내용에 따라서 양도가능하기 때문에 구별된다. 즉 개인정보는 이용자가 단순히 소비자로서의 권리청구가 아니라, 그의 개인정보는 포괄적인 인격권과 재산권으로서 포기나 양도 및 이전이 어려운 특성을 고려하여야 한다. 그러므로 개인정보의 수집이나 저장 및 처리에 관해서 신중하고 당사자의 동의나 통지가 필요하다.

(3) 개인정보의 개념과 적용범위의 한계

개인정보는 생존하는 자연인에 관한 성명이나 주민등록번호 등과 같이 당해 개인을 알아(식별) 볼 수 있는 부호·문자·음성·음향 및 영상등의 정보(다른 정보와 결합하여 식별가능한 경우도 포함)를 말한다(제2조6호). 비교법상 개인정보의 주체는 생존한 자연인에 한정하고 있는 점은 차이가 없다. 문제는 현행 주민번호는 개개인에게 고유한 ID로써 평생동안 불변하고, 또 다목적의 행정 및 사적 용도로 포괄적으로 사용한다는 점에서 다른 한정된 목적의 ID, 예컨대 사회보장번호(SIN)로 대체되어야 한다. 단기적으로 인터넷 사이트의 가입항목에서 제외하는 입법규정이 필요하다. 컴퓨터나 전자기기에 의한 개인정보

만을 한정하여 적용되기 때문에 오프라인의 수기에 의한 개인정보는 보호객체에서 제외된다. 특히 이 법은 민간부문의 개인정보에 관해서 정보통신망에 의해서 개인정보를 수집하고, 이용 및 처리하는 경우에 대해서 특별법의 지위를 갖기 때문에 민간부문의 전체로 확대 적용하려면 개인정보보호법의 일반법으로 재편되어야 할 것이다.

(4) 개인정보주체의 동의와 사업자의 통지

정보통신서비스제공자가 이용자의 개인정보를 수집하는 경우 그의 동의를 필요로 한다(제22조). 동의를 얻기 위해서는 개인정보관리책임자의 신원 등과 수집목적 및 이용목적, 제3자에게 제공할 경우에 그 제공목적과 그 정보의 내용 및 수령자 그리고 그의 권리와 행사방법을 고지하거나 이용약관에 명시하여야 한다(제22조 제2항). 사업자가 이를 이용자에게 통지함은 대개 서비스이용약관에 명시하는 것으로 갈음한다는 점이다. 사업자는 이용자에게 고지하는 방법과 이용약관에 명시하는 방법을 택일하도록 규정되어 있다. 개별적으로 이용자가 고지를 원할 경우에는 이용약관에 명시만으로 갈음하기 곤란하다. 구체적으로 제3자의 수령자를 사전에 특정하기 어려운 경우에는 고지가 필요할 것이다. 적어도 고지는 서비스이용약관에는 일반적인 공지사항을 제시하고, 고지는 개인정보의 주체에게 개별적으로 고지하는 절차를 병행하여야 유럽의 개인정보원칙과 부합된다고 판단된다. 또 정보통신서비스제공자는 그 이용자의 동의에 의해서도 고지범위를 초과하여서 제3자에게 제공할 수 없고(제24조 제3항) 또한 그 개인정보를 제공받은 자도 제공목적 이외로 이용하거나 제3자에게 제공하지 못한다(제4항). 여기서 수집의 목적과 제공의 목적이 동일한 경우와 상이한 경우를 어떻게 구분하며 또 사전 및 사후적인 그러한 목적을 개별적으로 판단하는 문제는 용이하지 않다. 따라서 이에 관한 구체적인 기준을 별도의 지침에 의해서 제시하는 것이 필요하다.

(5) 개인정보 처리의 제한

정보통신서비스제공자등은 타인에게 이용자의 개인정보의 수집·취급·관리등을 위탁시에 그 사실을 사전에 이용자에게 고지하여야 한다. 이는 개인정보의 처리자를 서비스제공자의 이행보조자로 명시함으로써 개인정보의 침해에 따른 분쟁에서 이용자의 입증책임을 완화할 수 있다. 따라서 처리자의 손해배상책임에 있어서 서비스제공자와의 내부관계를 고려하여 부진정연대책임 또 사용자의 책임을 물을 수 있기 때문에 정보주체의 손해배상을 용이하게 해결할 수 있다. 이외에 이용자의 동의 없이 개인정보를 거래·양도하는 행위를 효과적으로 제재하기 위하여 경제적 제재인 과징금의 부과제도를 도입하여야 할 것이다.

(6) 이용자의 권리

이용자는 개인정보 수집이나 이용 및 제3자에게 제공에 대한 동의를 언제든지 철회할 수 있다. 이는 정보주체의 자기정보에 대한 결정권과 자기 데이터에 대한 재산권의 인정을 전제로 해석할 수 있다. 따라서 정보통신서비스제공자는 정보수집의 목적 또는 수령목적을 달성한 경우에 그 정보를 지체없이 파기하여야 한다. 이는 이용자의 일방적인 청구에 의해서 그러한 집행을 가능할 것인가의 문제가 있다. 적어도 이용자가 이러한 청구에 불응하거나, 실질적으로 파기하지 않고 불이행하는 경우에 500만원의 과태료를 부과할 수 있다. 이는 개인정보보호의 위반에 대한 제재로서 미약하다고 본다. 이는 계약관계에 기

초하지만, 개인정보 이용에 대한 동의를 언제든지 철회할 수 있는 근거는 개인정보의 재산가치의 처분권에서 찾을 수 있다. 이용자는 정보주체로서 자신의 개인정보에 대한 열람, 오류의 정정청구, 철회권을 허용한다(제30조). 특히 영업양수(양도)나 합병과 상속으로 그에 대한 권리승계인은 이용자에게 그 사실을 통지하고, 이용자의 권리와 그 행사방법을 알려야 한다(제26조). 이 경우에 문제는 기업합병에 있어서 개인정보를 기업자산의 평가대상으로 포함시킬 경우에 그 개인정보의 소유권에 대한 귀속여부는 중요한 법적 문제를 야기할 수 있다. 그러함에도 개정법률은 이러한 개인정보의 법적 성질을 고려하지 않고, 단순히 기업이 수집 및 보유하는 개인정보를 기업소유권으로 인정하여 처리하는 입장을 채택한 것이 아닌가하는 의문을 제기할 수 있다. 실제로 개인정보는 기업의 자산가치로서 중요한 경제적 객체인 동시에 소비자의 인권보호의 대상임을 고려할 경우에 구체적인 법제개선을 요구한다.

(7) 청소년의 보호조치 명시

14세미만의 아동으로부터 개인정보의 수집·이용·제3자 제공하는 경우 법정대리인의 동의를 받도록 한다. 법정대리인은 아동이 제공한 개인정보의 열람 및 정정 철회권을 갖는다(제31조). 14세미만은 형사미성년자로서 일본의 15세 이하, 미국의 13세 미만과 비교되는 개념이다. 정보통신망의 유해정보로부터 청소년을 보호하기 위하여 자율표시제를 시행하고자 한다. 정보통신윤리위원회는 청소년보호법의 청소년유해매체물의 결정 또는 확인되어 고시된 정보를 정보통신망으로 제공하는 자는 청소년유해매체물을 표시하도록 한다(제42조).

(8) 정보통신망에서 금지행위의 유형과 문제점

정보통신망의 이용자가 금지행위를 위반한 경우 형벌을 부과할 수 있다(제48,62조). 적법한 접근권한이 없이 또는 허용된 권한을 초과하여 침해하는 경우(해킹행위), 정당한 이유없이 통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 악성프로그램을 전달 유포하는 행위를 금한다(제48조 제2항). 누구든지 정보통신망에 의하여 처리, 보관 또는 전송되는 타인의 정보를 훼손하거나 비밀을 침해, 도용 또는 누설을 금한다(제49조). 물론 문제는 가상공간의 익명 이용을 전제하지만, 일반에게 공개목적으로 제공한 정보로서 법익을 침해받은 자는 서비스제공자에게 그의 삭제 또는 반론의 게재를 청구할 수 있다(제43조). 또한 성폭력, 명예훼손 등의 불법행위로 권익을 침해당한 경우 피해자가 정보통신서비스제공자에게 해당정보의 삭제 등을 요청할 수 있도록 하고 있다(제49조). 물론 광고성 정보전송(junk(spam) mail)을 제한하고 있다(제50조).

