法學博士 學位論文

電子政府構築에 따른
自己情報管理統制權에 관한 硏究

2010年 2月

釜慶大學校 大學院

法 學 科

張 進 淑

法學博士 學位論文

電子政府構築에 따른 自己情報管理統制權에 관한 硏究

指導敎授 池 圭 喆

이 論文을 法學博士 學位論文으로 提出함

2010年 2月

釜 慶 大 學 校 大 學 院

法 學 科

張 進 淑

張進淑의 法學博士 學位論文을 認准함

2010年 **2**月 日

主 審 法學博士 **(**印**)**

委 員 法學博士 **(**印**)**

委 員 法學博士 **(**印**)**

委 員 法學博士 **(**印**)**

委 員 法學博士 **(**印**)**

<목 차>

<표 목 차>

제1장 서 론

제1절 연구의 배경과 목적

오늘날 정보통신기술의 발달과 함께 급변하는 국제적·사회적 환경에서 국민은 정부에 대하여 다양한 서비스를 요구하고, 각국은 이에 부응하기 위하여 전자정부 구축사업을 추진하고 있다. 특히 1990년대에 접어들면서 주요 선진국들은 정보인프라를 개선하고 국가경쟁력 강화를 위해 정부혁신을 적극적으로 추진 중에 있으며, 2000년대 이후 정부혁신의 전략적 핵심수단으로 전자정부(electronic government)를 적극 활용하고 있다. 그래서 세계적으로 전자정부 구축사업이 정부의 경쟁력을 좌우하는 중요한 요소로 인식되고 있는 상황이다.

우리나라에서도 1980년대 후반에 전자정부의 기본인프라 조성을 시작한 후, 전자정부사업이 국민의 편익 제고, 행정효율성의 향상 등과 같은 효과를 거두면서 정부혁신을 뒷받침하고 있으며, 현재는 이 분야에서 세계적인 선도국가로서 평가받고 있다. 특히 ≪2008년 UN 전자정부평가보고서(UN E-Government Survey 2008)≫에서는 전자정부 준비지수(E-Readiness Index) 부문에서 우리나라는 2004·2005년 연속 세계 5위를 차지하였고, 2008년에는 6위를 하였다. 그리고 온라인 참여지수(E-Participation Index) 부문에서는 2004년 6위, 2005년 4위, 2008년 2위로 각각 평가되어 종합 4위가 되었다.[1] 이처럼 세계적으로 우리나라의 전자정부가 인정받은 것은 국민의 편의와 행정 효율성의 극대화라는 목표하에 전자정부사업을 범정책적 차원에서 적극 추진하여 왔기 때문이다.[2]

---

1) 박선주, 전자정부 해외 동향 : UN E-Government Survey 2008 결과 분석, 한국정보사회진흥원, 2008, 44면. 그리고 미국 브라운 대학이 발표한 세계 전자정부평가에서 2003년 87위에 불과하였으나 2006년에는 198개국 중 세계 1위를 차지하기도 하였다. 또 2008년 미국 브루킹스 연구소(Brookings Institution)가 발표한 세계 전자정부평가 결과, 우리나라가 2006년에서 2008년까지 연속 3년 동안 세계 1위를 차지하였다고 밝혔다(http://blog.naver.com/happymogaha?Redirect=Log&logNo=140055234496 2009.12.13.방문). 그리고 일본 와세다대학의 전자정부 평가에서는 2005년 11위, 2006년, 5위, 2007년 4위 등으로 꾸준히 상승하고 있다는 것으로 평가되고 있다(박선주·김현정, 전자정부 해외 동향, 한국정보사회진흥원, 2008, 35면).

