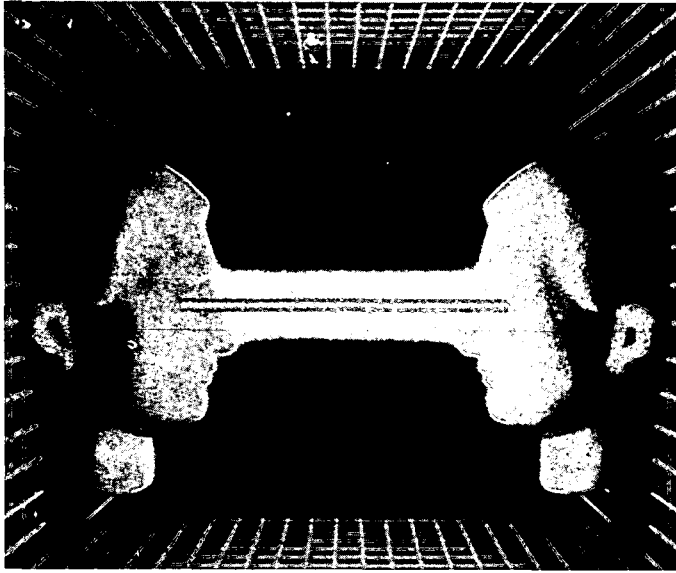


프라이버시 침해의 문제점과 그 보호대책

Privacy Protection



1. 개인정보의 보호현상

(1) 개인정보의 보호필요성

오늘날의 정보화시대 (information age)에는 뉴미디어나 고도정보통신시대라는 말이 매스컴을 떠들석하게 하고 있다. 이러한 정보화시대에는 정보의 공개나 확산이 널리 이루어짐과 동시에

정보비밀의 보호가 중요한 과제가 되고 있다. 이러한 비밀이 되는 정보에 대해서는 국가기밀¹⁾ 보호, 개인정보 보호 및 행정상의 정보공개외에 영업비밀은 나라의 안전보장상의 요청에 의한 것이고,²⁾ 개인정보 보호는 개인의 프라이버시보호가 중심이며, 행정상의 정보의 공개는 민주주의 이

념에서 나오는 것이다.³⁾

오늘날 컴퓨터보급이 확대됨에 따라 각종 자료가 전산화를 통해 데이터베이스로 저장되고 동시에 이들 정보의 상품화현상이 늘어났다. 그에 따라 개인정보의 수집 및 처리나 이용과정에서 여러형태의 남용위험이 생겨나고, 이로 인해 개인의 사생활침해 등 심각한 문제가 초래되고 있다. 일반시민들은 「자신의 정보가 본인이 알지 못하는 곳에서 관리되지 않는가」하는 불안을 가진다.

1989년에 My Sister Sam이라는 텔레비전연속극에 출연한 Rebecca Schaeffer라는 여배우가 자기의 팬에게 살해되었다. 범인은 캘리포니아주의 자동차등록소(DMV)에서 그녀의 주소를 구했다고 알려졌다.⁴⁾ 이는 극단적인 사례이지만, 미국연방대법원 판사인 Robert Bork씨가 임명동의청문회를 받을 때 생겨난 해프닝은 흥미롭다. 보크부부는 2년간 동네 가게에서 146개의 비디오테이프를 빌려 보았는데 이 목록을 주간지가 공개하였다.⁵⁾ 다행히 그들 부부는 건전한 비디오만 빌려 보았지만, 만약 그 속에 음란비디오가 한 둘만 들어 있었다더라도 그들은 명예에 치명적 손상을 입었을 것으로 생각된다.

이처럼 오늘날 개인의 정보를 보유하고 있는 정보시스템은 많이 있다. 공공기관의 경우 내무부의 주민등록이나 자동차보유자료를 비롯하여 국세청, 통계청등이 엄청난 양의 개인정보를 보유하고 있으며, 의료보험조합이나 은행 크레디트

카드회사 및 증권회사뿐만 아니라 대부분 기업은 고객데이터베이스를 보유하고 있다. 이와같은 개인정보는 당연히 본인의 프라이버시와 관계되므로 함부로 침해해서는 안된다. 따라서 개인정보를 포함한 정보시스템의 개발과 운용에 있어서는 개인정보 보호에 대한 충분한 배려가 필요하다. 이 때문에 한국에서도 이미 공공기관의 개인정보 보호에 관한 법률등이 제정되어 있다.

