정보통신시스템 침해범죄 사례와 안정성 확보를 위한 법적대책
- 인터넷상 개인정보 수집업체를 중심으로 -

양 근 원

I. 서론 : 「만민 정보수집시대」와 정보통신시스템 침해범죄

1. 만민 정보수집시대의 도래

컴퓨터와 네트워크로 이루어진 정보통신망은 "신속성"과 "정확성", "집약성"을 태생적 특징으로 하고 있다. Web으로 대표되는 인터넷은 일반대중들을 네트워크의 세계로 끌어 들이는데 성공하고 있으며 네트워크에서 흘러 다니는 각종 자료들을 끌어 모아 처리하는 기술은 나날이 발전하고 있다. 인터넷을 커다란 시장이나 사업 영역으로 여기는 생각들이 발전하면서 이제 마케팅 전략과 데이터 수집·처리·가공 기술이 결합되고 있다. 전통적으로 정보통신분야의 고유영역으로 여겨지던 기술들이 경영영역으로 흡수되기 시작했고 DBMS(Database Management System), MIS(Management Information System)같은 것들은 경영학의 기본이 되고 있다. 고객 DB는 기업의 핵심자산으로 인식되고 있으며 효과적인 마케팅, 고객관리를 위한 각종 기법들이 개발되고 있다. 그 재산적 가치 또한 점점 커지고 있다.[2)]

특히 개인정보를 중심으로 고객 정보를 수집하는 일과 네트워크 상에서 흘러 다니는 개인의 습관, 성향, 경제적 특징들을 연결하여 고객지향적 마케팅 전략을 수립하는 기법들이 크게 발전하고 있다. 이른바 CRM(Customer Relationship Management)같은 것들은 그 대표적인 것들이다. 네티즌들은 각종 인터넷 서비스를 이용하는 대가로 주민등록번호를 비롯한 자신의 민감한 개인정보를 제공할 것을 요구받고 있으며 이것은 이른바 "회원가입"이라는 명분으로 정당화된다. 우리나라 어지간한 포털사이트들의 경우 이렇게 모은 개인정보가 1,000만명 이상 분량이 된다. 수집되는 정보의 깊이와 넓이는 가히 무차별적이다. 누구라도 자신이 운영하는 사이트에서 개인정보를 수집할 수 있고 활용할 수도 있다. 성인에서부터 초등학생에 이르기까지 개인의 정보는 네트워크를 통해서 마구 수집되고 있다. 이렇게 모아진 회원정보와 회원으로서의 활동사항은 시스템에 데이터 베이스로 저장되며 매칭 시스템으로 분석하면 개인의 습성, 성향까지 그대로 알아 낼 수 있다. 사이버 공간상의 개인활동은 어떻게 보면 완전히 노출되어 있다고 할 수 있다.

대개 인터넷의 특징으로 "익명성", "비대면성" 같은 것을 들고 있다. 그러나 최근의 동향을 보면 이러한 명제가 현재의 시점에서도 그대로 통용될 수 있겠는가 하는 의구심을 갖지 않을 수 없다. 자신의 활동이 그대로 노출되는 상황하에서 익명성이 아니라 이제는 과거보다 더 개인의 존재와 정보들이 타인에게 드러나는 시대가 되었다고 볼 수 있는 것이다. 인터넷의 발달로 이제 이른바 『만민정보수집·제공의 시대』가 되었다. 지식정보사회에서는 정보를 장악하는 자가 개인에 대한 사회적 통제력을 가지게 되는 것이며 그것의 위력 또한 절대권력과 비교할만 하다.

---

1) 필자는 경찰청 컴퓨터범죄수사대장, 사이버범죄수사대장, 사이버테러대응센터 수사대장을 거쳐 현재는 경찰대학 교수로 재직중이다.

2) 우리나라 대표적 동창모임 사이트인 아이러브스쿨이 지니고 있는 자산가치는 5백억원 정도로서 이는 동창모임의 속성상 회원들의 입력하는 학력, 경력 등 실제적인 정보가치가 평가되는 것으로 생각된다. 야후코리아,아이러브스쿨 인수추진(경향신문 2000-08-10 34면 (경제) 기사) 참조

2. 개인정보 침해와 정보통신시스템 안전성

전통적으로 각 나라에서는 국가에 의한 개인정보 수집, 사생활 침해 문제를 심각하게 다루어 왔다. 그러나 앞에서도 언급하였듯이 이제는 정보수집의 주체가 민간으로 넘어가고 있다. 물론 국가에 의한 정보수집과 사생활침해가 사라진 것은 아니지만 이제 민간이 가진 정보통신기술을 이용하여 훨씬 용이하고 효율적으로 개인정보를 수집, 가공함으로써 그 질과 양이 오히려 정부의 그것을 능가하는 현상을 보이기고 있는 것이다. 따라서 이제까지 비교적 관심을 덜 가져 왔던 민간영역에서의 개인정보보호 및 정보통신시스템의 안전성 문제를 심각하게 고민해야 할 시기가 된 것이다. 그러나 민간영역에서의 개인정보보호 문제에 대한 제도적, 법적 대응은 아직까지 미비하기만 하다. 우리나라의 경우 공공기관에 의한 개인정보침해 문제를 다루기 위한 기본법으로 공공기관의 행정전산화 경향에 맞추어 지난 '94년에 "공공기관의개인정보보호에관한법률"을 제정하여[3] 공공기관에서 수집·처리·보관하고 있는 개인정보에 대한 엄격한 규정을 두고 있으나 민간부분에 대한 개인정보보호관련 일반 규정은 지난 '99년 기존의 "전산망보급확장및이용촉진등에관한법률"을 개정하면서 일부 개인정보보호에 관한 규정을 삽입하고 "정보통신망이용촉진등에관한법률"로 개칭한 것이 최초의 시도이다. 그러나 2001년 이 법률을 "정보통신망이용촉진및정보보호등에관한법률"로 다시 개칭하면서 개인정보보호에 관한 규정을 강화하였음에도 불구하고 업체 자체의 개인정보 유출 및 오용에 중심을 두고 있는 등 미흡한 수준이며 허술한 관리체계를 틈타 최근 몇 달 동안에만 사이버 공간상에서 우리나라 성인 네티즌 전체 규모와 비슷한 1,500만명분 이상의 개인정보가 침해당하여 유출되는 대형사건이 연달아 발생하였다.

본 고에서는 개인정보보호문제에 관해 여러 가지 문제가 있을 수 있지만 광범위한 문제를 포괄적으로 다루기보다는 민간부분의 개인정보 침해범죄와 관련하여 개인정보를 다루는 정보통신망의 안전성 문제에 관하여 생각해 보고자 한다.