2) 정부는 1987년부터 1999까지 진행된 제1차 국가기간전산망사업을 통해 주민, 토지, 금융 등 국가운영에 필수적인 주요 정보의 데이터베이스화가 이루어졌다. 1992년부터 1996년까지 진행된 제2차 국가기간전산망사업은 제1차 국가기간전산망사업에서 추진했던 사업들을 지속적으로 보

이처럼 눈부시게 발전한 전자정부의 핵심은 정보과학기술을 활용하여 행정기관 내부 또는 행정기관 사이의 업무의 효율성 제고와 대민 서비스의 전자적 수행에 있으며, 결국 어느 한 행정기관이 수집한 정보를 다른 기관이 공동으로 사용하게 된다. 이와 같은 행정정보공동이용은 정부의 능률성·투명성의 제고, 경제적 비용 절감, 정보접근의 평등권 확보, 정책결정에 대한 국민의 참여 강화 등의 효과를 가지고 올 수 있다.

그러나 다른 한편으로는 행정기관이 공동이용하는 행정정보에 개인정보가 포함되어 있다는 것이 문제된다. 즉 행정기관이 정보의 수집·이용·관리의 단계에서 개인의 정보가 개별적 또는 다른 정보와 결합하여 쉽게 공개될 수 있으며, 그 결과 행정기관이 당초의 수집목적과 다른 목적으로 사용하려고 시도하거나 개인이 인식하지 못하는 사이에 정보주체가 원하지 않는 용도로 개인정보가 유출될 위험성이 있다.[3] 특히 전산망에 대한 외부의 해킹이 빈번하고, 세계적으로도 보기 드문 개인식별번호인 주민등록번호를 광범위하게 사용하고, 그 번호 하나로 모든 정보를 검색·수집할 수 있는 상황에서 행정정보의 공동이용이 공적·사적 부문 모두에서 인권침해와 사생활의 자유를 침해할 수 있다. 따라서 행정정보공동이용에서 개인정보의 보호가 전자정부의 성공과 신뢰확보에 핵심적인 문제로 대두되고 있다.

행정정보공동이용에서 개인정보를 보호하기 위하여 무엇보다도 중요한 것은 개인이 행정기관이 보유한 자기정보의 열람·정정·차단·분리·삭제를 청구할 수 있는 권리 즉, 개인정보보호를 위한 자기정보관리통제권을 확립하는 것이라고 할 수 있다.

우리나라에서 전자정부와 행정정보공동이용에 관한 법률로서는「전자정부법」,「행정절차법」,「국가정보화기본법」등이 있으며, 개인정보호호에

완·발전시켜 나가면서 행정정보의 공동활용을 위한 전산시스템의 연계운영 대책 마련에 중점을 두었다. 2001년 1월 전자정부 추진과 관련하여 부처간 이견 조정·점검·평가 기능 등을 담당하기 위하여 민간전문가와 관련부처 차관으로 전자정부특별위원회가 구성·설치되었다. 동 위원회에서는 전자정부 11대 중점사업과 31대 로드맵과제를 선정하여 추진하는 등 전자정부 구축사업에 박차를 가했다. 이들 사업은 현재까지 많은 성과를 거두었으며, 현재도 계속해서 차세대 전자정부의 비전을 제시하며, 전자정부 고도화를 위한 노력을 진행하고 있다(전자정부특별위원회, 전자정부백서 2003, 전자정부특별위원회, 33-39면 참조).

3) 특히 컴퓨터로 데이터베이스화된 개인정보는 그 처리와 이용이 시공을 초월하여 간편하고 신속하게 이루어질 수 있게 되었고, 자동화된 정보처리와 정보파일의 결합을 통하여 여러 기관이 상호 정보교환을 용이하게 할 수 있게 됨에 따라 하나의 행정기관이 보유하고 있는 개인정보를 모든 행정기관이 동시에 활용할 수 있다.

관한 법률로서는「공공기관의 개인정보보호에 관한 법률」과「정보통신망 이용 촉진 및 정보보호에 관한 법률」등이 있다. 그러나 이러한 법률들은 개인정보의 보호 특히, 자기정보관리통제권을 보호하기에는 불충분한 부분이 너무 많고, 그 결과 정보사회에서 개인의 기본권을 충분히 보장하지 못하고 있는 실정이다.