(9) 개인정보 분쟁해결의 사법의존 억제

통신망을 이용한 정보수집과 이용 및 처리에 관해서 개인정보침해의 우려와 수단 및 다수의 이해관계가 복잡하게 관련된다. 따라서 유럽연합을 비롯한 대다수 국가는 개인정보보호원(privacy commissioner, data register)을 설립하여 분쟁의 조정과 중재 등을 이용하여 대다수 사건을 당사자간의 화해나 타협에 의해서 해결함으로써 정보통신의 신기술의 개발에 따른 침해유형의 다양화와 법규범의 지연으로 법원에 의한 분쟁해결을 가능한 자제하는 입장이다. 따라서 우리도 법원에 의한 재판과정이 2차의 정보공개 내지 침해를 야기하기 때문에 당사자간의 사적자치에 의한 계약의 이행을 위해서 중재나 조정의 절차의 도입방안을 명시하고 있다(제52조). 즉 한국정보보호진흥원안에 개인정보분쟁조정위원회를 설치하도록

한다. 정보통신서비스제공자 이외의 자가 정보통신망을 이용하여 개인정보를 수집·저장·처리하는 경우에 개인정보보호관련 의무를 부여하고 있다. 개인정보관리책임자 및 개인정보취급자 등의 권한과 책임을 명시한다. 또한 인터넷주소자원 확충업무, 국가간 개인정보이전, 통신망에서 청소년보호의무, 통신망안전성 유지 등의 업무를 위해서 다른 국가나 국제기구와 협력하고(제53조), 서비스제공자가 이용자의 개인정보에 관하여 법위반의 계약체결을 금지하도록 규율하고 있다(제54조).

(10) 개인정보분쟁조정위원회

① 합의제 심의기관의 지위

개인정보에 관한 분쟁을 조정하기 위하여 위원장 1인을 포함한 15인 이내의 위원(1인은 상임)으로 구성되는 개인정보분쟁조정위원회를 도입하고 있다. 위원의 임기는 3년으로 연임가능하고, 위원장은 위원 중에서 정보통신부장관이 임명한다(제33조). 위원은 자격정지 이상의 형벌을 받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직 또는 해촉되지 아니하나 일정 경우의 제척·기피·회피사유가 있으면 당해 피해구제청구사건에서 배제된다(제35조).

② 분쟁조정의 업무

개인정보와 관련한 분쟁의 조정을 원하는 자는 위원회에 조정신청을 하고, 분쟁조정위원회는 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 그런데 60일의 기간은 너무 장기간으로 30일 정도로 정하되, 사건의 경중을 따져서 30일 연장을 가능하게 하여야 할 것이다. 조정 자체가 물론 법원의 판결에 비해서 단기임에는 분명하지만, 온라인에 의한 기술적인 자원에 의해서 전문가들이 참여하여 결정하는 경우에는 30일 정도의 단기간으로 충분하다. 그리고 분쟁조정을 위해서 필요한 자료요청은 정당한 사유가 없는 한 당사자가 협력할 의무가 있다(제37조).

③ 조정성립의 합의효력

당사자가 조정안을 통보를 받은 날로부터 15일 이내에 조정을 수락한 경우에는 분쟁조정위원회는 조정서를 작성하고 당사자가 기명 날인하여야 하고(제38조1항), 이때 당사자간에 조정서와 동일한 내용의 합의의 성립으로 간주한다(제4항). 이 분쟁조정은 일정한 분쟁해결을 위한 합의로서 「각종분쟁조정위원회 등의조정조서등에대한집행문부여에관한규칙」(제정 1992.3.2 대법원규칙 제1198호, 개정 1998.7.6)에 의하여 재판상의 화해와 동일한 효력이 있다. 따라서 합의문서에 대한 집행문의 부여절차와 기타 필요한 사항은 이 규칙에 의한다(제1조 참조). 부연하면, 법원 또는 법원의 조정위원회 이외의 각종 조정위원회, 심의위원회, 중재위원회 또는 중재부 기타의 분쟁조정기관(이하 "조정위원회"라고 한다)이 작성한 화해조서, 조정조서, 중재조서, 조정서 기타 명칭의 여하를 불문하고 재판상의 화해와 동일한 효력이 있는 문서(이하 "조서"라고 한다)에 대한 집행문의 부여 신청의 방식과 부여절차는 다른 법령에 특별한 규정이 있는 경우 또는 성질에 반하지 아니하는 한, 동 규칙이 정하는 바에 의한다(제2조). 결국 개인정보의 분쟁에 관한 조정은 재판상 화해와 동일한 효력을 부여하고 있지만, 조정이 성립하지 않는 경우에는 법원의 재판절차에 의하여 해결할 수 있다.

Ⅶ. 결 론

1. 일반적인 논의

우리가 직면하는 긴급한 과제는 개인정보보호를 위해서 시장접근, 자율규제, 및 정부규제의 방식을 어떻게 운용할 것인가를 결정하는데 있다. 엄격한 의미에서 개인정보가 데이터베이스에 의해서 수집되거나, 복제되고 있다. 개인정보 이용에 관련된 경제적 논의와 기술이 근본적으로 변하면서 개인정보의 이용을 규율하는 제도 메커니즘을 변경하지 않을 수 없게 되었다. 오늘날 개인정보보호는 대다수 산업전반에 걸쳐서 제기되고 있다. 예컨대, 의료데이터의 정보, 신용내역, 금융거래, 장거리 통신통화, 인터넷 화면보기(page per view), 비디오테이프 대여(VCR rental), 인터넷 서비스의 제공, 통신판매(direct mail)에 의한 구매 등이 있다. 사실 순수한 시장모델은 기업의 프라이버시보호정책에서 두 가지 제한을 볼 수 있다. 하나는 고객의 기호에서 따른 제한으로서 대다수 소비자가 기업의 프라이버시 정책에 기초하여 그들의 소비의사를 기꺼이 변경하면, 그만큼 기업은 시장변화에 따르게 된다. 다른 하나는 기업의 프라이버시 관행에 대한 공표로 따른 제한이다. 기업이 소비자의 기호를 충족시키고자 충실하게 고지하면 소비자의 선택을 촉진한다. 이러한 시장모델은 중요한 요소로서 소비자의 기호와 기업의 행위가 프라이버시에 대한 관심과 이해를 제고시킨다는 점이다. 기업의 규제로서 공표의 효과는 다음과 같이 매체가 프라이버시 문제를 감지하는 정도, 그 통지가 도달하는 범위, 소비자들의 그에 대한 반응정도에 달려있다. 정부기관이나 피해자와 같이 특정한 당사자는 법원에 소송을 제기하는데, 이러한 소송은 배상과 행위금지의 두 가지 목적을 달성한다. 즉 배상은 프라이버시의 침해를 당한 개인에게 그 피해에 대한 경제적 손해전보로 실현된다. 행위금지는 기업에 대한 인센티브를 강조하는데, 기업이 프라이버시의 침해행위로부터 기대하는 이익을 초과하는 프라이버시 침해에 따른 기대비용(배상과 제재를 포함하는 형태)을 지불하여야 한다.

이와 반면에, 정부규제방식은 시장접근이 개인의 프라이버시 보호에 매우 취약하다는 가정에 기초하는 대신 개인의 프라이버시의 보호는 법집행에 의해서 실현된다. 프라이버시 규범이 법령, 규제기관, 법원의 판결에 의해서 정해진다. 실제로 프라이버시에 관한 문헌들은 자기정보통제권을 강조하고 있다. 이러한 인권의 접근은 유럽의 데이터보호에서는 매우 중요하고 또한, 정부의 데이터 수집에서 기본적으로 발전되었다. 개인은 국가의 강제력에 구속되는 반면에, 사기업에 의한 데이터수집은 기업과 고객간의 계약관계에 있어서 시장실패 이 있다. 프라이버시에 대한 시장실패의 원인은 정보 및 협상 비용에서 기인한다. 정보비용은 기업과 고객간의 정보의 비대칭성(asymmetry) 때문에 발생한다. 고객보다는 기업이 그 정보를 얼마나 사용할 것인지를 더 잘 알고 있기 때문이다. 고객은 기업의 프라이버시 정책의 특성을 이해하는데 상당한 비용을 지불해야 한다. 기업의 프라이버시 정책에 대한 고객의 학습비용은 그 정책을 실제로 기업이 준수하는지 여부를 감시하기 어렵기 때문에 증대된다. 개인정보를 수집하는 기업의 인센티브를 고려하면, 그 정보를 충분히 사용하여 영업이익을 얻거나, 직접 마케팅을 하거나 또는 제3자에게 정보를 판매함으로써 그 수익을 획득한다. 계약의 관점에서 기업은 개인정보를 사용할 인센티브를 갖는데, 고객이 그러한 정보사용을 쉽게 허용하지 않더라도 억제가 곤란하다. 소비자가 기업의 프라이버시 정책의 이해와 감시능력이 부족함으로 프라이버시에 대한 높은 협상비용이 증대한다는 점이다. 이러한 어려운 협상과정의 비용이 시민들 전체의 프라이버시 법익을 초과하게 된다.