II. 사이버공간과 개인정보 침해 범죄

1. 사이버공간에서의 개인정보보호 현황

미연방거래위원회(FTC)는 1998년 온라인 프라이버시에 관하여 조사하였다. 약 1,400여개의 웹사이트에 대한 조사에 기초하여 다음의 보고내용을 제시하고 있다.[4] 「사이트의 87%-97%가 소비자로부터 개인정보를 수집한다. 그 중 14%만이 그들의 정보거래에 관해서 고지하며, 또 약 2%만이 포괄적인 프라이버시 보호를 제시하고 있다. 아동 웹사이트의 89%는 아동으로부터 개인정보를 수집하는 것으로 나타났다. 따라서 미국은 개인정보보호를 위해서 **고지/경고 (Notice/Awareness)** 즉 기업체의 정보처리에 대해 소비자에게 통지할 것, **선택/동의**

3) 제정이유를 다음과 같이 설명하고 있다.
국가주요업무에 대한 전산화의 확대추진과 전국적 행정전산망의 구축 등으로 개인정보의 부당사용 또는 무단유출로 인한 개인사생활의 침해 등 각종 부작용이 우려됨에 따라, 공공기관이 컴퓨터에 의하여 개인정보를 취급함에 있어서 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 개인의 권리와 이익을 보호하려는 것임.

4) http://www.ftc.gov/reports/privacy3/toc.htm : Federal Trade Commission, Privacy Online : A Report to Congress, June 1998

(Choice/Consent) 즉 소비자로부터 수집하거나 소비자에 관한 정보의 사용 및 유포에 관하여 소비자에게 선택권을 부여할 것, **접근/참여(Access/Participation)** 즉 소비자가 기업체에 의해 수집되어 보관되는 관련 정보를 입수할 수 있어야 할 것, **통합/안전(Integrity/Security)** 즉 관련 데이타 수집자가 수집정보의 안정성과 완전성을 보증하기 위하여 적절할 수단을 강구할 것, **집행/배상(Enforcement/Redress)**의 5원칙을 개인정보규범의 핵심내용으로 제시하고 있다.

우리나라에서도 지난 2000년 6월 한국정보보호센터에서 300여개 사이트를 대상으로 개인정보 보호 모니터링을 실시한 바 있다. 그 결과 조사대상 300개 사이트 중 92%인 275개 사이트가 한 개 이상의 개인정보를 수집하고 있으며 쇼핑몰의 경우에는 90개 사이트 중 약 98%인 88개가, 일반회사 경우에는 210개 사이트 중 약 90%인 187개로 나타났다.[5] 한편 1999년 국내의 1,000개 웹 사이트를 대상으로 한 개인정보보호의 실태조사 결과에 의하면, 사이트 운영자들의 개인정보보호 조치가 미약하다는 사실을 확인하였다[6]. 대상 1,000개 사이트 중 936개(94%)의 사이트가 성명, 주소 외에 주민등록번호, 직장, 성별 등 다양한 개인정보를 수집하고 있었다. 그러나 무엇보다도 개인정보의 접근제어를 위해서 패스워드를 사용하는 경우는 71%의 663개 사이트에 해당하지만, SSL(Secure Socket Layer)와 같은 보안프로토콜을 사용하는 경우는 90개(9%)에 불과하여서 해킹의 위험에 노출되어 있다는 점이 부각되었다.
위에서 본 각종 조사자료에 근거해 보아도 현재 사이버 공간에서 운영하는 사이트의 대부분은 개인정보를 수집하고, 관리하는 기능을 가지고 있다. 그러나 개인정보의 안전을 위한 조치는 크게 미흡한 것으로 나타나 있다.
그 원인으로 생각해 볼 수 있는 것은
첫째 개인정보 안전 시스템의 비용 문제를 들 수 있다. 인터넷을 이용하여 영업활동을 하는 업체 대부분은 중소규모 벤처 형태의 기업으로서 안전관리에 소요되는 비용을 아직은 영업이익과 관련되지 않은 것으로 생각하고 있으며 낭비적 요소로 여기는 것이다. 그 비용 또한 수천만원 이상을 넘어서고 있다.
둘째로 정보통신망법상에서 비록 개인정보의 안정성을 위해 제28조 등에서 관련 규정을 두고 있지만 이는 훈시적 규정으로서 별도의 제재조치가 없기 때문에 기본적인 기능 외에 추가적 비용을 들여 기술적, 관리적 조치를 취할 의무가 없기 때문이다.
어쨌든 이러한 미비점으로 말미암아 우리나라에서는 최근 각종 개인정보 침해사례가 빈발하고 있다.

2. 정보통신시스템 및 개인정보 침해 유형과 사례

사이버 공간에서의 개인정보침해 사례의 경우로 여러 가지 다양하게 들 수 있겠지만 크게 내부인에 의한 개인정보 침해와 외부의 기술적 공격에 의한 개인정보 침해 경우로 나누어 생각해 볼 수 있다.
내부인에 의한 개인정보침해로는 관리자에 의한 개인정보 과다 수집, 부당 이용 및 유출, 개인정보 매매 등을 들 수 있고 이에 대한 각각의 처벌 규정도 마련되어 있다. 문제가 되는 경우는 대부분 개인정보 수집관리 업체가 고객의 정보를 매매하거나 부당하게 이용하는 경우이다. 외부의 기술적 공격에 의한 개인정보 침해의 경우로는 해킹 등의 기술적인 방법으로 개인정보 관리시스템에 무단 접근, 개인정보를 유출해 가는 경우를 들 수 있다. 물론 타인의 정보통신망에 부당하게 접속하거나 보호조치를 침해하는 경우 처벌 규정이 있기는 하지만 실제 이와 관련된 침해사례가 꾸준히 발생하고 있으며 심지어 개인정보를 유출, 판매하려는 시도가 발생한 적

5) http://www.cyberprivacy.or.kr
6) 국민일보 2000-02-22 16면 (과학.의학) 뉴스 등 참조

도 있다. 또한 공격 기술은 쉴 새없이 인터넷을 통해 공개되고 rootkit등 자동화된 도구들이 개발되며 실제 사례에서 보듯 현재 보안시스템에서 대표적으로 사용되고 있는 Firewall이나 IDS가 설치되어 있는 시스템도 침해를 당함으로써 그 한계를 여실히 드러내는 경우도 빈발하고 있어 심각한 문제로 대두되고 있다.

그동안 일어 났던 인터넷상에서의 외부의 기술적 공격에 의한 정보통신시스템 및 개인정보 침해 중요사례를 보면 다음과 같다.