이러한 배경에 따라, 본 연구는 전자정부 구축에 따른 행정정보공동이용에 있어서 개인정보의 공개 및 도용으로 인한 문제점 및 개인식별번호로 인한 기본권 침해의 위험 등을 검토하고, 우리나라 전자정부와 개인정보보호법제에 나타난 자기정보관리통제권 보장과 관련된 문제점을 분석하여 그 해결을 위한 법률적 제도적 개선책과 정책대안을 제시하고자 한다. 특히 이 연구의 결과물로서 행정정보공동이용에서 개인정보보호를 확립할 수 있는「(가칭)행정정보공동이용에 관한 법률(안)」을 제안함으로서 향후 입법 자료로 제시하고자 한다.

제2절 연구의 방법 및 범위

본 연구에서는 전자정부의 행정정보공동이용에 있어서 개인정보보호와 자기정보관리통제권에 관한 국내외 선행연구 자료와 개인정보보호에 관한 국제규범 및 각국의 법제에 대한 법적·제도적 접근방법과 분석적 접근방법·비교법적 접근방법을 사용하고자 한다.

먼저 제2장에서는 전자정부 일반론과 전자정부 구축이 개인에게 미치는 영향을 살펴보고, 전자정부의 법제를 비교법적으로 고찰한 후, 전자정부에서 나타나는 행정정보공동이용에 대한 헌법적 논의를 하고자 한다. 특히 여기서는 우리나라 관련 법제에서 나타난 문제점을 도출하여 개인정보보호의 필요성을 논하고자 한다.

제3장에서는 전자정부 등장에 따른 개인정보 침해 가능성이 증대되고 있으므로 개인정보공동이용을 새로운 기본권 제한으로서 인식한 바탕에서, 개인정보보호에 관한 비교법적 고찰을 통하여 우리에게 주는 시사점을 도출한 후 개인정보보호법제의 개선책을 논하고자 한다.

그리고 제4장에서는 전자정부에서 개인정보보호 문제를 자기 자신에 관한 정보를 스스로 관리·통제할 수 있는 개인의 법적 능력에 주목하여 개

인정보보호의 문제를 바라보고자 한다. 이 분석에서는 개인정보관리통제권을 확보하기 위한 개인정보보호법제의 정비와 개인식별번호제도의 개선방안을 논하고자 한다.

마지막으로 제5장에서는 연구를 요약하여 결론을 도출한 후, 연구의 최종 결과물로서「(가칭)행정정보공동이용에 관한 법률(안)」을 제안하고자 한다.

기본권으로서의 자기정보관리통제권은 공공부문을 구속하는 권리임에는 틀림없지만, 오늘날 민간부문에 있어서도 어떠한 형태로든 효력이 미친다고 할 것이다. 따라서 오늘날 민간부문에 있어서 개인정보보호는 공공부문 못지않은 문제 내지는 어쩌면 공공부문보다 훨씬 더 중요한 문제로서 이해되고 있다. 이러한 측면에서 개인정보의 보호를 위해서는 개인정보침해를 사전적으로 예방하거나 사후적으로 구제하기 위한 법제의 정비와 이에 못지않은 보안 시스템이나 보안 프로그램의 개발과 같은 기술적 차원의 연구개발도 중요하다. 하지만 여기서는 규범적 차원에서 개인정보보호 및 자기정보관리통제권에 대한 법제도적 보호방안에 주안점을 두고 연구를 진행하기로 한다. 따라서 본 연구에서는 규범적 방법에 입각하여 헌법적 근거를 바탕으로 하여 개인정보보호에 관한 현행 법령 및 판례 등을 체계적으로 해석하고 분석하고자 한다.