한편, 정부규제의 환상은 최소비용으로 정확히 최적의 규범을 집행할 수 있다고 가정한다. 공공이익을 위해서 수립·집행되는 규범에도 불구하고, 프라이버시에 대한 정부규제는 자칫하면 정부와 납세자에 대한 행정비용과 기업에 대한 집행비용을 증대시킨다. 방대한 양의 공공기록이 온라인으로 거래되고, 새로운 산업이 공공 및 민간 데이터를 개발하고 있다. 또한 다른 산업의 집행비용은 법규범의 유연성이 부족한데서 기인하고 있다. 그러한 변화가 적절하다고 정부기관이나 정책담당자가 공감할지라도 법규범을 변경하기는 어렵다. 이러한 유연성의 문제는 급격한 기술과 시장변화의 시기에는 특히 심각하다. 일련의 조건 속에서 공포된 법규범은 기술과 경제현실이 변동할 때에는 더욱 적절하지 않을 수 있다. 실제로 개인정보의 사용이 이러한 급격한 변화를 경험하면서, 규범이 급변하는 시장과 기술 현실에 충분히 능동적으로 적응하지 못하고 있다. 또한 규범의 경직성으로 인해서 의회가 제정한 법령은 중대한 집행비용을 초래하고 있다.

이 때문에 프라이버시의 위험이 높아지면서 강행규범이 이전보다 훨씬 많이 필요하다는 결론에 이르고 있다. 정부규제의 성과는 법규범이 시장, 기술 및 프라이버시 보호의 변화에 대처할 수 있는 역량에 달려있다. 특히 정부실패의 가능성은 공무원이 프라이버시 보호영역에서 공공복리의 실현 정도와 관련되는데, 만약 공무원이 무능하면 규제비용은 증대하고 효율성이 낮아진다. 공공선택이론에 따라서 공무원들은 막강한 이익집단의 영향을 받거나 또는 그들이 다른 목적, 예컨대 그 기관의 세력강화를 추구한다는 것이다. 프라이버시(privacy)법에 대한 이익집단의 영향력을 고려하면, 정치과정이 산업 또는 소비자의 지위를 강조할 것인지는 분명하지 않다. 더구나 공무원의 전문성이 결여되거나 또는 이익집단의 각종 로비에 무력한 경우에 정부실패를 초래할 수 있다. 이를 대비하여 공무원의 전문성을 전제조건으로 인적 및 업무의 독립성을 법적으로 보장하여야 한다. 또한 국가기구의 운영에 있어서 예산과 업무집행에 대한 감독방식을 어떻게 보완할 것인지가 핵심과제이다.

요컨대 정부규제만이 민간의 개인정보를 효율적으로 보호하는 수단이 아니다. 온라인 환경에서 개인정보는 정보주체, 정보제공자, 정보처리자 등에 의한 개인정보의 오·남용의 억제는 온라인에서 정보유통에 따른 침해를 용이하게 포착할 수 없다. 때문에 개인정보보호를 위한 정부규제의 보충방안으로서 자율규제도 적극 권장하는 정책이 중요하다. 사업자가 자율적으로 적절한 수준의 개인정보지침을 실천함으로써 시장신뢰를 구축할 수 있다. 따라서 정부와 민간 모두가 프라이버시보호의 자율규제를 병행하는 동시에 프라이버시의 보호기술개발도 활성화하여야 한다.

2. 구체적인 논의

향후 우리의 프라이버시 법제는 시급한 과제로서 (가칭) "개인정보보호법"을 이법화하되, 다음과 같은 몇 가지 선행조건을 충족하여야 할 것이다.

첫째, 공공부문의 개인정보와 민간부문의 개인정보보호를 중(장)기적으로 통합하여 운용하되, 현재는 민간부문과 공공부문을 분리하여 운용함이 가능하다. 이를 위해서는 개인정보은행(personal data bank)을 창설하여 민간부문의 개인정보와 공공부문의 개인정보를 통합가능성을 대비한다. 특히 민간부문의 정보시장을 활성화하는 조건으로서 현행 주민번호 제도는 특정한 행정목적의 운전면허, 납세자번호, 의료보험제도에 의한 특정하고 제한적인 ID제도로 전환되어야 한다. 현행 주민등록번호제도는 OECD나 유럽연합의 협약에 비추어보면 정보보호원칙에 반할 뿐만 아니라, 현행 헌법상 사생활의 비밀과 자유 및 정보

자기결정권에 명백하게 위배된다는 점을 상기할 필요가 있다.[30]

둘째, 현행 공공부문의 개인정보보호는 각 공공부문에 정보담당관을 선임하여 우선적으로 개인정보감독기구의 지원과 협력에 의해서 사실조사와 고충처리를 시행하고, 이를 보충하는 분쟁조정위원회의 조정과 합의절차를 거치도록 한다. 이러한 합의 자체에 불만이 있는 경우에는 직권에 의한 형사고발이나 법원에 손해배상의 재판절차를 거치도록 한다. 중대한 사안은 개인정보감독기구의 자문을 거쳐서 공공기관의 장이 형사고발을 할 수 있고 또는 민간부문에서의 개인정보분쟁에 대한 조사 및 분쟁조정을 전담하도록 한다. 이러한 감독기구는 중앙Q분만 아니라 지방사무소를 설치하여야 한다. 물론 각 지방자치단체의 특성을 고려하여 단계적으로 지자체의 감독사무소를 설치할 수 있다.

셋째, 개인정보은행은 모든 행정의 공정성과 투명성, 특히 과세의 투명성을 확보하기 위해서 중요한 기구이다. 개인정보은행은 접근과 이용에 따른 모든 인적 및 물적 사항에 대해서 기록을 하는 점에서 향후 국민들의 행정수요와 과거의 행정수요를 예측하거나 평가할 수 있기 때문에 중요한 행정목적의 기능을 기대할 수 있다. 개인정보은행은 각 지역마다 독립적으로 운용하기 때문에 지방자치단체가 정보처리 및 관리자로서의 정보사회의 주도자로서 기능을 강화할 필요도 있기 때문에 중요한 의의를 갖는다.

넷째, 민간부문에서 사용하는 개인정보로서 개인 ID제도를 사용하는 것을 억제하여야 한다. 특히 기업이나 단체가 수집 및 처리하여 데이터베이스화하는 개인정보의 소유권에 대한 명확한 입법방침이 전제되어야 한다. 이를 방치하는 경우에 정보자기결정에 근거하여 사업자가 개인정보 주체와 계약에 의한 이용강제나 불공정한 데이터사용을 조장할 우려가 있다. 그러한 결과로 정보산업에 대한 사후 규제조치가 현실성이 없는 것으로 실패하거나 공무원의 무능으로 인해서 정부규제의 실패를 초래할 것이기 때문이다.

다섯째, 민간과 공공부문의 개인정보에 대한 규제정책은 시민사회의 자율성과 독립성을 갖은 시민단체들의 권리주장과 정책형성에 대한 참여를 통해서만이 진정한 권리의 실현이 가능하다. 따라서 정부가 사업자단체나 기업들의 입법로비에 의해서 일방적인 이익을 보장하거나 또는 소비자의 이익을 희생시키는 우를 범하지 않도록 감시와 비판기능을 한층 강호하기 위해서는 국제NGO 단체들과 유기적으로 연대할 수 있는 계기를 마련하여야 한다.

30) 자세한 내용은 정영화, "현행 주민등록번호의 헌법문제와 행정개선방안", 민주사회와 변론, 민주사회를 위한 변호사모임, 2001(3/4), 참조.

■ 참고문헌 ■

김철수(2000). 헌법학개론, 박영사.
정영화(2000). 전자상거래법 (제1판), 다산출판사.
———(2001) 전자상거래법 (제2판), 다산출판사.
———(2000). 사이버스페이스와 프라이버시", 헌법학연구(제6권 제3호), 한국헌법학회.
———(1999). "전자정부에서의 공공정보의 접근 및 유통에 관한 법정책론 연구", 공법연구(제27권 제2호), 한국공법학회.
———(2000). "정보법령에 관한 법이론", 세계헌법연구(제5권), 국제헌법학회한국학회.
———(2000), "가상공간에서의 프라이버시 연구", 한국주관성학회 정기학술대회 발표논문
———외(2000), 개인정보보호 감독기구 도입을 위한 법제개선방안연구, 한국정보보호센터
한국정보보호센터(1999). 정보화 역기능 실태조사.
한국전산원(1997). 정보사회의 정보이용자 권익향상 방안.
헌법재판소, 헌재판례집, 제1권-제7권 2집
Alan F. Westine(1967). Privacy and Freedom, Atheneum(N.Y.), 1967
Edward Bloustine(1964). "Privacy As an Aspect of Human dignity," 39 New York University Law Review
Ethan A. Nadelman. "Drawing the Line on Drug Testing",(Onlinr available); http://www.lindesmith.org/library/ethan-drugtesting2.html.
Fred H. Cate(1997). Privacy in the Information Age, Brookings Institute Press.
Geoffery R. Stone and Richard A. Epstine, Bill of Rights in the Modern State, The University of Chicago Press, 1992.
Graham Pearce and Nicholas Platten, "Achiving Personal Data Protection in the European Union", Journal of Common Market Studies, Blackwell Publishers Ltd, 1998.
James Gleick(1996). "Behind Closed dooes: Big Brother Is Us", New York Times, September 29.
Marc Rotenberg, The Privacy Law Source Book 1999, EPIC(Washington DC), 1999.
Murry long and Suzanne Morin LL.B, The Canadian Privacy Law Handbook- Applying Canada's New Private Sector Privacy Law, Centrum Information, 2000.
Ruth Gavison(1980). "Privacy and the limits of Law," Yale Law Journal 421.
Samuel Warren and Louise Brandeis(1890), " the right to Privacy", Harvard Law Review.
Volio Fernando(1981). "Legal personality, Privacy and Family", in Henkin(ed), The International Bill of Rights, Colombia University Press.
ACLU, Genetic discrimination in the Workplace Fact Sheet
http://www.privacy.org/piccountries/hungary/hungarian-id-decision-1991.html
http://www.bknet.org/laws/nationalid.html
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)
기타 주요국가의 privacy act 참조

[기조발제-2]

개인정보 보호와 프라이버시에 관한 몇 가지 법적 이슈

이은우(민주사회를위한변호사모임, 변호사)

I. 우리의 개인정보 보호에 관한 법률체계

1. 개인정보보호에 관한 법제의 현황(2001. 5. 24. 현재)

현재 우리나라에는 개인정보의 보호에 관한 일반법은 없고, 분야별로 세분된 개인정보 보호에 관한 법률들이 있다.