1) 2000. 7 사이버 증권사 등 고객정보 15만명분 유출 사건

가) 증권정보 전문제공업체 고객비밀 등 5만명 정보 유출, 도용

- **개 요**

서울 강북구 번동 김모군(23, B대학교 전자계산학과 3년)은 홈페이지 제작관련 프리랜서로 일하면서 2000. 4. 5 자신이 재택사원으로 근무하였던 웹마케팅 회사인 (주)B시스템의 NT서버에 불법 접속하여, 증권금융정보 전문제공업체인 (주)A정보 고객정보 관리자의 관리소홀로 서버에 저장되어 있던 (주)A정보의 고객 ID, 비밀번호, 주민등록번호, 회원들의 증권사명, 계좌번호, 거래지점, 성향 등 5만여명의 정보가 상세히 저장되어 있는 고객정보데이타 파일을 자신의 컴퓨터로 다운받아 타인의 비밀을 침해하였다가 검거됨

- **보안상의 특징**

· 사내 중요 정보를 다루는 직원의 퇴사시에는 반드시 사용하던 계정 등에 대한 삭제조치를 해야 함에도 불구하고 그대로 방치하여 사건 유발

· 타인의 계좌번호, 비밀번호 등 극히 중요한 정보를 허술하게 관리

나) 유명 시스템업체 고객 11만명 정보 유출, 판매 사건

- **개요**

경기도 고양시 덕양구 강매동 거주 김모군(24, A대학 3학년 휴학중)은 '99년 11월경부터 청소년 및 PC방을 상대로한 벤처기업인 (주)C월드를 경영하여 오면서 자신이 만든 초등학교 동창 모임 홈페이지에서 얻은 접속자료를 분석하여 친구들의 직장, 근무지에 대한 인터넷자료를 파악해오다, 2000년 5월 25일 국내 유명 정보시스템관련 협력업체로서 고객 데이터 관리 및 마케팅을 대행해 주는 (주)D정보시스템사에 근무하는 친구의 시스템에 MS Window 공유기능상의 헛점을 이용하여 불법 접속한 뒤 시스템에 저장되어 있는 근무지, 전화번호, 주소, 직책 등이 담긴 11만명 상당의 고객데이타를 유출하여 자신의 시스템에 저장하여 두었다가 건당 500만원씩에 판매할 목적으로 가공의 인물을 내세워 공짜 메일주소를 만든 뒤 2000. 6. 15 - 7. 10간 주로 PC방을 돌아다니면서 인터넷 컨설팅 업체 등 130여명에게 E-mail을 보내 그 중 고객의 근무지, 전화번호, 주소, 직책 등 상세한 정보가 담긴 100여명의 개인정보를 샘플로 보내는 등 타인의 개인정보를 불법유출, 판매하려다가 검거, 구속됨

- **보안상의 특징**

· 다수의 기업 및 기관에서 내부네트워크용으로 사용되는 마이크로소프트(MS) 윈도우95, 98의 공유기능(NetBIOS)은 대부분 LAN상의 자료 공유 기능으로 사용하고 있는 점을 이용

· 공유기능은 인터넷 통신규약(TCP/IP)을 기반으로 하기 때문에 인터넷에 연결된 세계 어느 컴퓨터라도 공유 폴더를 통하여 접근 가능하여 자료가 유출될 위험이 있으므로 방화벽 등 보안장치가 없는 시스템에서는 윈도우공유기능을 사용하지 않는 것이 바람직(공유기능 사용시 암호 설정을 해도 암호 해독프로그램으로 쉽게 해독가능)

2) 2000. 12 70여개 사이트 650만명 개인정보 유출 사건

- **개 요**

대전 유성구 거주 피의자 金모군(17세)는 대전소재 A상업고등학교 정보처리과 2학년생으로서 2000. 7. 초순경부터 자신이 평소 관심을 갖고 실력을 쌓고있는 시스템해킹을 통하여 이를 제공받을 목적으로 「A모임 사이트」에 자신이 제작한 'IPSCANER'라는 취약점검색 프로그램을 이용, 취약점을 찾아낸 후 데이터베이스에 불법 접근하여 회원ID, 비밀번호, 성명, 주민등록번호, 생일, 주소, 출신학교, 직업, E-mail주소, 전화번호 등이 입력된 약 570만명 분의 개인정보를 자신의 컴퓨터로 다운받아 저장하는 등 최근까지 46개의 인터넷 사이트를 해킹하여 개인정보 약 630만명 분을 유출함으로써 정보통신망에 의하여 처리·보관되는 타인의 비밀을 침해하고, 피해사이트인 (주)B정보통신 시스템관리자에게 E-mail을 보내 해킹사실을 고지하며 보안취약점을 알려줄테니 디지털카메라, PDA 등을 달라고 협박하던 중 검거됨

- **보안상의 특징**

· 주로 Windows NT시스템에서 사용되는 각종 DB는 ASP프로그램에 의해 핸들링되고 소스에는 DB와 연동될 수 있는 계정과 암호가 포함되어 있으며 해커는 ASP소스를 볼 수 있는 취약점을 이용하여 DB연결 계정을 찾아내 DB 클라이언트 프로그램을 이용하여 DB 유출
· 시스템상의 각종 버그 패치에 소홀하여 피해 야기
· 중요 DB 시스템은 반드시 외부와의 연결을 차단하도록 Firewall등에서 IP, 연결 포트 등에 대한 접속 규칙을 면밀히 검토 적용해야 하나 백업 시스템에 대한 관리 소홀로 시스템 허점 유출

3) 2001. 5 780만명 개인정보 유출 사건

- **개 요**

피의자 金모군(19세, 서울시 서초구 서초동) 등은 최근 마케팅, 리서치 등에 있어서 개인정보의 활용성이 높아 개인정보를 수집, 판매하면 큰돈을 벌 수 있을 것이라고 생각하고 자신들의 해킹 실력을 발휘하여 다량의 고급정보를 보유하고 있는 인터넷 사이트를 집중적으로 해킹, 회원정보를 수집, 판매하기로 공모한 후 2001. 3월 중순경 경기 평택시 소재 피의자 李모군의 집에서 신용카드결제승인처리업체인 A정보통신 홈페이지 웹게시판의 취약점을 이용한 해킹 방법을 사용하여 성명, 주민등록번호, 신용카드번호 등이 포함된 신용카드영수증 복권당첨자 내역에 관한 개인정보 46만명 분을 유출하는 등 약 780만명에 달하는 개인정보를 유출한 후 추적을 피하기 위해 외국의 메일시스템을 이용하여 자신들이 판로로 계획하여 미리 메일주소 등을 확보하여 두고 있던 마케팅, 리서치 전문업체 관계자 약 2,000여명을 상대로 2000. 3. 26경부터 3차례에 걸쳐 동 개인정보를 판매하겠다는 내용의 이메일을 보낸 후, 피의자들이 보관하고 있던 개인정보에 관심을 보여 회신메일을 보내온 불상의 자들에게 샘플을 추출하여 이메일을 통하여 보내주는 등 판매를 시도하다가 첩보를 입수하고 추적한 경찰에 검거됨