제2장 전자정부 구축에 대한 헌법적 접근

제1절 서설

1. 전자정부 개설

가. 전자정부의 개념 및 범위

1) 전자정부의 개념

전자정부라는 용어는 미국에서 처음 사용되었는데, 전자은행 서비스(electronic banking) 개념에서 확장된 것이다. 미국에서는 전자정부(electronic government)를 공통의 정보통신기반 위에 하나로 연결된 각종 서비스를 언제, 어디서나, 어떤 방법으로든 제공할 수 있는 정부로 표현하며, 영국에서는 정부가 고객이라고 할 수 있는 일반국민과 기업에게 제공하는 각종 서비스를 전달함에 있어 종래의 전통적인 수단이외에 발전된 정보기술(information technology)을 적용하여 서비스를 확대하고 서비스의 질을 향상시키는 한편 정부행정의 효율성을 높여 나가는 것[4]이라고 한다.

우리나라「전자정부법」제2조 제1호에서도 전자정부란 정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부라고 정의하고 있다. 즉, 전자정부란 정보기술을 기반으로 하여 입법·사법·행정 등 국가업무의 전자적 처리와 유기적 연계로 행정의 효율성과 투명성을 제고하여, 국민과 기업이 원하는 서비스를 언제 어디서나 쉽게 접근하고 이용할 수 있게 하며, 참여민주주의에 대한 국민의 요구에 적극 부응하는 정부[5]를 말한다. 국민은 정보기술을 활용한 전자정부를 통하여 사이버 공간에서 국가권력과 만날 수 있다. 그리고 온라인(on-line)상의 전자정부는 오프라인(off-line) 정부가 담당하는 기능과 역할을 수행하게 된다.[6]

---

4) 행정자치부, 전자정부법의 이해와 해설, 행정자치부, 2007, 4면.
5) 위의 책, 3면.
6) 강경근, "전자정부의 헌법적 과제", 공법연구 제35권 제1호, 한국공법학회, 2006, 122-123면.

전자정부의 목적은 정보기술의 이점을 활용하여 정부의 비효율성과 비민주성을 극복하여 선진행정을 구현하는 데 있으며, 정보 시스템과 인터넷 등 전자적인 수단을 이용하여 행정의 효율성과 투명성을 향상시키고, 국민에게 제공하는 정부의 서비스 품질을 개선하며, 국민의 능동적인 국정참여를 유도할 수 있는 효과적인 수단이 된다. 또 정보통신기술을 활용·확대함으로써 산업발전을 견인할 수 있는 전략적 수단이 될 수도 있다.[7)]

2) 전자정부의 범위

전자정부를 협의로 파악하면 행정서비스의 디지털화, 온라인 네트워크화를 의미하고, 광의로는 행정 및 사회 전체의 민주적 혁신을 뜻한다.[8)] 전자정부의 역할과 범위는 정부(government: G), 기업(business: B), 시민(citizen: C)으로 분류하여 표현될 수 있다. 정부와 시민의 관계(G2C)의 변화는 전자정부를 통해 다양하게 나타날 수 있다. 정부 측에서는 시민지향적인 질 높은 행정서비스 제공이 가능해진다. 즉, 시민 위주의 다양하고 선택의 폭이 넓은 행정정보 서비스를 제공할 수 있게 된다. 동시에 시민의 편에서는 행정에 대한 참여기회의 확대와 의견 반영이 가능해지며 시민 스스로가 필요한 문제해결의 중심에 서는 민주행정을 구현[9)]할 수 있다.