(1) 공공기관의개인정보보호에관한법률 : 공공기관이 보유하고 있는 개인정보의 보호에 관한 법률
(2) 정보통신망이용촉진등에관한법률 : 정보통신서비스제공자의 개인정보보호에 관한 법률
(3) 신용정보의제공과이용에관한법률 : 신용정보의 보호에 관한 법률
(4) 통신비밀보호법 : 통신과 대화의 비밀보호
(5) 기타 개별법 : 의료법, 약사법, 회계사법, 변리사법, 보험업법 등

2. 문제점

(1) 프라이버시보호에 대한 기본적인 인식의 미비 : 주민등록제도.

(2) 통합적인 법률의 부재 : 개인정보와 관련한 프라이버시 기본원칙(개인정보 수집이나 제3자 제공시 동의, 개인정보의 정확성과 안전성 보장, 통합의 금지 등)을 모든 부문에서 관철시킬 수 있는 법률의 부재. 현재 정통망법의 개정으로 범위를 확대하였으나 대통령령에 범위를 위임함(개정 정보통신망이용촉진및정보보호에관한법률 제58조 정보통신서비스제공자외의 자로서 재화 또는 용역을 제공하는 자중 대통령령이 정하는 자에게도 준용됨). P2P 기술의 발달, 마케팅 기술의 발달로 소비자보호운동의 중요한 문제임.

(3) 기술의 발전에 따른 개인정보 유출가능성에 대한 적극적인 규정의 미비 : 기술의 발전은 개인정보의 유출가능성을 기하급수적으로 늘려가고 있음. 개인정보가 범죄적 행위로 인하여 유출될 경우 입게 되는 피해는 매우 클 것임. 현재의 법률 규정은 이러한 개인정보의 유출가능성에 대해서는 무방비인 상

태임. 개인정보보호를 위한 기술발전의 촉진을 위한 강제력이 있는 법률규정의 마련할 필요가 있음(규제와 조장의 양 측면에서. 예컨대 기술적 보호조치의 수준에 대한 가이드라인, 컴퓨터 프로그램의 허점으로 인한 개인정보의 유출가능성에 대한 대응수준을 높일 필요, 기술개발의 촉진).

(4) 개인정보보호를 위한 실효성있는 구제수단이 미비 : 현재 소송상의 구제의 곤란.

(5) 개인정보 수집, 제3자 제공, 통합에 대한 당사자의 동의를 얻으면 가능하도록 하고 있는 원칙을 재고할 필요성은 없는가?

II 발신번호표시서비스와 개인정보보호 및 프라이버시 보호

1. 발신번호표시서비스의 도입

(1) 발신번호표시서비스의 도입취지

정보통신부는 2001. 4. 1. 부터 발신번호표시서비스를 도입하기로 하였다. 정보통신부는 그 도입배경으로 전화 익명성을 악용한 음란·협박·폭언 등 전화폭력이 이미 위험수위를 넘어섰으며 최근에는 특정인에게 집요하게 전화를 걸어 괴롭히는 '전화 스토커'와 이해집단 구성원들의 '항의전화'가 등장, 새로운 사회문제가 돼왔다는 점을 들고 있다.

정보통신부는 우리나라는 95년부터 전화폭력을 받은 수신자에게 '통화종료후 발신번호확인서비스'를 제공해 왔으나 신청절차가 번거롭고 이미 전화폭력을 받은 뒤에 이뤄져 통신 사생활을 근본적으로 보호하는 데는 한계가 있었다면서 새로운 제도의 도입이 불가피했다고 밝히고 있다.

(2) 발신번호표시서비스의 내용

발신번호표시서비스는 ▲수신자가 모든 발신번호를 받아보도록 하되 ▲발신자는 전화번호부 등재방식처럼 발신번호표시를 거부할 수 있고(통화별로 발신번호표시를 거부하는 방법과 아예 회선자체의 발신번호표시를 거부하는 방법이 있다) ▲수신자도 발신번호를 표시하지 않는 익명전화를 거부할 수 있으며 ▲특수번호와 전화폭력 등의 경우에는 언제나 발신번호가 표시되도록 운영된다. 한편 발신번호표시서비스를 이용하려면 액정표시창을 지닌 전용전화기를 사거나 기존 전화기에 별도의 표시장치를 붙여 통신업체에 서비스를 신청해야 한다.

발신자가 자신의 전화번호를 수신자 전화기에 표시되지 않도록 하려면 전화를 걸 때마다 일정한 식별번호를 누르거나(통화별 블로킹), 아예 그 회선의 발신번호가 표시되지 않도록 하는 '회선-블로킹서비스'를(회선별 블로킹) 사업자에게 신청해 놓으면 된다. 이는 발신자 보호를 위한 것으로서 서비스 요금은 무

료다.

수신자도 '블로킹'일 경우 수신자 전화기 표시창에 이를 표시하는 '블로킹호 표시' 서비스, 또는 블로킹호를 자동으로 수신 거부하는 '블로킹호 수신거부' 서비스를 이용할 수 있다.

다만 협박이나 폭력전화를 받은 수신인이 통신사업자에게 신청하면 발신자가 발신번호표시를 거부하더라도 표시가 된다. 범죄신고(112)나 화재조난신고(119) 등 특수번호도 언제나 발신번호가 표시된다.

유선전화의 경우 전전자교환기 1,600만 회선은 서비스 개시시점부터 전면 제공되고 반전자교환기 865만 회선은 우선 '호-블로킹' 서비스만 제공되며 '회선-블로킹'은 내년 7월부터 제공된다.

(3) 정보통신부가 주장하는 도입효과

전화폭력 방지 말고도 다양한 부가서비스가 가능해 유선전화도 단순한 음성통화용에서 고도의 정보통신 수단으로 변모하는 계기가 될 전망이다. 발신번호가 표시되는 액정화면을 이용하면 이메일, 인터넷 정보이용·검색 등 데이터 부가서비스가 가능하며 부재중에 걸려온 전화번호를 확인할 수 있어 맞벌이부부 등에게는 매우 유용하다.

이는 유선전화 분야에 새로운 수익원이 될 수 있으며 액정화면 전화기가 대량 개발 보급돼 유선전화기 시장규모가 매년 30% 이상 늘어나 2003년에는 지난해 보다 121% 늘어난 3,980억원 규모가 될 것으로 예상된다.

(4) 정보통신부가 제시하는 앞으로의 보완사항

번호표시를 할 수 없는 구식 교환기가 문제. 496만 회선의 반전자교환기 전체와 초기 전전자교환기 369만 회선 등 전체의 35.1%인 865만 회선이 이 서비스를 제공할 수 없다. 이들 교환기는 특히 대도시의 37.5%, 서울에는 51.6%가 집중 배치돼 있다.

따라서 올해 반전자교환기 대·개체 예산규모를 당초 1,240억원(178만 회선)에서 2,000억원(260만 회선)으로 늘려 서비스 이용불가능 비율을 30% 이내로 줄이고 나머지 235만 회선도 당초 2004년보다 1년6개월 앞당겨 2003년 상반기까지 모두 교체할 계획이다. 서울지역의 서비스 이용불가능 비율도 올 11월까지 40% 이내로 줄인다.

또 다른 과제는 전화번호 노출을 꺼리는 가입자들 불만. 지난해 인터넷 여론조사 결과 응답자의 85.1%가 서비스 도입에 찬성했지만 실제 서비스 시행 초기에는 블로킹기능 등을 이해하지 못하는 이용자들의 불만이 예상된다. 정통부는 업계와 공동으로 28억원의 예산을 들여 홍보활동과 번호표시서비스 공개신청 등으로 이 제도를 국민들에게 널리 알리는 데 주력할 방침이다(정보통신부 보도자료 참조).