- **보안상의 특징**

· 재산적 가치가 큰 정보를 관리하는 시스템 집중 선별 공격
· DB운영시스템 등 중요 시스템을 Firewall 안단에 배치하였으나 Web으로 처리되는 DB와의 연동문제로 Firewall 바깥단의 Web서버와 연결될 수 밖에 없는 점을 이용
· 최근 Web에 사용되는 각종 cgi, php, asp로 짜여진 프로그램들이 보안상 많은 문제를 지니고 있으며 이 점을 이용 Web서버를 선제 공격한 뒤 DB서버 공격
· 필연적으로 취약할 수 밖에 없는 Web서버는 반드시 외부 네트워크에 위치시키는 것이 기본

원칙임에도 일부 기업체에서는 Firewall 내부에 위치시킴으로써 결과적으로 모든 네트워크가 공격에 노출

· 일부 업체에서는 보안관제서비스도 받고 있었으나 Web을 통한 공격기술은 많은 경우 네트워크 IDS에서조차 감지하지 못하고 있었으며 수사과정에서 통보하여 비로소 피해사실을 인식한 경우가 많음

한편 한국소비자보호원 사이버소비자센터에서는 2000년 10월 전국 만 15세이상 5,243명을 대상으로 "개인정보 보호 및 스팸메일에 대한 소비자 의식조사"를 실시한 결과[7] 네티즌들은 각종 인터넷 사이트 회원 가입 시 요구하는 개인정보량에 대해 86.8%가 과다하다고 응답하고 있으며 개인정보를 제공함으로써 프라이버시가 침해될 가능에 대해 전체 95.7%가 우려한다고 응답하였다. 나아가 인터넷 서비스의 안전성 · 보안성에 대해서는 75.1%가 신뢰하지 않고 있으며 79.3%가 신용카드 결제 시 위험 부담을 느끼고 있는 것으로 나타나 실제로 발생하고 있는 개인정보 침해 사례와 무관하지 않음을 보여주고 있다. 나아가 인터넷 서비스 업체의 과다한 개인정보 수집, 안정성 확보의 미비가 향후 지식 정보사회 발달의 큰 걸림돌로 작용하고 있음을 보여주고 있다.

III. 입법례 및 현행법의 문제점

1. 외국의 개인정보관련 입법례 개관

1) OECD

경제협력개발기구(OECD)는 1980년(9월) 「프라이버시 보호와 개인정보의 국제유통에 관한 지침」[8]에서 개인정보보호를 위한 8원칙을 제시하였고, 또한 1998년(10월) 「범세계적 네트워크상

7) http://safe.cpb.or.kr/textdata/HOMEPAGE/200101/1900003/ecre010119.pdf 참조

8) Guidelines Governing the Protection of Privacy & Transborder Flow of Personal Data 한국정보보호센터, 개인정보 보호 및 활용을 위한 IT 분야의 활성화 방안에 관한 연구(2001.3), p. 9이하 참조)

그 내용을 보면 다음과 같다.

(1) 수집의 제한 : 개인정보의 수집은 제한되어야 한다. 그리고 그러한 정보는 적법하고 정당하게 취득되어야 하고, 정보주체의 적절한 인식과 동의가 있어야 한다.

(2) 데이터의 질(정보내용의 정확성 원칙) : 개인정보는 사용되어야 할 목적과 관련이 있어야 한다. 그리고 그러한 정보는 목적에 필요한 범위 내에서, 정확하고 완전하고 최신이어야 한다.

(3) 목적의 특정성(목적 명확성 원칙) : 개인정보가 수집되는 목적은 정보수집 당시에 특정되어야 한다. 그리고 계속되는 사용은 그러한 목적 혹은 그러한 목적에 부합될 수 있는 기타의 목적 그리고 목적이 변경된 경우는 명시된 기타의 목적의 달성에 제한되어야 한다.

(4) 이용의 제한 : 개인정보는 임의로 누출되거나 이용되어서는 안되고, "특정된 명확한 목적"과 관련된 것 이외의 목적을 위해서도 마찬가지다. 단 정보 주체의 동의가 있는 경우와 법에 의하여 강제되는 경우는 예외로 한다.

(5) 보호 지침(안전확보의 원칙) : 개인정보는 데이터의 손실, 권한없는 접근, 파괴, 사용, 변경이나 누출과 같은 위험성에 대비하여 합리적인 보호지침에 의하여 보호되어야 한다.

(6) 공개성 : 공개성에 관한 개인정보에 대하여 일반적인 정책이 있어야 한다. 개인정보의 존재와 성질을 입증하기 용이하여야 하며, 물론 본래 목적을 위한 것이어야 하고, 정보 수집자의 식별과 주요 거주지 역시 입증이 용이하여야 한다.

(7) 개인의 참가 : 개인은 다음과 같은 권리를 보유하여야 한다.

1) 정보수집자로부터 자신에 관한 정보를 가지고 있는지 여부에 대한 확인받을 수 있는 권리

2) 자신과 관련된 정보를 (다음과 같이) 본인에게 통지하도록 하는 권리

의 프라이버시 보호에 관한 각료선언」에서는 1980년에 채택한 8원칙이 인터넷 환경에도 적합하다는 점을 동의하여 각국이 네트워크 환경에서 효율적인 프라이버시 보호를 위한 조치를 취할 것을 촉구하였다.

2) EU

유럽연합(EU)은 1995년(10월) 「개인데이터의 처리와 자유로운 유통에 관한 개인보호지침」[9]을 채택하였다. 이 지침은 EU 수준으로 적절하게 개인정보를 보호하지 않는 국가에 대해서는 개인정보의 데이터 이전을 금지하고 있다. 1997년(12월)에는 「정보통신부문의 프라이버시 보호와 개인정보처리에 관한 지침」[10]을 채택한 후, 1999년(2월)에는 인터넷 이용자와 서비스 제공자(ISP)의 법률관계를 규정한 「인터넷 개인정보의 수집 및 처리에 관한 개인보호지침」[11]을 채택하였다.

3) 미국

미국은 1998년(11월) 개인정보보호를 위한 안전보호원칙(Safe Harbor Principles)을 제시하였다. 이 원칙은 7가지 사항[12]을 포함하였으며, 1999년(11.15) "International Safe Harbor Privacy Principles(Draft)"로 수정 제안되었다.

기타 미국의 프라이버시와 관련된 법률로는 「전기통신프라이버시법」, 「소비자 인터넷 프라이버시보호법」(Consumer Internet Privacy Protection Act), 연방 인터넷 프라이버시보호법(Federal Internet Privacy Protection Act), 사회보장온라인 프라이버시보호법(Scocial Security On-line Privacy Protection Act), 아동프라이버시 보호와 부모동의법(Children Privacy Protection and Parental Empowerment Act)등을 들 수 있다.