(2) 개인정보의 정의

보호의 대상이 되는 개인정보란 무엇인가. 후술하는 개인정보 보호법에서는 다음과 같이 정의하고 있다. 「생존하는 개인에 관한 정보로서, 당해정보에 포함되어 있는 성명, 주민등록번호등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도, 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)을 말한다. (법 제2조 2호) 여기서 주민등록번호「등」에는 번호, 기호 기타의 부호에 의해 식별할 수 있는 것을 말한다.

개인정보보호법은 컴퓨터의 처리에 관한 개인정보의 취급을 대상으로 하고 있다. 그러나 문서만을 작성하는 등의 단순업무처리를 위한 행위로서 대통령령이 정하는 행위를 하는 것을 제외한다. 결국 메뉴얼처리의 것은 포함하지 않는다. 우리나라에서는 이것이 통념으로 되어 있다고 하겠다.

- 1) 주요제국의 국가기밀보호규제, 입법참고자료 제265호, 1989년 12월 국회사무처 입법조사국.
- 2) 최근 일본의 후지TV 서울지국장이 취재의 이름으로 군사기밀을 수집한 충격적인 사건이 있었다(조선일보, 1993년 6월, 30)
- 3) 홍준형, 정보공개청구권과 정보공개법, 법과 사회 제6호 창작과 비평사 1992년 76년; 국민의 알 권리 보장을 위해 정부는 행정정보의 공개제도를 위한 행정정보공개법을 1995년에 제정할 목표를 두고 있다(중앙일보, 1993년 6월 19일, 22면).

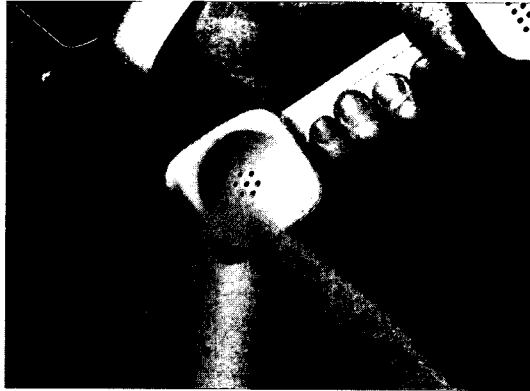
2. 개인정보 보호의 제도화

정보화시대에는 누구라도 행정기관이나 기업등

- 4) James Hamey, DMV : Registered Driver : License Plate : Confidentiality, USA TODAY, March 10, 1992, at 3A.
- 5) Personalities, Washington Post, Sept. 26, 1987, at C3

의 타인의 자신의 정보를 전혀 알수 없게 할 수는 없다고 생각한다. 문제는 타인에게 알려지는 정보의 내용과 이용방식이다. 이 점에서 개인정보의 보호에 관한 제도화인 입법조치가 필요하다.

우리나라에서는 행정에 대한 신뢰성을 확보한다는 관점에서 「공공기관의 개인정보 보호에 관한 법률」(이하「개인정보보호법」이라 부른다)을 1994년 1월에 공포하였다.⁸⁾ 동법은 공공기관의



(1) 공공기관의 개인정보 보호

오늘날 대부분의 선진국에서는 개인정보 보호의 법률이 제정되어 있다. 1973년 스웨덴의 데이터법에 이어, 미국은 1974년 연방프라이버시보호법(Privacy Protection Act)을 제정하여⁶⁾ 연방정부가 개인의 자료를 허가없이 공개하는 것을 금지시켰다.⁷⁾ 이어 독일은 1977년 연방데이터보호법, 프랑스는 1978년의 정보처리 데이터파일 및 개인의 자유에 관한 법, 영국은 1984년의 데이터보호법, 일본은 1988년의 행정기관이 보유한 전자계산기처리에 관한 개인정보의 보호에 관한 법률을 만들었다. 대체로 1970년대 말에서 1980년초에 제정된 이들 나라들의 프라이버시 보호입법은 데이터베이스의 등록과 데이터의 사용, 저장, 전송에 관한 제한을 기본골격으로 하고 있다. 다만 국가에 따라서 법률의 내용(예, 개인정보의 정의, 규제대상의 분야)은 다르다.

컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적당한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 제정되었다.(동법 제1조). 동법은 1992년 4월 10일에 입법예고된 후, 1993년 말 국회를 통과하여 내년 1월부터 시행하게 되었다.