2. 발신번호표시서비스의 여러가지 형태

(1) 발신번호표시서비스와 자동발신번호표시서비스

(i) 신청한 자에게 번호 표시를 허용하는 발신자의 발신번호만을 표시해 주는 발신번호표시서비스(Caller Idnetification Service)와, (ii) 모든 발신자의 번호가 자동적으로 기록되는 자동발신번호표시서비스(Automatic Number Identification)가 있다. 예를 들어 112나 119같은 긴급전화의 경우는 모든 발신자의 번호가 자동적으로 기록되는 자동발신번호표시서비스가 적용된다. 한편 미국의 경우 800이나 900(수신자 요금부담 서비스)의 경우 요금의 계산을 위해서 자동발신번호표시서비스를 적용하고 있다.

(2) 발신번호만 표시하는 서비스와 발신자의 성명, 주소 등을 표시하는 서비스

표시되는 내용에 있어서도 발신번호만을 표시하는 발신번호표시서비스와 발신자의 성명, 주소 등의 개인정보까지 같이 표시하는 서비스가 있을 수 있다.

3. 발신번호표시서비스의 법적 문제

(1) 법적근거

전기통신사업법 제54조의2 (송신인의 전화번호의 고지 등)
① 전기통신사업자는 수신인의 요구가 있는 경우에는 정보통신부령이 정하는 바에 의하여 송신인의 전화번호 등을 알려줄 수 있다. 다만, 송신인이 전화번호 등의 송출을 거부하는 의사표시를 하는 경우에는 그러하지 아니하다.
② 전기통신사업자는 제1항 단서의 규정에 불구하고 전기통신에 의한 폭언·협박·희롱 등으로부터 수신인을 보호하기 위하여 정보통신부령이 정하는 바에 의하여 수신인이 요구를 하는 경우와 특수번호 전화서비스중 정보통신부령이 정하는 경우에는 송신인의 전화번호 등을 수신인에게 알려줄 수 있다. [본조신설 2001

아직 정보통신부령에는 개정법률이 반영되지 않았음.

(2) 개인정보 보호의 기본원칙에 합당한가?

개인정보 보호의 기본원칙은 개인정보를 수집 또는 제공하기 위해서는 당사자의 동의를 얻어야 한다는 것이다. 동의라고 볼 수 있으려면 당사자에게 정보수집 또는 정보제공의 목적, 상대방, 제공되는 정보의 내용 등에 관하여 충분히 알 수 있도록 명시적으로 이를 게시하거나 설명한 후 당사자의 동의를 받아내야 한다. 과연 현재의 발신번호표시서비스는 당사자의 정보수집, 정보제공의 동의를 얻은 것으로

볼 수 있는가? 특히 700, 080 서비스 등에 발신번호자동기록을 도입할 경우에는 더 큰 문제이다.

(3) 발신번호표시서비스는 사업자를 위한 제도이다

발신번호표시서비스는 사업자를 위한 제도이다. 이 제도가 본래 목적하는 장난전화, 음란전화 등은 발신번호표시거부를 택할 경우 실효성이 없다. 그러나 발신번호표시서비스는 사업자들에게는 매우 유용한 개인정보를 수집할 수 있는 서비스이다. 전화번호가 각 사업자별로 축적이 될 경우 그것이 가지는 경제적 가치는 매우 클 것이다. 미국의 경우 발신번호표시서비스를 통한 사업자들의 이익은 천문학적인 액수에 이른다고 한다.

우리나라의 경우 발신번호표시제도가 도입되고 몇 달 내로 텔레마케팅관련 사업이 번창할 것이 분명하다. 특히 우리나라의 경우 텔레마케팅에 대한 규제가 없으므로 더더욱 그러하다.

(4) 익명권의 보장

공공기관에 대한 의견의 표시, 이익단체에 대한 의견의 표시 등에 있어서 익명으로 남아있을 권리는 프라이버시와 표현의 자유의 보장을 위해 필요하다. 그러나 발신번호표시서비스는 이러한 익명권을 침해한다.

(5) 알리고 싶지 않은 정보의 제공

전화를 거는 사람은 자신의 신원, 거주지, 이름 등이 공개되지 않으리라는 기대를 한다. 그러나 발신번호표시서비스는 그 기대를 무너뜨린다. 전화번호는 가입자의 이름, 거주지를 드러내며(전화번호부에 이름과 거주지를 공개하는 경우), 특히 전화번호는 내밀한 프라이버시의 영역이고, 프라이버시의 최후보루라고 할 수 있는 가정을 직접 대표하는 유일한 값이기 때문에 매우 심각한 개인정보이다. 그리고 전화번호는 가정마다 유일한 값이므로 여러 다른 정보(예를 들어 의료정보와 신용정보)와 통합될 경우 프라이버시 침해의 위험은 더욱 커진다. 그리고 전화번호는 아무런 중간 매개없이 직접 외부와 연결이 되는 통로역할을 하므로 전화번호 공개에 따른 프라이버시 침해의 현실성은 다른 정보에 비해 높을 수 밖에 없다.

(6) 수집 및 이용의 제한가능성

현재는 없다. 2001. 7. 1. 부터 시행되는 정통망법에 의하면 대통령령이 정하는 사업자의 경우 수집한 정보의 제3자 제공의 금지, 수집목적 외의 사용금지, 목적달성시 폐기 등의 의무가 부과된다. 그러나 전화번호의 경우 우리나라는 텔레마케팅에 대한 규제가 없으므로 그 실효성은 매우 낮을 것이다. 전화번호가 매매되어도 텔레마케팅업체가 전화를 하는 것에 대한 규제가 없으므로 매매된 사실이 입증이 되지 않는다면 현실적으로 적발 내지는 처벌이 곤란할 것이기 때문이다.

3. 대 책

(1) 최선책

폐기가 바람직하다. 얻을 수 있는 장점에 비해 피해가 너무 크기 때문이다. 더욱 더 큰 문제는 잠재적인 위험이다.

(2) 차선책

도입이 시기상조이다. 국민들의 개인정보보호에 관한 인식이 충분치 못하기 때문이다. 그에 반해 텔레마케팅업체들의 개인정보수집 및 오용에 대한 동기는 너무나도 크다. 최소한 대등한 입장이 되도록 홍보 및 교육이 이루어지고, 개인정보유출에 대한 효과적인 제도적 장치가 마련된 후에 도입되어야 할 것이다.

(3) 삼선책

텔레마케팅에 대한 규제가 도입되어야 한다. 미국의 경우 텔레마케팅업체에게 거부의 의사표시를 한 경우 1년에 1회를 초과하는 영리목적의 전화가 오는 경우에는 500$ 또는 피해액 중 큰 금액을 손해배상하도록 입법이 마련되어 있다. 그리고 텔레마케팅 전화에 대한 몇 가지 규제가 이루어지고 있다. 사업자나 공공기관 등에게는 발신번호표시서비스를 제공하지 않는 것도 연구해 볼만한 하나의 방법일 수 있다. 전화번호의 매매나 오용에 대한 강력한 처벌입법이 마련되어야 하고, 보관기간, 외부유출에 대비한 안전성 확보의무 등이 마련되어야 한다.

III 사업장에서의 개인정보 보호(감시)

1. 컴퓨터 단말기, 전자메일(음성메일), 인터넷 등 감시도구의 비약적 발달

2. 전화나 전자메일의 감청 내지는 검열의 허용여부

(1) 전화의 감청 : 동의를 받아야 함.

(2) 전자메일의 검열 : 동의를 받아야 함.

(3) 컴퓨터 이용의 검열 : 현재 법률의 규정이 없음.

IV 주민등록번호의 보호

1. 국민에 대한 고유한 ID 번호의 부여 문제

2. 주민등록번호로 공개되는 정보

3. 주민등록번호의 남용

4. ID theft

V. 텔레마케팅에 대한 규제

1. 현행법률

방문판매등에관한법률이 텔레마케팅을 규제하는 법률임. 이 법률에는 철회권의 보장, 광고의 표시사항, 손해배상의 제한 등에 대한 규정만 있음. 텔레마케팅 행위 자체에 대한 규제가 없음

2. 미국의 전화소비자보호법(Telephone Consumer Protection Act of 1991)

(1) 발신금지요구자 목록

소비자의 요구가 있을 경우 텔레마케터는 발신자 리스트에서 삭제하여야 하고, 발신금지요구자 리스트를 운영하고 있음을 명시적으로 문서를 통하여 밝혀야 한다.

만약 발신금지요구를 했는데도 1년에 1회를 초과하는 전화를 할 경우에는 텔레마케터에게 발신금지를 요구하고, 손해배상(징벌적 배상)을 할 수 있다. 배상액은 500$과 실손해액 중 큰 금액으로 한다. 만약 텔레마케터가 과실이 아닌 고의로 전화를 한 것이 확인될 경우에는 1500$과 실손해액 중 큰 금액을 배상하여야 한다.

위와 같은 위반사항이 있을 경우 연방통신위원회에 제재를 요구할 수 있다.

단 세금이 면제되는 비영리 단체의 경우는 예외로 한다.