3) 전자정부의 특성

전자정부는 다양한 개념으로 정의되고 있으나 그 공통적인 요소는 정보기술의 이용과 행정업무의 혁신적 능률화, 그리고 대국민서비스의 향상으로 정리할 수 있을 것이다.[10)]

전자정부는 기존 오프라인 서비스에 정보기술을 도입함으로써 정부가 제공하는 다양한 정보에 대한 접근을 지리적·사회적·경제적으로 손쉽게 접근할 수 있는 계기를 마련해준다. 또한 모든 대국민 서비스와 관련된 행정업무를 인터넷을 통하여 전자적으로 처리할 수 있게 됨으로써 기존의

7) 행정안전부·한국정보사회진흥원, 전자정부사업 백서 :2003-2007, 행정안전부, 2008, 20면.
8) 박동진, 국가혁신을 위한 차세대 전자정부 전략, 정보통신정책연구원, 2005, 17면.
9) 전자정부특별위원회, 앞의 주 2), 96면.
10) 김일환, "전자정부와 개인정보보호", 공법연구 제37집 제1호, 한국공법학회, 2008, 343면.

행정업무가 보다 신속하게 제공될 수 있고, 보다 적은 비용으로 향상된 업무를 수행할 수 있게 된다. 그리고 공급자 중심의 행정서비스 제공에서 탈피하여 수요자 즉, 고객지향적 행정서비스를 추구하는 열린 정부가 실현된다.

이처럼 전자정부는 다양한 요소들의 결합으로 성립될 수 있으나, 그 공통적인 개념요소는 정보기술을 이용 또는 활용하여 행정업무의 혁신적인 능률화와 대국민 서비스의 향상이라고 할 수 있다. 또 정보통신기술을 활용하여 고객지향성, 국가정보의 공개성, 유연성, 통합성, 신속성 등을 모색하는데 이것은 산업시대의 관료제와는 다른 특성이 된다.

전자정부의 특성으로 들 수 있는 것은, 첫째, 먼저 정보통신기술에 바탕을 두고 있는 정부라는 점이다. 디지털 혁명과 멀티미디어 네트워크 혁명으로 특징 지워지는 후기 정보시대에 들어서 정보의 개혁과 새로운 정보통신기술의 힘을 통하여 공공서비스 제공비용을 저하시키고 동시에 정부와 국민간의 관계를 개선시킬 것으로 본다.[11]

둘째, 전자정부가 기존 산업사회의 정부형태와 다른 이념적 차이를 보이는 것은 대정부의 고객서비스의 질을 한 차원 높게 개선시키는 고객지향적 정부라는 점이다. 전자정부는 무엇보다 공급자(정부) 중심에서 탈피하여 수요자(국민) 중심의 행정 서비스를 제공하려고 하는 것이다.[12] 이 고객지향적 정부는 정부통신기술을 활용하여 행정업무혁신(BPR) 등을 통하여 작고 생산적·효율적인 정부를 구현하여 고객지향적인 열린 정부의 실현을 목적으로 한다.

셋째, 작지만 효율적인 정부이다. 전자정부의 실현을 통해 납세자의 부담을 덜어주고 행정서비스의 품질을 향상시키려는 것이다. 미국의 국가성과평가위원회(National Performance Review)의 표현을 빌리자면 저비용·고성능의 정부(government that works and costs less)를 창조하는 것이다. 이것은 행정의 전자화를 통하여 행정 서비스를 비용-효과적이며, 신속하고 안전하고 안정적으로 공급함으로써 실현할 수 있다.

넷째, 전자정부는 결과에 책임을 지는 시스템을 활용한다. 전자정부의

---

11) 서순복, "신 공공관리에 관한 보완적 접근 : 정보기술을 활용한 행정개혁", 한국사회와행정연구 제10권 제2호, 서울행정학회, 1999, 74면.

12) 윤영민, "전자정부의 구상과 실천에 관한 비판적 접근", 국가기간 전산망저널 제3권 제3호, 한국전산원, 1999, 6면.

구현은 국민이 정부의 정책과정에 참여할 수 있도록 사이버공간에서 정보공간을 마련하여, 보편적인 접근을 할 수 있어야 하므로, 정부 조직구성원의 민주적인 자세가 확보되어야 할 것이다.