동법은 정보화사회를 위한 법령정비대책의 일환으로 제정된 것이지만, 특히 최근 공공기관이 보유한 개인정보의 남용가능성이 제14대 국회의 원선거운동과정에서 현실화되면서 이에 대한 비판여론이 빚발치자 대응책으로 마련된 것이라 할 수 있다.⁹⁾ 다만 명칭에서도 알 수 있는 바와 같이 법률의 적용범위는 우리나라의 국가행정기관이나 지방자치단체등 공공기관에 한정되어 있다

6) 黃祐呂, 미국에서 있어서의 정보공개법과 사생활보호법, 미래 정보화사회의 공법적 대응, 한국공법학회, 1989. 5. 26, 학술대회자료, 27면. 祝
7) 5 U.S.C § 552a(1988).

8) 뿐만 아니라 국민의 통신의 자유와 통신비밀을 보호하기 위한 통신비밀보호법이 1993년 12월 17일 법률 제4650호로 제정되어 금년 6월부터 시행하게 되었다. 그에 따라 전화협박이나 타인의 대화비밀등이 보장되게 되었다.(동법 13조 및 14조 참조).
9) 홍준형, 정보공개청구권과 정보공개법, 법과 사회 제6호 창작과 비평사 1992년 98면

(외국에서는 민간분야도 규제대상으로 하는 국가가 많다). 동법은 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관한 기본법적 성격을 가진다(동법 제3조 1항 참조).¹⁰⁾ 그러나 이 법은 보호대상인 개인정보의 범위를 컴퓨터에 수록된 것에 국한시킨 점(제2조 참조), 개인정보의 이용 및 타기관에게 제공하기 위한 요건에 대한 판단권을 당해공공기관의 장에게 부여하고 있다는 점(제10조 1항), 처리정보의 열람 제한에 대한 사유가 지나치게 광범위하고 포괄적이라는 점(제13조) 등의 문제점이 있다. 그런 점에서 국민이 참여할 수 있는 통로인 「개인정보정보심의위원회」(법 20조)를 잘 활용할 필요가 있다고 본다. 동 위원회는 정책이나 제도개선등에 관한 심의기능을 가지나 실제로는 일종의 자문기관으로 보인다. 이 기관의 조직과 기능을 미국에서 논의되고 있는 데이터보호위원회(Data Protection Board, DPB)¹¹⁾로 확대개편할 필요성에 대한 연구검토가 있었으면 한다.

(2) 민간부문의 개인정보 보호

전술한 개인정보보호법은 그 적용대상을 공공기관에 국한시키고 적용제외기관, 즉 민간기관에 관련된 개인정보의 문제는 이 법에 유의한 개인정보의 보호를 위한 조치의 강구와 소관중앙행정기관장의 의견제시와 권고만을 규정함으로써(법 제22조) 실질적으로 자율적 규제에 맡기고 있다.¹²⁾ 그 점에서 이 법률은 민간분야에서는 적용되지 않지만, 민간사업자들에게도 일응의 지침이 된다고 하겠다.

민간분야에 대해서는, 미국의 경우 일반적, 포괄적인 보호법은 없고 영역에 따라 개인정보보호법을 두고 있다. 즉 소비자 신용정보자료에 대한 규제를 하는 1970년의 공정신용조사보고법(Fair Credit Reporting act),¹³⁾ 금융기관이 개인의 자료를 연방기관에게 알려주기 전에 해당 개인에게 통지할 것을 규정한 1978년의 금융프라이버시권리법(Right to Financial Privacy Act), 종합유선방송사업자가 가입의 동의를 얻지 않고는 가입자의 정보를 공개할 수 없게 한 1984년의 유선통신정책법(Cable Communications Policy Act), 전자통신에 대해 허가없이 끼어드는 것을 방지한 1986년의 전자통신프라이버시법(Electronic Communications Privacy Act)과 비디오테이프사업자가 개인자료를 공개하지 못하게 한 1988년의 비디오프라이버시보호법(Video Privacy Protection Act)¹⁴⁾ 등이 있다.