(2) 전화발신 시간의 제한

상대방의 동의가 없는 경우 또는 양자간에 영업관계가 형성되어 업무수행을 위하여 필요한 경우 외에는 텔레마케터는 오전 8시부터 오후 9시 사이에만 전화발신을 할 수 있다.

(3) 팩스의 사용

텔레마케터는 팩스기나 컴퓨터 등을 이용하여 상대방의 사전 동의없이 영리성 광고를 내용으로 하는 팩스를 보내서는 안된다.

(4) 녹음된 메시지나 자동전화발신장치 사용

텔레마케터는 상대방의 동의가 있거나 긴급한 상황에 대처하기 위한 목적이 아닌 경우에는 녹음된 메시지나 자동전화발신장치를 사용할 수 없다. 녹음된 메시지는 비상업적 목적이나, 사전에 영업적인 관계가 형성된 경우, 상업적 광고가 포함되지 않은 경우, 세금이 면제되는 비영리단체만이 사용할 수 있다.

긴급 전화와, 병원, 휴대폰, 페이저에 대한 자동전화발신과 녹음된 메시지의 이용, 수신자가 비용을 부담하도록 하는 자동전화발신과 녹음된 메시지의 이용은 금지된다.

녹음된 메시지에는 사업의 명칭과 전화를 건 자나 법인의 명칭 등이 녹음메시지의 시작부분에서 언급되어야 한다. 텔레마케터는 주소나 전화번호를 알려주어야 한다.

3. 미국의 텔레마케팅과 소비자 사기방지법(The Telemarketing and Consumer Fraud Abuse Prevention Act)

(1) 발신금지요구자 리스트 : 전화소비자보호법과 유사

(2) 시간제한 : 전화소비자보호법과 유사

(3) 발신자 정보공개 : 텔레마케터는 (i) 판매전화라는 점, (ii) 판매하는 물품이나 용역이 무엇인지, (iii) 판매자의 신원을 즉시 명확하게 밝혀야 한다.

4 전화소비자 보호와 텔레마케팅의 규제에 관한 법률의 도입필요

(1) 발신번호표시서비스의 도입에 따른 법률의 정비필요

발신번호표시서비스의 개시로 사업자들의 발신번호의 수집과 이용이 급속히 확산될 것임. 그러나 현재 법률이 미비하고, 소비자와 사업자들의 개인정보보호의식이 낮기 때문에 발신번호의 남용과 오용이 우려됨.

발신번호의 수집과 이용의 제한, 텔레마케팅의 규제, 처벌규정의 신설 및 강화가 필요함.

(2) 전기통신사업법

전기통신사업법에서 발신번호의 수집과 이용의 제한규정을 두어야 한다. 해당번호 가입자의 사전동의를 얻도록 할 필요가 있다. 정통망법은 개인정보의 수집과 이용에 당사자의 사전동의를 요구하나, 정통망법 규정이 포괄하는 범위 밖일 가능성이 있고, 전화번호라는 개인정보의 내밀성으로 인하여 보다 강력한 규제가 필요하므로 별도의 입법이 요구된다. 전화번호 정보의 통합의 금지조항도 고려해 볼 필요가 있다.

(3) 방문판매등에관한법률

텔레마케팅(통신판매)에 대한 규율이 필요한데, 방문판매등에관한법률에 신설하는 것이 바람직하다.

그 내용은 미국의 전화소비자보호법의 규정처럼 발신금지요구제도, 배상제도, 발신시간의 제한, 발신자의 정보공개, 자동전화발신장치와 녹음된 메시지의 이용제한 등의 내용이 포함되어야 할 것이다. <끝>

[사례발표-1]

주민등록관련 피해사례 실태 및 주민등록번호문제의 환기

윤현식(주민등록법 개정을 위한 행동연대)

Ⅰ. 들어가며

주민의 거주관계 등 인구의 동태를 상시로 명확히 파악하여 주민생활의 편익을 증진시키고 행정사무의 적정한 처리를 도모[31]하기 위하여 제정되고 시행되는 현행 대한민국 주민등록법은 나름의 타당한 목적성을 가지고 있으며 효과적으로 운영되고 있는 듯이 보인다. 그러나 도처에서 주민등록법과 관계된 문제들이 나타나고 있으며, 특히 개인정보의 보호와 프라이버시 보호라는 차원과 관련하여 주민등록법의 문제들이 더욱 부각되어 나타나고 있다.

주민등록법 자체가 가지는 문제점은 우선 목적범위를 넘어선 과도한 정보의 수집 및 관리가 이루어지고 있으며, 이렇게 수집되고 관리된 정보가 정보주체의 동의 없이 오용되거나 남용될 가능성이 대단히 높다는 것이다. 두 번째 문제와 관련하여 특히 행정전산망이 더욱 체계적으로 갖추어지면서 해킹 등에 의한 불법접근 및 도난, 또는 파손의 사례가 갈수록 늘어가고 있는 현재의 추세를 바라보면 개인정보와 프라이버시의 보장에 대한 불안감은 더욱 증폭될 수밖에 없는 상황이다.

그러나 지난 수 십 년의 세월동안 국가안보와 사회질서유지라는 당위론적 목적의식에 길들여진 국민들은 이러한 위기감을 실제로 느끼면서도 이 위기감의 근본 원인인 주민등록법에 대해서만은 필요성이라는 측면에 경도되어 문제를 제기하지 않거나 아예 문제점을 느끼지 않고 있는 것이 현실이다. 또한 주민등록법 자체가 개인에 대하여 특정한 형태의 직접적인 침해사례를 구성하는 일이 거의 없다는 것도 국민의 이러한 인식에 중대한 영향을 끼치는 한 요인일 것으로 파악된다. 따라서 위에서 언급한 두 가지 주민등록법의 문제점 자체는 단기간 내에 국민일반의 정서로 파급되기는 어려울 것으로 생각된다.

그럼에도 불구하고 지난 몇 년 동안 주민등록법 및 주민등록증에 대하여 국민이 심각한 의문을 제기할 만한 사건이 있었고, 이러한 의문을 기반으로 부당한 주민등록법의 내용 및 시행상황에 대한 비판이 형성되었음은 고무할만한 일이 아닐 수 없다. 특히 1996년 스마트 카드 도입이 사회적인 이슈가 되었던 때에 고조된 프라이버시에 대한 인식과 1999년 플라스틱 주민등록증의 발급과 때를 맞추어 지문날인에 대한 문제가 제기 되었으며 더 나아가 시민운동의 차원에서 지문날인 거부가 진행되었던 것은 높이 평가해야할 부분이다.

31) 주민등록법 제1조(목적)

이러한 인식의 고양과 시민운동의 태동에도 불구하고 아직까지 주민등록법을 비롯한 국가등록제도에 대해 전 국민적 비판이 형성되지 못하는 것은 국민들이 아직까지 지문을 찍거나 함부로 주민등록번호를 사용하는 것을 침해 자체로 인식하지 못하고 마치 당연한 일인 것처럼 인식하는데서 기원한다. 따라서 주민등록법 및 이와 관련된 부대상황에서 직접적인 침해가 일어났거나 침해의 가능성이 있는 사례를 확인함으로써 앞으로 어떤 일이 일어날 수 있는지를 예측해 보는 것은 중요한 인식형성의 과정이라고 생각한다. 이러한 문제의식을 바탕으로 주민등록법과 관계되었거나 혹은 주변적 상황이지만 반드시 짚고 넘어가야할 사례들을 확인하고 이에 대하여 간단하게 고찰하도록 하겠다.

Ⅱ. 구체적 피해사례

1. 과도한 개인정보의 요구

(1) 물건은 아무나 반납하나?