나. 전자정부 추진 현황

1) 국내 전자정부 추진

우리나라에서의 전자정부는 1986년부터 제1차 행정전산망사업이 추진되면서 시작되었다. 1987년부터 주민등록, 부동산, 자동차, 고용, 통관관리, 경제통계를 6개의 전산망기간사업을 우선사업으로 구성하여 이 분야의 중점적 개발을 시작하였는데, 전자정부사업이 조성된 것은 1995년「정보화촉진기본법」이 제정되고 다음 해인 1996년 제1차 정보화촉진기본계획이 수립되면서부터라고 할 수 있다.[13)]

그러나 전자정부사업이 본격적으로 추진된 시기는 2001년 전자정부 11대 사업이 시작된 이후라고 할 수 있다. 이 시기에는 전자정부가 행정개혁과 대국민 서비스 혁신을 위한 전략적 수단이 될 수 있다는 인식이 점차 커지면서 전자정부 로드맵 31대 과제가 2003년부터 추진되었다. 그리고 현재는 이 과제가 종료되고, 2007년 수립된 차세대 전자정부 사업의 검토와 수정을 통해 선정된 전자정부 지원사업 12대 과제가 추진되고 있다.[14)]

한편 현 정부에 들어서는 전자정부 기능 중 정보통신부의 정보화촉진기본계획과 정보화추진위원회의 관리 기능, 개인정보관리정책 기능, 전자서명관리 기능, 정보해소격차 기능 등이 강화되었다. 또한 행정안전부가 자체개혁을 통해 산하 81개 위원회 중 60개를 폐지하는 계획을 발표하면서 기존 정보사업화를 주도했던 정부혁신지방분권회의가 폐지되며, 그 대신에 대통령직속 민관합동위원회인 국가정보화전략위원회와 행정안전부가 중심이 되어 전자정부사업을 비롯한 정보화사업이 전개되고 있다.[15)]

---

13) 현재 정보화촉진 기본계획은 제5차까지 수립되어 있다. 1996년 제1차 정보화촉진기본계획을 시작하여, 제2차 정보화촉진기본계획(Cyber Korea 21), 제3차 정보화촉진기본계획(e-Korea Vision 2006), 제4차 정보화촉진기본계획(U-Korea 기본계획), 제5차 정보화촉진기본계획(국가정보화 기본계획(2008~2012))이 수립되었다: 국회예산정책처, 전자정부 지원사업 평가, 국회예산정책처, 2009, 6면.

14) 위의 책, 5-6면.

현재 우리나라의 전자정부의 위상은 세계적으로도 인정받고 있으며, UN이 제시하고 있는 5단계 전자정부 발전단계 모형의 최종단계(통합처리)를 80% 정도 달성한 것으로 평가받고 있다.[16] 우리나라 전자정부 기반 조성기를 년도 별로 구분하면, 다음 <표 1>과 같다.

<표 1> 우리나라 전자정부 추진경과

년도	구 분	추진 내용	비고
1978	전자정부 태동기	행정전산화 추진	● 부처단위로 단위업무 전산화에 치중
1987-1995	전자정부 초창기	행정전산망 구축	● 주민, 부동산 등 13개 우선업무 추진 ● 단위업무의 전국단위 온라인화 ● 「전산망보급확장과 이용촉진에 관한 법률」(87. 6)
1996-2000	전자정부 기반조성기	정보화촉진	● 초고속 정보통신 기반 구축, 인터넷 활성화 ● 전자정부 종합 실천계획(99.9)
2001-2002	전자정부 본격착수기	전자정부 11대 과제	● 전자민원, 전자조달 등 11대 과제 ● 단위업무간 부분적, 제한적 연계 ● 「전자정부법」 제정(2001. 3)
2003-2007	전자정부 고도화 성숙기	전자정부 로드맵	● 4대 혁신분야, 3대 로드맵 과제 ● 다부처 사업기반으로 연계강화 ● 전자정부법 개정(2007. 1)

*행정자치부, (함께 가는 희망한국 건설을 위한) 차세대 전자정부 추진계획, 행정자치부 2007, 9면 참조 정리.