그러나 잡지사가 구매자의 동의를 얻지 않고 구매자명부를 DM광고업자에게 판매하여도 판매자의 프라이버시를 침해하지 않는다는 판결¹⁵⁾등이 나옴에 따라 민간부문에서의 개인정보 대금업의 규제등에 관한 법률(30조)과 할부판매법(42조의 4)에서 신용정보를 현금수요자의 반환능력이나 구입자의 지급능력의 조사이외에 사용하는 것을 금지하고 있다. 또한 통산성이 1989년에 민간부분에서의 전자계산기처리에 관한 개인정보의 보호에 관한 지침을 마련하여, 관계사업자단체에 통달(우리나라 고시에 해당)을 내렸다.¹⁷⁾ 그에 따라 각각의 업체가 개인정보 보호의 이념에 맞추어 가이드라인을 두고 있는 바(예, 정보

10) 공공기관의 컴퓨터에 의하여 처리되는 개인정보라도 통계법이나 국가안전보장법과 관련되는 것에 관하여는 이 법을 적용하지 아니한다(동법 3조2항).

11) Joshua D.Blackman, A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector, Santa Clara Computer and High Technology Law Journal, Vol. 9, No.2 1993 p.436

12) 홍준형, 전계 논문, 99면.

13) 굴고, 크레디트카드의 법률문제에 관한 연구, 1988년 137면.

14) 동법은 전술한 Bork사건 이후에 제정되었다.

15) Shibley v. Time 341 N.E.2b 337, 338(Ohio Ct.App. 1975).

16) Blackman, supra p.460.

17) 병전순일, 정보법, 유배각 1993년 150면.

서비스산업협회)¹⁸⁾, 금융기관에서의 개인데이터보호를 위한 취급지침(금융정보시스템센터, 1987년) 등의 자주 규제가 중요한 역할을 하고 있다.

우리나라에서도 신용카드업법에 개인정보규정이 있다. 즉 신용카드업법 제14조는 다음과 같이 규정하고 있다.

제14조(신용자료등의 비밀보장) (1)신용카드업자의 임원 및 직원은 그 업무를 수행함에 있어 알게 된 신용카드회원 직불카드회원 신용카드가맹점 기타 거래자의 신용에 관한 자료나 제11조의 규정에 의하여 금융기관으로부터 제공받은 자료 또는 정보(이하 “자료등”이라 한다)를 업무외의 목적에 사용하거나 본인의 동의없이 다른 사람에게 제공 또는 누설하여서는 아니된다. 다만, 다음 각호의 1에 해당하는 경우에는 그러하지 아니한다.

1. 재무장관 또는 한국은행감독원장이 업무상 필요한 감독·검사를 위하여 자료등을 요구하는 경우
2. 법원의 관한 법률의 규정에 의한 질문 조사를 위하여 소관관서의 장이 서면으로 자료등의 제공을 요구하거나 과세에 관한 법률의 규정에 의하여 제출의무가 있는 과세자료의 제공을 요구하는 경우
3. 조세에 관한 법률의 규정에 의한 질문 조사를 위하여 소관관서의 장이 서면으로 자료등의 제공을 요구하거나 과세에 관한 법률의 규정에 의하여 제출의무가 있는 과세자료의 제공을 요구하는 경우

(2)제1항 단서의 규정에 의하여 자료등을 알게 된 자는 그 알게 된 자료등을 목적외의 용도에 사용하거나 다른 사람에게 제공 또는 누설하여서는 아니된다.

18) 그 구체적인 상황은 통산심(기계정보산업국 정보처리진흥과)에 있는 개인정보보호조치등록부제도를 열람하면 알수 있다고 한다.

또한 금융실명제의 실시에 따라 개인의 금융거래비밀이 종전보다 널리 보장되고 있음은 최근의 국정감사에서도 여실히 증명되었다. 일반적으로 사기업이 직무상알게 된 사적인 정보를 정당한 이유없이 불특정다수인에게 공표하거나 제3자에게 누설한 경우에는 프라이버시권리의 침해가 되어 원칙적으로 채무불이행이나 불법행위가 된다고 할 것이다.

3. 개인정보 보호의 원칙

개인정보 보호의 원칙은 경제협력개발기구(Organization for Economic Cooperation and Development, OECD)이사회가 1983년 9월 23일에 발표한「가이드라인」에 있다. 우리나라나 일본의 개인정보보호법도 이 가이드라인에 준거해서(다만 조건을 완화해서)제정되어 있다.¹⁹⁾ 이 가이드라인은 국내적인 문제와 국제적인 문제의 쌍방을 포함하고 있는 바, 제2부 국내처리에 대한 8원칙의 요점은 다음과 같다.²⁰⁾

- ① 수집제한의 원칙 - 적법하고 공정한 수단에 의해 본인의 동의하에서 수집하여야 한다.
- ② 데이터 품질의 원칙 - 이용목적에 따라 정확, 안전한 최신데이터 유지.
- ③ 목적명확화의 원칙 - 목적 범위내에서의 데이터 수집과 이용.
- ④ 이용제한의 원칙 - 데이터의 타목적이용의 금지.²¹⁾

19) 견장무지, 대야행부, 영화소태랑, 길전정부 편, コソビグ-夕と 법률, 공립출판(주), 1992년 199면.