- 합리적인 시간 내에
- 무료 또는 과다하지 아니한 (적절한) 액수로
- 합리적인 방법으로
- 쉽게 이해할 수 있는 형식이어야 한다.

3) 위의 (a)와 (b)가 거부되는 경우, 이유를 밝히도록 하고, 그러한 거부에 대하여 이의를 제기할 권리

4) 자신과 관련된 정보의 무효를 주장할 수 있고, 만일 이의가 인정되지 않을 경우 그 데이터를 파기, 변경, 완전화, 보충케 하는 권리

(8) 입증책임(책임의 원칙) : 정보 수집자는 위에서 언급된 원칙들에 영향을 끼치는 기준에 부합된다는 것을 증명하여야 한다.

9) Directive 95/46/EC of the European Parliament and 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"
이 지침에서는 두 가지의 목적을 제시하고 있는 바, 제1조 제1항에서는 "자연인의 기본권과 자유를 보호하고 특히 개인정보처리과정에서 프라이버시를 보호하는 것"과 제1조 제2항에서는 "회원국가는 1항에서 부여되는 보호와 관련된 이유를 들어 회원국가 사이에 개인정보의 자유로운 흐름을 제한하거나 금지해서는 아니된다."고 규정하고 있다. 한편 정보보호관제도를 두고 있고, 개인정보의 침해에 따른 손해배상에 있어서 정보관리자측에 과실이 있음을 추정하도록 규정하고 있다.
(정재훈, 민간부문에서의 정보프라이버시 보호(1997, 정보법학회 세미나, p18)

10) Directive of the European Parliament and the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.

11) Recommendation No R (99) 5 「Guidelines for the protection of individuals in connection with the collection and processing of personal data on information highways」

12) 고지(NOTICE), 선택권(CHOICE), 제3자 정보제공(ONWARD TRANSFER), 안전성(SECURITY), 데이터 무결성(DATA INTEGRITY), 접근(ACCESS), 집행(ENFORCEMENT)

4) 영국

1984년 7월 제정되고 다시 1998년 개정된 영국의 정보보호법은 공공부문과 민간부문의 컴퓨터에 의한 개인정보의 처리를 규제하기 위한 법으로서, 정보보호의 원칙, 정보보호등록관과 심판소의 설치, 개인정보 처리의 등록 및 감독, 정보주체의 정정·말소 청구권과 한계 등을 규정하고 있다.[13] 또한 다른 EU회원국과 마찬가지로 개인정보보호를 위하여 정보보호 등록관을 두고 있다. 개인정보를 보유하고 이용하고자 하는 자 및 정보서비스를 제공하는 컴퓨터정보회사는 등록관에게 정보의 이용목적과 정보원의 내용 등을 기재한 등록서류를 제출하도록 하고 있어, 어떠한 사람도 등록부에 등록하지 않고는 개인정보를 보유할 수 없도록 하고 있다.[14]

5) 일 본

일본은 1997년 통산성에서 "민간부문에 있어서 전자계산기 처리에 있어서 개인정보의 보호에 관한 가이드라인"을 제정, 고시한 바 있다. 또한 최근 연합뉴스의 기사(2001. 3. 27)를 참고하면 일본 정부는 개인정보보호와 관련된 5개 기본원칙을 준수하도록 한 개인정보보호법안을 가결하였다고 한다.[15]

2. 우리나라의 개인정보보호관련 법령(정보통신망법을 중심으로)

정보통신기술의 발전에 따라서 개인정보보호에 관한 근거법률이 기능적으로 산재하고 있다. 특히 우리나라에서는 그동안 공공기관에서 수집관리하는 개인정보에 관하여는 일찍부터 공공기관의개인정보보호등에관한법률에 관련 규정을 두고 있었으나 민간부분에서 관리·보관하는 개인정보에 대해서는 신용정보 등 특정한 경우를 제외하고는 일반적인 규정이 없었다. 그러나 최근 정보통신망에 의한 개인정보 수집·보관 현상이 증가함에 따라 이들이 가지고 있는 개인정보 침해우려가 증대되어 지난 1999년 기존의 전산망보급확장및이용촉진등에관한법률을 개정하여 정보통신망에 의해 처리 보관되는 개인정보보호에 관한 일반적 규정을 두고 법명도 정보통신망이용촉진등에관한법률로 바꾸어 1999년 7월 1일부터 시행해 오고 있었다. 그러나 정보통신망에 의한 개인정보침해 문제가 계속 제기됨에 따라 2001년 OECD의 8원칙을 감안, 개인정보보

13) 김종호, 지식정보사회의 개인정보 침해사례분석과 보호정책에 관한 연구, p. 81.
14) 김종호, 전게논문, p. 82.
15) 도쿄=연합뉴스, 2001. 3. 27) 김용수특파원 = 일본 정부는 27일 각의에서 인터넷을 통한 개인 정보 유출 및 고객 정보 전매를 막기 위해 기업이나 단체가 개인 정보를 다룰 때지켜야 할 의무사항 등을 규정한 개인정보 보호법안을 가결했다.
법안은 개인 정보를 데이터 베이스로 보유하고 있는 개인정보 취급 사업자를대상으로 개인 정보의 적정 취득, 투명성 확보, 제3자 제공 제한 등의 5개 기본 원칙을 준수하도록 했다.
이 법안은 특히 개인 정보를 ▲본인의 동의 없이 제 3자에게 유출하는 행위를 원칙 금지시키는 한편 ▲본인의 요구가 있을 경우 정보 개시, 정정, 사용 중지 등의조치를 취하고 ▲당사자의 고충을 신속, 적절하게 처리할 것을 사업자에게 의무화,당국의 개선 명령을 따르지 않을 경우 벌금을 부과하도록 한 것이 특징이다.
법안은 그동안 논란이 거듭돼온 보도 기관의 개인 정보 취급에 대해서는 학술연구, 종교 활동, 정치 활동 분야와 마찬가지로 개인 정보 보호법의 기본 원칙은 준수토록 하되 의무 규정 적용 대상에서는 제외시켰다.

호와 관련된 규정을 대폭 강화하고 처벌규정도 강화하여 법명도 정보통신망이용촉진및정보보호등에관한법률로 바꾸어 2001년 7월 1일부터 시행하고 있다.

따라서 우리나라 개인정보보호와 관련된 법체제는 공공기관에 관한 것은 공공기관의개인정보보호등에관한법률이 민간부분에 관한 것은 정보통신망이용촉진및정보보호등에관한법률(이하 정보통신망법이라 한다.)이 기본적으로 규율하고 있다고 할 것이다. 기타 단행법으로는 전자서명법(개인정보의 열람, 수집동의권 등 보장), 통신비밀보호법(불법감청 등 금지), 전기통신사업법(개인정보공개의 금지 등) 등을 들 수 있다.