2) 외국의 전자정부 추진

정보통신기술의 혁명으로 정보화 사회가 진행됨에 따라 세계 각국에서는 정보통신기술을 정부 전체 또는 행정의 전반에 걸쳐 응용하는 전자정부 구상이 태어났다. 1970년대와 1980년대를 거치면서 행정의 각 기관별로 정보 시스템이 구축되기 시작하였는데, 전자정부라는 새로운 개념이 급속히 확산된 것은 민관 쌍방에서 인터넷 이용이 가속하기 시작한 1995년 전후라고 할 수 있다.

15) 류현숙 외, Web 2.0 시대 정부신뢰 제고를 위한 전자정부 추진전략 연구, 한국행정연구원 2008, 86면.
16) 행정자치부, 함께 가는 희망한국 건설을 위한 차세대 전자정부 추진계획, 행정자치부, 2007, 8면.

각국 정부는 부처간 및 부문간의 이해를 초월하여 정부 및 행정부문의 관계를 근본적으로 묻는 새로운 개혁에 착수하였는데, 그 수단으로서 인터넷을 비롯한 정보기술을 이용하게 되었다. 따라서 전자정부는 처음부터 행정개혁과 일체화된 개념이라 할 수 있다.

이후 민간 인터넷을 활용한 각종 서비스가 등장함으로써 네트워크를 통하여 시민 또는 기업이 사용하는 것과 같은 형태로 행정정보를 공개한다는 이른바 정보공개 개념 또는 네트워크를 통한 각종 질 높은 행정 서비스를 제공함으로써 이용자의 편리성[17]과 행정부의 효율성을 동시에 추구하는 전자정부가 전세계적으로 활발히 구축되기 시작하였다. 특히 주요 선진국들에서는 그간의 전자정부의 성과를 기반으로 하여 고객의 가치창출을 위한 서비스와 고도화된 IT기술을 통하여 협업 및 통합·성과관리 등에 초점을 맞추고 있다.[18]

(1) 미국

미국은 1970년대부터 전자정부 구현의 필요성을 느끼고 있었고, 간헐적인 법제정이나 개정을 통해 전자정부 구축을 위한 방향으로 나아가고 있었다고 볼 수 있다. 1980년대 들어와서 미국은 4가지 목적(행정기관간 업무연계, 기업 및 시민관련 정부기관 내 상호운영성 확립, 소프트웨어 및 장치의 보편화, 행정비용의 절감)하에 대규모 아키텍처 사업을 추진해오고 있었지만,[19] 전자정부개념을 본격적으로 행정에 도입하기 시작한것은 클린턴 행정부에 의한 체계적인 법제정이나 행정부 주도의 프로젝트들에 의해 가속화되고 본격화된 것이라 할 수 있다.[20]

이후 미국의 전자정부는 2001년까지 범국가적 전략 없이 부처단위로 정보화를 추진한 결과, 투자 대비 생산성 및 대국민 서비스 개선이 저조한 것으로 평가됨에 따라, 2002년부터 대통령 관리 아젠다(PMA: President Management Agenda)에 포함되어 추진되고 있다. 미국의 전자정부전략(e-Government Strategy)은 부처별 운영과 정보기술에 대한 투자를 연계

17) 한국정보사회진흥원, 전자정부법 개정방안 연구, 한국정보사회진흥원, 행정안전부, 2008, 32면.
18) 류현숙 외, 앞의 책, 86면.
19) 최향미, “전자정부 해외 동향 : 해외 주요국의 범정부EA 성숙도 비교연구”, 전자정부 포커스 제2권, 2008, 23면.
20) 임지봉, 미국의 전자정부법제, 한국법제연구원, 2001, 11면.