20) 송상현/안경환, 컴퓨터안전과 프라이버시보호에 관한 연구, 1988년 11월 한국과학재단 28면.

21) 예를 들면 전화회사가 전화가입자의 주소와 성명등을 무단으로 타인에게 판매하는 것은 당초의 수집목적을 면세한 행위로서 가입자의 인격적 이익을 침해한 것이 된다.

⑤ 안전보호의 원칙—데이터의 분실, 부당한 접근, 부당한 수정, 부당한 열람에의 안전 조치.

⑥ 공개의 원칙—시스템의 주지.

⑦ 개인참가의 원칙—본인의 데이터에의 접근, 데이터에의 이의신청, 데이터의 소거, 수정등의 권리.

⑧ 책임의 원칙—제원칙을 실시하기 위한 데이터관리자의 책임.

여기서 본인이라 한 것은 시스템이 갖는 개인 정보가 대상으로 한 개인을 가리킨다.

4. 시스템관리상의 문제점

여기서 민간부문의 정보처리서비스에 문제를 한정해서, 개인정보 보호에 대해서 OECD제원칙을 기준으로 하여 재래방식의 시스템 관리에 있어서 문제가 되는점을 열거한다. 말할 필요도 없이, 민간사업자의 시스템에 있어서는 민간부문에서의 규제가 없는 우리나라 일본에서는 OECD원칙에 반하더라도 위법은 아니다.

시스템관리자의 입장에서 보면 OECD원칙중 ②, ③, ⑤, ⑧은 보안관리의 원칙에서 보더라도 자명하다.

더욱이 ①, ⑥, ⑦에 대해서는 재래의 시스템 관리자의 의식속에는 전혀 없었던 원칙이다. 이들 원칙을 달성하기 위해서는 코스트의 증가를 견뎌내야 한다. 결국 시스템의 효율성을 희생시키지 않을 수 없는 점이 있다. 특히 ④에 대해서는 시스템관리자의 상식과는 전혀 상반하고 있다.

(1) 데이터베이스의 다목적 이용

원래 데이터베이스는 데이터의 다목적이용을 하기 위한 도구이다. 예를들면 오늘날 많은 기업이 고객 데이터베이스를 갖고 있다. 이 고객 데

이터베이스를 이용해서 통신판매 시스템을 만드는 것 등은 더욱 전형적인 응용이다. 그러나 이것은 OECD원칙의 ③, ④에 반한다.

(2) 개인정보의 열람, 정정

본인으로부터 정보의 열람청구, 정정청구가 있었던 경우 그것에 어떻게 응하는가 하는 점이다. 시스템 운용자측에서 보면 현실의 시스템이라는 것은 복수의 데이터베이스군이 뒤섞여 연결되어 있는 것이다. 이와같은 데이터베이스의 연기속에서 정보주체나 소비자가 청구하는 데이터베이스를 어떻게 구별하고 관리해야 하는가의 현실적 순서는 아주 번잡한 것으로 될 수 있다.

개인정보보호법에서는 본인에 관한 정보의 열람(사본의 수령)을 청구할 개인의 권리와 처리기관의 장의 열람허용의무를 규정하고 있다. 즉 정보주체가 서면으로 본인에 관한 처리정보의 열람을 보유기관의 장에게 청구할 수 있으며, 이 경우 일반적으로 30일 이내에 열람하게 할 수 있다(법 12조). 또한 본인의 처리를 열람한 정보주체는 당해 처리정보의 정정을 청구할 수 있으며, 이 경우 지체없이 필요한 조치를 취하여 당해 청구인에게 통지하여야 한다(법 14조).