1) 정보통신망법에 있어서의 개인정보보호 개요

개정된 정보통신망법에서는 OECD에서 권고하고 있는 개인정보보호 지침에서 제시된 개인정보보호 기준을 대폭 수용하고 있다고 생각된다.

우선 제22조부터 제40조까지 개인정보와 관련하여 규정하고 있다. 주요내용으로는 개인정보의 수집제한(제22, 23조), 개인정보의 이용 및 제공 제한(제24조)을 규정하고 있으며 특히 제28조에서는 개인정보의 보호조치에 관해서 정보통신서비스 제공자에게 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안정성 확보에 필요한 기술적·관리적 조치를 강구할 의무를 지우고 있다.[16] 또한 제30조 이하에서는 이용자의 권리에 관해서 규정하면서 동의철회권, 개인정보 열람 및 정정 요구권 등 적극적인 권리를 보장하고 있다.

나아가 제32조에서는 이용자의 손해배상 청구권과 정보통신서비스제공자의 입증책임 부담을 규정하고 있는 것은 특이하다.[17] 더욱이 제33조 이하에서는 개인정보와 관련된 분쟁을 해결하기 위하여 개인정보분쟁조정위원회를 둔 것은 그동안 세계 선진국가들이 독립적인 개인정보보호기구를 두고 있는 경향을 따른 것이라 할 수 있다. 한 걸음 더 나아가 제58조에서는 개인정보와 관련된 규정들을 "정보통신서비스제공자 외의 자로서 재화 또는 용역을 제공하는 자 중 대통령령이 정하는 자가 자신이 제공하는 재화 또는 용역을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에 이를 준용한다."고 규정하여 규정의 대상을 오프라인 사업자에게로 확대하고 있다.

정보통신망법의 개인정보 규정은 그동안 개인정보 관련범죄 중에서 공공기관의개인정보보호등에관한법률이나 신용정보의이용및보호에관한법률 등에서 특별히 규정하고 있는 사항 외에는 규제할 수 없었던 법률상의 맹점을 상당부분 해결하여 정보통신업체 혹은 정보통신업체가 아니더라도 개인정보를 부당하게 취급하는 행위에 대해서 규정하고 있다는 측면에서는 상당히 진일보한 것으로 평가된다.

2) 인터넷상의 개인정보침해범죄 예방을 위한 안전성 확보 문제

16) 제28조 (개인정보의 보호조치) 정보통신서비스제공자등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 조치를 강구하여야 한다. [[시행일 2001·7·1]]

17) 제32조 (손해배상) 이용자는 정보통신서비스제공자등이 이 장의 규정을 위반한 행위로 손해를 입은 경우에는 그 정보통신서비스제공자등에 대하여 손해배상을 청구할수 있다. 이 경우 당해 정보통신서비스제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

이제 여기에서는 정보통신망법상의 개인정보보호와 관련된 다른 제반규정의 문제는 접어두고 안전성확보 문제를 짚어 보고자 한다.

우선 동 법 제28조에서는 정보통신서비스제공업자에게 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성확보를 위한 기술적·관리적 조치를 강구할 의무를 부담시키고 있으며 다시 제45조에서는 정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하여야 한다고 규정하고 있다.[18] 제28조의 규정은 개인정보를 관리하는 내부적 안정성확보조치에 중점을 둔 것이라면 제45조에서는 내·외부적 보호조치를 포함한다고 할 수 있다. 다만 동 법 제48조에서는 제45조에서 규정한 보호조치를 침해하는 행위와 관련하여 과거의 법이 같은 조에서 직접적으로 규정하고 있는데[19] 반하여 별도의 조항으로 분리, "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 아니 된다."로 규정함으로써 그 범위를 크게 확대하여 단순 보호조치 침해행위가 아니라 접근권한 초과행위까지 처벌할 수 있도록 규정하고 있다.

나아가 현행 정보통신망법은 보호조치에 대한 이행을 담보하기 위해 정보보호에 관한 지침을 정하여 고시하고 정보통신서비스제공자에게 그 준수를 권고할 수 있도록 하고 있다. 그러나 이는 권고사항일 뿐 정보통신서비스제공업체가 따라야 할 법적의무까지는 없다고 할 것이다. 또한 개인정보의 안전성확보를 위한 조치에서는 더욱 훈시적인 규정과 손해배상청구소송시의 입증책임부담을 제외하면 이의 이행을 담보할 수단이 없다. 따라서 개인정보를 수집·관리하는 정보통신서비스제공업체가 비록 동 법에서 규정하고 있는 안전조치, 보호조치를 강구하지 않았다 하더라도 의무이행을 강제할 수는 없는 것이므로 그 실효성이 의심된다 할 것이다.

물론 손해배상청구소송에 있어서 입증부담을 정보통신서비스제공업자에게 지운 것은 향후 개인정보보호를 위한 정보통신서비스제공업자의 관리의무에 대한 실효성을 담보하기 위한 조치로서 환영할만 하다. 하지만 사실상 정보통신서비스 제공자가 관리하는 개인정보 침해의 문제는 위에서 언급한 사례에서 보듯 외부에서도 얼마든지 해킹 등을 통하여 집약된 데이터를 짧은 시간 동안에 유출가능하고 그 대상 또한 자칫 사이버 공간을 이용하는 전 네티즌들이 될 수 있는 등 광범위한 현상을 낳게 되므로 좀 더 강력하고 실효성 있는 안전성 이행확보 수단이 요구된다고 할 것이다.

---

18) 제45조 (정보통신망의 안정성 확보 등) ①정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하여야 한다.
②정보통신부장관은 제1항의 규정에 의한 보호조치의 구체적 내용을 정한 정보통신서비스의 정보보호에 관한 지침을 정하여 고시하고 정보통신서비스제공자에게 그 준수를 권고할 수 있다.

19) 개정전의 정보통신망이용촉진등에관한법률 규정은 다음과 같다.
제19조 (정보통신망의 안정성 확보등) ①정보통신서비스제공자는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 강구하여야 한다.
③누구든지 불법 또는 부당한 방법으로 제1항의 규정에 의한 보호조치를 침해하거나 훼손하여서는 아니된다.