한 시민이 영등포의 한 백화점에서 물건을 구입하고 난 후 생각이 바뀌어 바로 반품을 하고 환불을 신청했는데 영수증 반환과 함께 주민등록번호, 주소, 전화번호, 성명, 판매일자 및 반품사유를 쓰도록 요구하였다. 이 시민은 해당직원에게 이의를 제기하고 개인정보의 유출을 피하려 하였으나 그 결과 상당한 시간을 환불을 위하여 소요해야했으며, 직원들로부터 불친절한 대접을 받아야만 했다.[32]

(2) 범죄제보도 개인정보와 함께

서울 강남경찰서는 범죄신고·제보나 불편사항 등을 신고하기 위해 강남경찰서 홈페이지(kn.smpa.go.kr) '열린경찰서'나 자유게시판에 들어가면 제목과 함께 이름, 주민등록번호, 연락처, 이메일, 내용, 비밀번호를 입력하는 상자가 나온다. 그리고 상자 위에는 "기입사항을 전부 입력해야 답변드리는 데 도움이 될 것"이라는 문구가 나온다. 시민들은 여기에 대해 자유게시판에 글을 올리는데 까지 개인정보를 요구할 필요가 있는가와 개인신상정보의 강제적 기입이 시민들의 의사표현을 제약할 수 있음을 항의하였으나 강남서의 관계자는 "마구잡이식" 게시를 방지하고자 했다고 대답하고 있을 뿐이다.[33]

(3) 학생증은 신분증이 아니랍니다

한 이동통신업체는 이동통신서비스 가입시에는 학생증으로 가입을 하게 해주었으나 해지를 하려고 하자 주민등록증이나 운전면허증이 있어야만 해지가 가능하다고 요구하였다. 이 학생은 당장 주민등록증을 발급받을 수 없는 상황이 있음을 설명하는 한편 가입당시에는 분명히 학생증으로 신원을 확인하였다는 것을 밝혔으나 해당 이동통신업체는 끝내 해지를 해주지 않았고 이 학생은 계속 기본요금을 납입하게 되었다. 이동통신업체의 입장은 학생증은 해당학교가 학교 내에서만 신원을 확인하기 위한 목적으로 만들어진 것으로서 학교 이외의 곳에서 신원확인을 위한 기능을 할 수 있는 것이 아니라는 것이다. 그렇다면 애초 가입당시에 이러한 사실을 이야기해주었더라면 이 학생의 경우 이와 같은 피해를 입지 않았

32) 인터넷 한겨레. 2001년 4월 20일
http://www.hani.co.kr/section-001042000/2001/05/001042000200105031828703.html
33) 인터넷 한겨레, 2001년 4월 10일.
http://www.hani.co.kr/section-005000000/2001/04/005000000200104100203071.html

을 것임에도 불구하고 가입할 때와 해지할 때의 신원확인 기준이 달라짐으로 인하여 입은 피해에 대해서는 책임을 지지 않고 있다.[34]

(4) 남들 다 하고 안 하면 서운하고 ...

주민등록법 개정을 위한 행동연대의 조사에 따르면 회원가입제 인터넷 웹사이트의 경우 무작위로 선정된 총 547개 사이트 중 주민등록번호를 요구하는 곳은 500개 사이트(91.41%)였고, 주민등록번호를 기재하지 않는 사이트는 31개 사이트(5.67%)였으며 주민등록번호의 기재가 선택사항인 곳은 모두 16개 사이트(2.92%)였다. 모든 사이트들은 성명, 주소, 연락처, 이메일 등의 개인정보사항을 필수로 기재하도록 되어있었으며, 주민등록번호와 같은 신원확인에 가장 용이하게 사용할 수 있는 정보를 원하는 경우도 이처럼 많이 발견할 수 있었다. 인터넷 웹사이트들의 이러한 행태는 실제로 어떤 특정한 목적이 있어서라기 보다는 일반적 관행의 형태라고 판단된다. 즉 우리 나라의 경우 신원확인을 위한 개인정보의 요구가 그동안에 너무나 자연스럽게 이루어져 왔으며, 또 한편 이러한 신원확인 요구를 당하는 시민의 입장에서 역시 이러한 행위들이 아무런 저항의 필요성을 느끼지 못할 만큼 당연하게 인식하고 있었다는 것을 반증하는 것이다.[35]

이상의 사례에서 확인할 수 있는 문제점은 다음과 같다.

우선 공공기관에서건 사기업에서건 업무관계에 있어서 문서를 작성하는 등의 행위에 반드시 신원정보의 제공을 필요로 하고 있으며, 이처럼 요구하는 개인정보의 내용이 이해할 수 없을 정도로 포괄적이고 지나치다는 것이다. 매장에서 바로 반품을 하는 고객에게 주민등록번호를 비롯한 개인정보를 요구하는 이유가 무엇인가? 더구나 반품사유를 적으라고 하는 것은 사후 서비스를 위한 것인가, 아니면 단순한 설문조사를 위한 것인가? 반품을 하는 이유는 여러 가지가 있을 것이고 만일 물건에 하자가 있어서라면 그것은 당연 반품사유일 뿐인데 물건의 하자 이외의 경우 개인이 회사를 상대로 그 이유를 고지할 필요성은 어떠한 이유에서도 납득이 가지 않는다.

다음으로 발생하는 문제점은 위에서 든 예들은 그나마 개인정보라는 측면에서 자신의 신상정보에 대하여 일정한 의식을 가지고 있는 사람들의 경우에 발생한 사례들이라는 것이다. 다시 말하여 많은 시민들은 이러한 사례들이 무수하게 발생함에도 불구하고 그것이 자신에 대한 직접적인 피해라고 인식하지 않는다는 것이다. 이렇게 일상화된 상황에서 자신의 신원확인 수단인 개인정보를 아주 쉽게 남들에게 넘겨주고 있는 것이 오늘날 우리의 자화상인 것이다. 자기앞수표를 사용할 때마다 수표 뒷면에 자신의 주민등록번호까지 이서해야만 하는 것이 우리의 현실이라는 이야기다.

또 하나의 문제는 이처럼 과도한 개인정보를 요구하는 사회적 관행은 책임의 문제와 밀접하게 연관되어 있다는 것이다. 이동통신업체와 계약을 함에 있어서 가입시에는 별다른 신분증을 요구하지 않다가 계약해지시에는 주민등록증을 비롯하여 신원확인을 할 수 있는 별도의 신분증을 요구하는 것은 업체가 자신의 책임에 대한 부분을 가입자에게 전가하기 위한 일종의 장치로서 신분증을 활용하는 것임에 다름없다. 실제로 신용카드가입이나 또는 이동통신가입을 유도하는 가두 행사에서는 신분증이 없이도 본인임을 확

34) 인터넷 한겨레, 2001년 4월 20일
http://www.hani.co.kr/section-001042000/2001/00104200020010222182770 4.html
35) 주민등록법 개정을 위한 행동연대. 2001년 4월 조사

인할 수 있는 각종 개인정보를 제공하는 즉시 계약이 이루어지고 해당서비스를 이용할 수 있는 것이 현실이다. 그러나 계약관계를 종료하고자 하는 경우에는 위의 사례와 마찬가지로 상당한 제약이 수반된다. 결국 계약해지조건을 까다롭게 하는 한편 나중에 돌아올 수도 있는 책임소재를 무마하기 위하여 신원확인과정을 소비자측에 어렵게 하는 것이 하나의 관례로 형성이 된 것이다.

2. 개인정보 유출 및 개인정보관련 범죄

(1) 개인정보 매매

1998년 6월 광명시에서는 광주시거주 유권자 35만명의 인적사항이 수록된 디스켓 7장이 거래되었고, 이를 통해 우편판촉행위를 하던 사람이 1999년 11월에 검거되는 일이 발생했다. 사건의 경위는 흡사 첩보영화의 한 장면을 방불케 한다. 생활정보지에 난 광고를 보고 한 보험회사 대리점 소장이 이를 사들였으며, 이 과정에서 '김부장'이라는 사람이 이 정보를 넘겨주었으며, 은밀한 접선으로 만나 보험회사 대리점 소장은 김부장이라는 사람에 대하여 어떠한 인적상황도 모르는 등 전형적인 미스테리형식의 극화가 실제로 전개되었다. 물론 전적으로 보험회사 대리점 소장의 진술만을 토대로 이루어진 시나리오인데다가 이 사람의 과거전력에서도 개인정보를 불법적으로 유출했던 적이 있었으며, 줄거리의 앞 뒤가 제대로 맞아떨어지지 않는 등 시나리오의 완성도는 극히 떨어지는 것이었지만 어쨌든 선거인명부라는 집합적 개인정보 파일이 불법적으로 시중에 유통될 수 있는 가능성이 있다는 것은 대단히 위험천만한 일이 아닐 수 없다. '김부장'이라는 사람은 대리점 소장에게 "광명시청에서 빼낸 선거인 명부이니 틀림이 없다"는 말을 들었다고 하는데 김부장이라는 사람이 가공의 인물이냐의 여부와 상관없이 공공기관에서 관리되어야 하는 개인정보의 내용임은 분명한 사실이고 따라서 공공기관의 개인정보 관리실태에 헛점이 존재한다는 사실은 명확한 것으로 판단된다. 대리점 소장은 공공기관의개인정보보호에관한법률을 위반한 혐의로 구속되었다.[36]

(2) 컴퓨터는 보물창고

열아홉살 먹은 김모군은 물경 780만명의 개인정보를 해킹하여 판매하려다가 검거되었다. 김모군은 구속되었고 공범인 이모군은 불구속 입건되었다. 김모군과 이모군은 신용카드결재 승인처리업체 1개와 9개 일반 인터넷 사이트에 침입해 780만명이나 되는 사람들의 개인정보를 빼냈다. 이들은 이렇게 입수한 개인정보를 마케팅 및 리서치를 전문으로 하는 업체에 판매하려 하였다. 이들이 빼낸 개인정보는 주민등록번호, 신용카드번호, 기타 개인의 신원확인을 위해 밀접한 정보들이 총망라되어 있으며, 성명, 주민등록번호, 주소, 연락처, 이메일 등이 포함된 개인정보는 건당 50원, 이 기본정보에 신용카드번호, 은행계좌번호 또는 현금카드번호가 포함된 개인정보는 건당 300원, 여기에다가 연봉 등 소득관련 정보가 포함된 개인정보는 건당 600원에 판매하려 하였다고 경찰은 발표했다. 김모군의 경우 이번 사건은 처음이 아니었고 이전에도 80여개 업체를 해킹해 600여만명의 개인정보를 유출했다가 입건된 바 있었다. 김모군 한 사람이 가볍게 해킹하여 알아내 개인정보는 도합 1400만명에 가까운 것으로 이것은 우리 나라 경제활동인구의 1/3을 초과하는 인원이며, 이들의 가족들까지 합치면 거의 우리 나라 모든 국민의 개인정보를 다 알 수 있는 정도의 숫자가 산정된다.[37]