(3) 분산처리

최근의 정보시스템은 다운사이징화와 오픈시스템화의 방향에 있다. 이들의 목표는 지금까지 중앙에서 독점하고 있었던 관리기능을 다수의 현장에 이관하는 것이다. 현장은 시스템 관리에 아마 참여이고 따라서 보안관리의 의식도 희박하다. 그 결과 개인정보 보호의 시스템도 취약하게 된다. 더욱이 시스템을 오픈하면 데이터베이스에 비관계자가 쉽게 접근하게 된다. 이것도 시스템을 취약하게 하는 것이다.

일반적으로 단말기측에서는 개인정보 보호에 관한 관리의식이 약하다. 그 때문에 예를들면 하

드카피의 폐기처분에 대한 관리수준이 낮고, 개인 정보가 기업밖으로 유출되는 경우가 많게 된다.

(4) 퍼스널컴퓨터의 경우

분산처리의 극단적인 사례로서, 현장에서의 퍼스널컴퓨터의 사용이다. 퍼스널컴퓨터의 보안관리기능은 낮고, 또한 현장의 개인정보에 대한 관리의식도 약하다. 따라서 만약 퍼스널컴퓨터안에 개인정보 데이터베이스를 탑재하게 되면 보안관리가 불충분하게 되는 경향이 있다.

더욱이 가까운 장래에 IC카드가 개인정보를 탑재한 초소형 컴퓨터로서 사회속을 전전유통할 가능성도 있다.²²⁾ 이 경우 보안문제는 더욱 현저하게 될 것이다.

(5) 아웃 소싱의 경우

최근에는 정보처리 서비스를 외주하는 경우가 많아졌다. 이때 발주자와 수주자는 앞에서 말한 OECD의 제원칙을 고려하여 이를 분담하여 유지하는 노력이 필요하다고 본다. 이 점에 대해서 발주자와 수주자는 서로 개인정보 보호의 원칙을 의식한 계약을 체결하고, 그같은 관리시스템을 설정할 필요가 있다.

(6) 월경데이터의 유통

국제간 정보의 흐름을 보통 월경정보유통(Transborder Data Flow, TDF)이라한다. 이러한 TDF의 문제가 국제적으로 논의되기 시작한 것은 대체로 1980년대에 와서이다.²³⁾ 개인정보의 보호는 개인의 기본적 인권의 보호차원에서 뿐만 아니라 오늘날은 TDF규제의 필요성에서 논의되고 있다. 왜냐하면 국제적인 정보네트

워크시스템을 구축할 경우에 D국에서는 규제대상으로 되는 개인정보가 A국에서는 규제밖이 될 수 있으며, 이 경우에는 자국의 개인정보보호법에 대한 실효성이 위협받을 수 있기 때문이다.²⁴⁾ 이는 동시에 개인정보보호제도가 월경데이터에 대한 유통의 장벽이 되는 문제도 생겨난다.

영국과 프랑스등의 개인정보보호법은 개인정보 보호법이 없는 국가와의 사이의 개인정보의 온라인 송수를 금지하고 있다.²⁵⁾ 또한 개인정보보호법이 아니라 은행법등의 업법에 의해 개인정보의 국외와의 송수를 금지하고 있는 국가도 있다. 최근에 EC의 집행위원회(European Commission)는 프라이버시에 대한 적절한 보호수준을 갖추지 못한 국가들과의 개인정보이동을 금지시키는 지침초안(draft Directives)를 발표하였다.²⁶⁾ 그에 따라 민간부문에서의 개인정보를 위한 포괄적입법이 없는 미국에서는 이 지침초안에 대한 상호주의요건을 충족하지 못한다는 점에 대한 논의가 일고있다.²⁷⁾

이처럼 개인정보 보호에 대한 법률은 국가마다 다르기 때문에 법적문제나 법적용의 충돌문제가 생겨나게 된다. 이러한 문제를 해결하기 위한 국제적기준의 수립을 위한 노력이 전술한 OECD와 EC의 각료이사회(Council of Europe)에서

24) George W. Coombe, Jr. & Susan L. Kirk, Privacy, Data Protection and Transborder Data Flow : A Corporate Response to International Expectations, Business Lawyer, Vol. 39, 1983 p. 37.

25) 실제로 미국의 제약회사가 개발한 신약을 유럽에서 인체임상실험을 하였는데, 이 자료를 컴퓨터데이터베이스화하여 미국의 FDA에 제출하려고 하였다. 그러나 유럽제국은 이러한 개인의 의료정보를 해외로 유출하지 못하게 규정하고 있기 때문에 결국 미국제약회사는 이 자료를 FDA에 내지 못했다 한다. (Transborder Data and Communications Report, Vol. 7, No. 1, 1984 p.12; 방석호 전제논문에서 재인용)

26) Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, art. 24.1, 1990 O.J. (c277) 3,10

27) Blackman, supra p. 459

22) 실제로 이미 지난해 후반에 광주은행은 IC칩이 내장된 레이저카드를 크레디트카드로 사용하고 있다.