2) 정보통신업체의 개인정보 수집과 관련된 문제

공공기관의개인정보보호등에관한법률에서는 개인정보를 수집하는 공공기관에 대한 제한규정을 두고 있다. 우선 개인정보를 보유하고자 하는 공공기관에서는 행정자치부장관에게 사전에 통보해야 할 의무가 있으며 연 1회이상 관보에 공고하도록 규정되어 있다. 그러나 민간 정보통신서비스제공자는 누구라도 제한 없이 개인정보를 수집할 수 있으며 사실상 그 수집범위도 제한이 없는 것으로 판단된다. 물론 정보통신망법 제23조에서는 필요한 최소범위의 정보수집을 명시하고 그 외의 정보를 제공하지 아니한다는 이유로 서비스 제공을 거부할 수 없도록 규정하고 있다.[20] 나아가 제23조 제2항의 규정을 위반하는 경우에는 500만원의 과태료 처분을 하도록 규정하고 있으나 실제 "필요한 최소범위의 정보수집"에 대해서는 하위법령에서도 아무런 규정을 두고 있지 않아 정보통신업체가 수집할 수 있는 개인정보의 범위에 대해서는 불명확하다. 따라서 과태료 처분 규정 또한 실효성을 발휘할 수 있을지 의문이다.

한국소비자보호원 사이버소비자센터의 의식조사결과[21] 네티즌들의 86.8%는 각종 인터넷 사이트 회원 가입시 요구하는 개인정보량이 과다하다고 응답하고 있으며 개인정보 중 제공하기 가장 꺼려하는 것으로 예금계좌(81.4%), 신용카드(78.3%), 주민등록(77.9%), 자택주소(51.6%), 휴대폰번호(39.6%) 등을 들고 있다. 이는 실제적으로 사생활 침해와 밀접하게 관계된 정보들이다. 그러나 대부분의 사이트에서 예금계좌, 신용카드 번호를 제외한 나머지 정보들을 요구하고 있는 실정이며 전자상거래, 온라인 쇼핑몰 등에서는 신용카드 정보가 필수적으로 요구되고 있다. 나아가 실명확인을 위해 입력된 개인정보를 바탕으로 금융기관 등에서 신용정보 제공 동의서를 통해 만들어진 신용정보회사의 데이터베이스와 연동시키는 사이트도 점점 늘어가고 있는 추세이다.

IV. 사이버공간의 개인정보침해범죄 방지를 위한 법적대책

위에서 제기한 문제를 토대로 현실적으로 심각하게 다가 오고 있는 민간 정보통신업체에서의 개인정보침해 범죄를 방지하기 위해서 우선 개인정보를 수집·관리하는 정보통신망에 대해서는 기본적으로 좀 더 강화된 규제와 관리가 필요하다고 본다. 실제적인 필요에 의해서 일정한 수준이상의 개인정보를 수집하는 경우 수집할 수 있는 주체를 제한적으로 허용하며 필요한 경우 이를 허가 혹은 등록제로 전환하되 반드시 일정기준이상의 안전 및 보호조치를 취하는 경우에 한하고 날로 발전하는 침해수법에 비추어 정기적인 행정지도를 받도록 하는 것이다. 물론 규제적이고 행정편의주의적인 발상이라는 비판이 있을 수는 있으나 적어도 정보통신서비스 이용자들에게 필요없이 과대한 정보를 요구하거나 수집하지 않도록 하는 조치가 필요하며 개인의 소중한 정보가 범죄인의 손에 유출되지 않도록 하는 최소한의 의무를 지우는 일이 필요하다고 할 것이다.

---

20) 제23조(개인정보의 수집의 제한 등) ① 정보통신서비스제공자는 사상·신념·과거의 병력 등 개인의 권리·이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 이용자의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.
② 정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보외의 개인정보를 제공하지 아니한다는 이유로 당해 서비스의 제공을 거부하여서는 아니된다.

21) http://safe.cpb.or.kr/textdata/HOMEPAGE/200101/1900003/ecre010119.pdf 참조

1. 개인정보 수집 등록제 도입 및 개인정보 수집의 제한

개인정보의 유출 및 그로 인한 프라이버시 침해를 방지하기 위해서는 관련법령을 정비하여 개인정보를 수집할 수 있는 자격을 제한하고 개인정보의 범위를 명확히 하여야 한다. 실제 신용정보의이용및보호에관한법률에서는 신용정보업을 영위할 수 있는 주체에 대한 엄격한 자격요건을 정하고 금융감독위원회의 허가를 얻어서만 영업이 가능하도록 규정하고 있다.[22]

외국의 사례에서도 보았듯이 영국을 비롯한 EU회원국들은 OECD의 개인정보보호를 위한 8개 원칙을 실질적으로 담보하기 위해 그 형태는 여러 가지이나 정보보호등록관 같은 개인정보 감독기구를 두고 있다. 물론 우리나라에서도 한국정보보호진흥원, 개인정보분쟁조정위원회 같은 기구를 통해서 개인정보 침해 문제를 다루고 있지만 실제로 개인정보 감독기구로서의 역할은 미미하다고 할 것이다.

따라서 효율적인 개인정보보호업무를 추진하기 위해 행정기구로서 개인정보 수집업체의 등록, 관리 업무를 수행할 감독기구를 신설하여 「개인정보 수집의 등록제」를 시행하는 것이 바람직하다. 수집주체를 제한하는 구체적인 방안으로 인터넷상의 개인정보를 구분하되 성명, 전자우편 등 네티즌들이 제공하기를 꺼리지 않는 정보에 대한 수집은 특별한 제한이 없도록 하지만 주민등록번호 등 개인의 신상정보와 밀접한 관련이 있는 정보를 수집하는 경우에는 일정한 자격요건이 있는 업체만이 가능하도록 하고 사전 등록하도록 하는 것이 바람직하다. 물론 정보통신부에서는 지난 2000년 학계, 업계 등이 참가한 공청회를 통해 개인정보지침을 만들고 6월 1일부터 시행하고 있으며, 서비스제공자가 이용자의 개인정보를 수집하는 경우에는 기본적인 서비스 제공을 위하여 필요한 필수항목과 부가적인 서비스 제공을 위하여 필요한 선택항목으로 구분하여 이용자가 기입할 수 있도록 조치하고 있지만[23] 여기에서 규정하고 있는 필수항목과 선택항목의 구별도 명확하지 아니하여 실제 정보통신업체들은 주민등록번호, 주소, 전화번호 등을 필수항목으로 하고 있어 실질적으로 이용자들은 중요한 정보라고 생각하는 것들을 제공할 수밖에 없는 실정이다.
또한 정보통신망법 제23조 제2항의 규정도 개정하여 필요한 최소한도의 개인정보가 무엇인지 명확히 하는 것도 필요할 것이다.