36) 연합통신. 1999년 11월 09일
http://news.naver.com/read?command=read&id=1999110900000017014
37) 인터넷 한겨레, 2001년 4월 12일

(3) 행정자치부에게 감사하는 사기범

개인정보관리와 보호를 위해 불철주야 애쓰는 행정자치부의 서비스 시스템이 오히려 사기범들을 도와 개인정보의 유출과 악용을 도와준 웃지 못할 사건이 발생하였다. 행정자치부가 1998년 12월부터 시행하고 있는 주민등록번호 음성확인서비스를 이용해 일단의 범죄행각이 저질러진 것이다. 원래 행정자치부는 플라스틱 주민등록증을 사용하기 전의 구 주민등록증이 위조 및 변조가 쉬워 범죄 등에 악용되는 사례가 많아 본인의 확인을 용이하게 하기 위하여 이 자동음성확인서비스를 시행했다고 한다.[38] 그러나 위변조의 가능성이 구 주민등록증보다도 훨씬 어렵다고 선전해왔던 플라스틱 주민등록증 체제에서조차 이러한 행위가 가능한 것은 위변조의 문제는 범죄자의 행위와 관련한 문제이지 신분증의 재질로 인한 문제가 아님을 보여주는 증거이다. 이 사건은 용의자가 타인명의로 카드 등을 개설한 후 이 카드를 이용하여 거액의 금품을 취하거나 사용한 것으로 특히 "카드회사가 주민번호와 이름만 맞으면 전화통화로 카드신청인이 본인인지 여부를 확인하는 허점을 이용해, 미리 사무실과 전화를 마련해놓고 카드회사에서 신분 확인 전화가 오면 임시로 고용한 여직원을 시켜 확인해주는 새로운 수법"을 사용하는 지능적인 면모를 보여주기까지 하였다. 이 사건 이후 행정자치부는 부랴부랴 주민등록증 발급일자를 모르면 해당 서비스를 이용하지 못하도록 하는 조치를 취하였다.[39]

(4) '실수'로 벌어진 개인정보 공개

1999년 연말에 서울시 공무원의 실수로 1800여명에 이르는 아르바이트 응시생들의 개인정보가 인터넷 사이트에 떠오른 일이 있었다. 1999년 12월 9일 서울시는 아르바이트 학생을 온라인으로 모집하는 과정에서 접수된 대학생들의 명단을 공개하면서 여기에 접수자의 주민등록번호, 전화번호, 집주소, 학과, 학년, 개인소개서 까지 모든 개인정보를 완전히 공개한 것이다. 해당 학생들의 항의를 받고 담당 공무원이 30여분만에 해당자료를 사이트에서 지웠으며, 서울시는 프로그램 관리자가 내부 자료를 링크시키는 과정에서 발생한 우연한 일이라고 해명했다.[40]

(5) 전자상거래, 믿을 수 있나?

미국 공정거래위원회(FTC, www.ftc.gov)는 전자상거래에 따른 피해유형의 대표적인 유형을 소개했다. 피해유형으로는 (1) 피해자의 이름으로 신용카드가 발급되고 사용대금이 피해자의 계좌로 청구되는 경우, (2) 개인정보누출사실을 확인하지 못하도록 대금청구서의 주소를 변경하고 피해자의 개인정보를 이용하여 이동통신 및 은행계좌까지 개설하여 명실상부 피해자로 행세하는 경우가 대표적이다. 이러한 피해들은 주로 더 많은 개인정보가 수집 보관되어있는 데이터베이스를 대상으로 벌어지게 된다.[41]

그런데 전문가들의 입장에서는 이러한 전자상거래 과정에서 발생할 수 있는 개인정보 도용 피해를 막기에는 국내 수준이 아직 미치지 못하는 것으로 파악되고 있다고 한다. 정보통신서비스업체들이 경품이나

http://www.hani.co.kr/section-005000000/2001/04/005000000200104121444706.html

38) 인터넷 한겨레, 1998년 10월 22일.
http://search.hani.co.kr/data/news/1998/1022/4002100241.html

39) 인터넷 한겨레, 2001년 1월 27일
http://www.hani.co.kr/section-005000000/2001/005000000200101271907009.html

40) 한겨레신문, 1999년 12월 21일.
http://news.naver.com/read?command=read&id=1999122100000073014

41) 인터넷 한겨레, 2000년 3월 31일
http://news.naver.com/read?command=read&id=2000033100000037014

현금을 내걸고 회원을 모으면서 각종 개인정보를 수집하는 반면에 정작 이러한 측면의 보호를 위한 관리에 대해서는 상당히 허술한 면을 보이고 있기 때문이다. 한국정보보호센터가 1999년 11월 정부, 공공기관, 쇼핑몰, 통신사업자, 일반 회사 등 국내 1000개 웹사이트를 대상으로 실시한 조사결과, 조사대상 가운데 개인 정보에 대한 접근 제어를 위해 패스워드를 사용하고 있는 경우는 71%였고, SET나 SSL 같은 암호 프로토콜을 사용하는 경우는 10%에 지나지 않았음이 확인되었는데 이를 보더라도 개인정보에 대한 안전장치가 매우 허술하다는 것을 잘 알 수 있다.[42]

(6) 개인정보확인? 돈만 벌면 되지!

요즘 거리에서 직접 회원을 모집하고 있는 일부 신용카드회사들의 경우 회원가입을 위하여 별도의 절차를 필요로 하지 않고, 주민등록번호와 개인정보 몇 가지를 서류에 기입하는 즉시 회원가입을 끝낼 수 있도록 하고 있다. 별다른 신원확인절차 없이 신청에 필요한 주민등록번호만을 청취해 발급해줌에 따라 타인의 주민등록번호를 도용하여 신용카드를 발급받아 사용하는 범법행위가 늘어가고 있다. 이러한 사건들의 경우 피해자들이 신고를 하더라도 아무런 단서가 남아있지 않기 때문에 범인을 검거한다는 것이 매우 어려운 일이 되고 만다.[43]

(7) 개인정보 유출에 교육계도 한몫

올해 초에 강원교육청은 정기교원인사에 즈음하여 초등 신규교사 700명의 명단과 이들의 주민등록번호, 발령지를 함께 인터넷에 공개해 물의를 빚은 바 있다. 교육청 관계자의 해명은 인원이 700명으로 많은 수에 달하고 이들 중 다수의 동명이인이 있어서 혼돈을 피하고자 불가피하게 주민등록번호를 함께 올린 것이라고 하는데 과연 주민등록번호의 등재가 꼭 필요한 작업이었느냐에 대해서는 의문의 여지가 남는다.[44]

(8) 주민등록증 아세톤 위조사건

위변조를 막기 위해 구 주민등록증을 일제히 바꾸어가면서 국민에게 발급한 새 플라스틱 카드가 오히려 구 주민등록증보다도 훨씬 용이하게 위변조된다는 사실을 보여주는 사례가 바로 아세톤으로 주민등록증을 위조한 사건이었다. 사건의 주인공들은 타인의 주민등록증을 아세톤으로 지우고 유명인사의 이름과 주소 등을 실크스크린 기법으로 인쇄하여 변조하는 수법을 사용하였다. 이들은 이렇게 변조한 주민등록증과 인감증명을 가지고 토지를 담보로한 거액의 대출을 받으려다가 검거되었다. 플라스틱 주민등록증이 발급될 당시부터 이러한 방식의 위변조가 가능하다는 점이 지적되어왔으나 당국은 일관되게 위변조의 가능성이 구 주민등록증에 비하여 현저히 떨어진다는 점만을 강조해 오다가 결국 이러한 사건이 발생하게 되었고, 이에 따라 행정자치부는 실효성 있는 대책을 마련하겠다고 공언하였으나 아직 별다른 대책이 발표되고 있지 않은 상황이다.[45]

42) 인터넷 한겨레, 2000년 4월 3일
http://news.naver.com/read?command=read&id=2000040300000092014

43) 인터넷 한겨레, 2001년 4월 20일
http://www.hani.co.kr/section-001042000/2001/001042000200104011828707.html

44) 인터넷 한겨레, 2001년 2월 26일
http://www.hani.co.kr/section-005000000/2001/005000000200102261737993.html

45) 인터넷 한겨레, 2월 5일
http://www.hani.co.kr/section-005000000/2001/005000000200102052222991.html