23) 방석호, 정보의 흐름과 그 법적 문제들, 법과 사회 제4호 창작과 비평사 1991년 235면.

있었다. 그 내용은 대체로 한 회원국이 개인의 프라이버시보호만을 이유로 다른 나라로 흘러가는 데이터의 월경을 원칙적으로 막지 못하며, 동시에 프라이버시를 안전하게 보호하기 위한 합리적이고 적절한 조치를 취하여야 한다는 것이다.²⁸⁾

5. 개인정보 데이터베이스의 판매

오늘날 기업이 전문적으로 개인정보의 데이터베이스를 구축하여, 그 자체로서나 또는 서비스로서 그 데이터베이스를 시장에 판매하는 경우가 생겨나고 있다. 이 경우 정보를 본인으로부터만 수집하게 된다면 많은 비용과 노력이 요구된다. 따라서 현실적으로 정보수집에 대한 다양한 수준이 있을 수 있다.

(1) OECD원칙을 준수하는 경우

이 예로는 일본의 자금업체나 신평업체가 공동으로 이용하고 있는 개인신용정보시스템이 있다. 우리의 카드업체도 이러한 방향으로 가도록 노력하고 있다.

(2) 제도적으로 공개되어 있는 정보를 이용하는 경우

법률적으로 공개되어 있거나 공개가 허용되고 있는 개인정보를 이용하는 경우가 있다. 전자의 예로서는 고액납세자명부, 후자에 관해서는 기업의 임원명부 등이 있다.

(3) 공지의 정보를 이용하는 경우

이에 대해서는 사회의 관행으로서 인정되고 있는 경우가 많다. 예를들면 전화번호부의 데이터베이스 등이다. 다만, 전화번호부의 경우에는 별도로 저작권의 문제가 발생할 수 있다.²⁹⁾

(4) 인쇄매체가 전자화한 경우

원래는 인쇄매체로서 간행되어 있었던 것이 전자화(데이터베이스, CD-ROM)되는 경우가 근래에 생겨나고 있다. 예를들면 신문의 축쇄판, 세대주명이 들어간 주택지도등이다. 특히 축쇄판의 경우에는 OECD의 제원칙, 그 중에서도 ①, ⑦의 원칙은 「알 권리」에 의해 방해받고 있다고 할 수 있다.

최근인 1991년에 미국의 Lotus Development사와 Equifax는 공동으로 Lotus Marketplace라는 CD-ROM을 제작하였다. 그 속에는 8천만의 가게와 1억2천만명의 소비자에 대한 성명, 주소, 예상소득 및 좋아하는 상품 100가지등의 정보가 들어 있으며, 이를 중소기업들에게 695달러에 판매할 예정이었다.³⁰⁾ 그러자 약 3만명의 소비자가 자기들의 이름을 CD-ROM에서 삭제해줄 것을 요청하여 결국 판매를 못하게 되었다. 그러나 그 판매를 금지하는 법은 아직껏 미국에도 없다고 한다. 이는 곧 소비자의 항의를 회사임원들이 받아들인 사례이다.

(5) 서비스만 판매하는 경우

개인정보 데이터베이스 자체를 기업밖으로 내보내는 것은 아니지만, 그것을 이용한 서비스를 시장에서 판매하는 사업자가 있다. 예를들면 direct mail(DM)발송대행업 등이다.

(6) 개인정보 보호를 의식하지 않는 경우

개인정보 보호에 대해서는 전혀 의식하지 않고 개인정보의 교환, 판매를 하는 경우도 있다.

(이 글은 한국정보시스템감사인 협회에서 주최한 컴퓨터범죄와 프라이버시보호에 대한 강연 및 토론회의 김문환 국민대법과대학 교수의 글을 옮긴 것이다.)

28) 방석호, 전계 논문 236~237면.

29) 미국연방대법원의 Feist Publications v. Rural Telephone 판결(1991년) 참조.

30) Jacob Sullum, Secrets for Sale: Do Strangers with Computers Know Too Much About You?, REASON, Vol.23, April 1992, at 29.