2. 주요 개인정보 수집업체에 대한 안전성확보 이행강제

프라이버시 보호에 관한 OECD 가이드라인은 프라이버시 보호원칙의 하나로 "안전보호의 원칙"을 제시하였고 미국의 1974년 프라이버시법은 적절한 관리적, 기술적 및 설비적 방어조치를 확립할 의무를 규정하고 있다.[24] 프랑스는 프라이버시보호기관에 컴퓨터 시스템의 안전성에 관한 대책을 감독하는 강력한 법적 권한을 부여하고 있으며 이 기관은 각 시스템의 안전성에 관한 대책을 감독하는 강력한 법적 권한을 부여하고 있고 일본의 경우에도 1988년 개인정보보호법에서 개인정보의 안전 확보에 대해 규정하고 있다.[25] OECD는 안전성확보에 관한 내용을 더욱 세분화 하여 1992년 11월에 "정보시스템의 안전성에 관한 가이드 라인"을 제시하고 공공부문과 민간부문에 다 적용할 것을 권고하고 있다.[26]

---

22) 제4조 (영업의 허가) ①신용정보업을 영위하고자 하는 자는 제3항의 규정에 의한 업무의 종류별로 금융감독위원회의 허가를 받아야 한다. [개정 97·8·28, 99·1·29, 99·5·24]
23) http://www.cyberprivacy.or.kr/indexf/indexf_d1.htm 참조
24) 김종호, 전게논문, p. 67.
25) 김종호, 전게논문, p. 68.
26) 김종호, 전게논문, p. 70.

앞에서도 언급하였다시피 우리나라의 정보통신망법에서도 안전성 확보와 관련된 규정을 두고 있으나 이는 다분히 훈시적 규정에 불과하다 할 것이다. 따라서 중소규모의 정보통신서비스제공업체에서는 대부분 아무런 보호조치도 취하지 않고 있는 것이 앞에서 본 통계에서 나타나 있다. 심지어 개인의 신용정보와 밀접하게 관련되어 있는 증권계좌, 비밀번호 등을 관리하는 사이버증권 사이트조차도 아무런 안전·보호시설 없이 운영하는 경우도 있다. 그러므로 개인정보를 수집, 보관, 관리하는 업체로 하여금 안전성 및 보호조치를 강구하는 것을 의무화할 필요가 있다.

우선 그 방안으로 앞에서 언급한대로 주요 개인정보 수집업체에 대한 등록제를 시행하는 경우 일정 기준이상의 안전시설, 보호조치를 강구하는 경우에만 등록되도록 하는 제도를 도입하는 것이다. 나아가 안정시설, 보호조치의 경우에는 그 침투기술이 급속히 발전하므로 주기적으로 그 기준을 고시하고 그 기준에 따르도록 행정지도를 할 수 있도록 하는 것도 필요할 것으로 판단된다. 실제 개인정보 침해사례를 분석해 보면 최초에 한 번 설치된 보호시설, 보안시설은 최근의 기술로 쉽게 뚫을 수 있으며 더 이상 보안설비로서의 기능을 상실하는 경우가 많기 때문이다.

V. 맺음말

기존의 사례에서 보듯 개인정보 유출 피해자는 1건에 수백만명에 이른다. 또한 제시된 조사사례에서 보듯 우리나라의 네티즌들은 정보통신서비스제공업체들에 의한 개인정보 수집에 대해서 신뢰감을 갖지 못하고 있으면서도 서비스를 받기 위해 자신의 소중한 개인정보를 큰 의식없이 제공하는 성향을 지니고 있다. 특별히 우리나라 인터넷 업체들이 요구하는 개인정보의 깊이는 외국 정보통신업체들이 성명, 간단한 거주지, 전자우편 주소 등만을 요구하는 것과는 아주 대조적이다. 또한 이제 개인정보의 자산적 가치가 인정되고 수집한 개인정보를 판매하는 인터넷 업체도 생겨났다. 그러나 개인정보유출로 피해를 입은 피해자들은 자신의 피해구제에 무관심한 편이다. 최근에 YMCA에서 개인정보 유출 사건에 대한 집단소송을 준비중이라는 보도도 있었지만 우리나라에서는 아직 집단소송제도가 도입되기 전이고 도입된다하더라도 우선 자본금 2조원이상의 업체를 대상으로 단계적으로 도입된다 한다.[27] 사실상 개인정보 유출 피해자는 자신의 개인정보가 사업자들뿐만 아니라 범죄자들의 손에 넘어갈 수도 있는 상황을 맞고 있으나 관련법령의 미비와 사업자들의 무관심 속에 그냥 지나치고 있는 것이다.

이제 지식정보사회에서 개인의 프라이버시 보호문제는 어떤 면에서 보면 충분조건이 아니라 필요조건이다. 현실공간에서의 안전한 생활 못지 않게 사이버 공간에서의 안전한 생활도 중요하며 국가는 사이버공간에서 일어나고 있는 개인정보 침해 범죄로부터 국민을 보호하기 위한 다각적인 대안을 마련해야 한다. 또한 개인정보보호 문제는 헌법에서 보장하고 있는 사생활 보호와 관련된 국민의 정당한 권리를 보장하기 위한 조치와도 관련이 깊다. 그 대안의 하나로 범죄의 위험이 큰 환경에 대한 규제와 예방조치를 의무화한다는 관점에서 이제 개인정보 수집의 핵심주체로 부각되고 있는 정보통신사업자에 대해 구체적이고 실효성 있는 대책을 마련하는 것이 절실한 시점이 아닌가 한다.

27) 2001년 9월 23일자 연합뉴스 참조(http://www.yonhapnews.co.kr)

참 고 문 헌

1. 단행본
· 김연수, 개인정보보호:고도지식정보 사회의 개인정보와 Cyber Law, 사이버출판사, 2001
· 김철수, 헌법학개론,(서울 : 박영사), 1997
· 변재옥, 정보화 사회의 프라이버시와 표현의 자유, 서울:컴퓨티게이션북스, 1999
· 개인정보보호지침 제정을 위한 공청회 자료집, 한국정보보호센터, 2000

2. 논 문
· 김연수, 개인정보 보호 및 활용을 위한 IT 분야의 활성화 방안에 관한 연구, 한국정보보호센터, 2001
· 김종호, "지식정보사회의 개인정보 침해사례분석과 보호대책에 관한 연구". 경희대학교 대학원 박사논문, 2001
· 정영화, Cyberspace에서 Privacy(현행 개인정보보호법제의 문제점을 중심으로), 동아일보 인터넷 신문, 2000
· 정재훈, 민간부문에서의 정보프라이버시 보호, 정보법학회 세미나자료, 1997
· 조광희, 정보사회에 있어서 개인의 정보공개와 프라이버시 보호와의 관계에 관한 연구, 언론연구, 1994
· FTC(미연방거래위원회) 온라인프라이버시 보고서 번역본, 한국정보보호센터, 1998
· Safe Harbor Translation, Safe Harbor Privacy Principles, 한국정보보호진흥원, 2001

3. 인터넷 홈페이지
· http://www.cyberprivacy.or.kr
· http://www.kisa.or.kr
· http://www.ftc.gov
· http://safe.cpb.or.kr
· http://www.yonhapnews.co.kr