시키기 위한 범국가적 이니시어티브로서, 시민과 기업에 대한 대민서비스의 품질을 향상시키고 시스템 및 자원의 중복을 배제해 나가는데 목표가 있다.

2002년 전자정부 수립 이후, 정부혁신과 예산을 총괄·조정하는 예산관리처(OMB: Office of Management and Budget) 주관으로 예산관리처 전자정부국, 총무처, 최고정보책임자협의회(CIOC: Chief Information Office Council) 등을 중심으로 전자정부를 추진하고 있다. 전자정부법에 따라 2003년부터 조성된 전자정부기금(e-Government fund)은 2009년 회계연도에는 710억 달러로(2008년 대비 3.8% 상승) 추정되고 있다.

미국의 전자정부사업은 크게 4분야 24개 전자정부사업으로 추진되고 있다. 이는 2001년 가을 예산관리처 주관으로 연방정부가 참여하여 선정하였다. 전자정부사업의 4분야는 정부 대 시민(G2C: Government to Citizen), 정부 대 기업(G2B: Government to Business), 정부 대 정부(G2G: Government to Government), 내부 효율성 및 효과성(Internal Efficiency and Effectiveness)이며, 전자인증(E-Authentication)이 별도 분야로 책정되어 전체 24개 사업에 대한 안전성을 보장하는 사업으로 추진되고 있다.[21] 또 미국 연방정부 관리 예산처(OMB)는 연방 정부가 추진해 온 전자정부 성과보고서에서 미연방정부는 연간 약 710억 달러를 투자하여 세계 최고 수준의 정보·서비스 사용자인 동시에 관리자가 됨으로써, 모든 미국 시민을 위한 전자정부 서비스 제공을 위해 노력하고 있다. 그리고 2008년 헬스 IT 프로그램에서 3가지[22] 아키텍처를 활용해서, OMB는 회계연도 2009에 전체 기관의 분산된 494개의 투자 프로그램(54억 달러)을 효과적으로 정렬하여 11개의 세그먼트 아키텍처로 구성하였으며, OMB가 도입·사용해 온 데이터참조모델(DRM)은 정부기관간 상호운용성과 정보공유의 핵심 툴로 이를 활용한 국가정보교환모델(NIEM) 개발에 박차를 가했다. 또한 OMB는 지난 7년간 보안관리, 정보프라이버시, IT인력확보 등의 성과를 제시하면서 향후 전자정부의 또 다른 발전 가능성을 확신[23]하고 있다고 했다.

---

21) 류현숙 외, 앞의 책, 88-89면.

22) 엔터프라이즈 아키텍처(Enterprise Architecture) : 전사적 아키텍처, 세그먼트 아키텍처(Segment Architecture) : 영역별 아키텍처, 솔루션 아키텍처(Solution Architecture) : 시스템 아키텍처.

23) Expanding E-Government : Achieving Results for the American People(2009.1.); NIA,

(2) 영국

영국의 전자정부는 1990년대부터 내각사무처와 수상실의 책임하에 전자정부국(eGU : e-Government Unit)이 실질적인 정책과 사업을 수행해왔으며, 현재 정부개혁 전략과 관련해서는 장관급의 최상위 추진조직부터 실무, 기술차원의 체계적인 추진체계를 구성하여 추진 중이다.

2000년 4월 정부의 현대화 정책과 함께 발표한 전자정부전략(e-Government Strategy)을 시작으로 정부 공공서비스의 온라인화 및 기반의 구축을 중심으로 시작되었다.[24] 2005년 3월에는 중앙정부 및 지방정부 관계자 30명으로 구성한 최고정보책임자협의회(CIOC: Chief Information Office Council)가 설치되었다. 이 협의회의 역할은 전자정부 사업의 성공률을 높이는 자문을 제공하는 것이다. 같은 해 11월에는 협의회의 주도 아래 새로운 전자정부 추진전략으로써 '기술기반의 정부혁신전략(Transformational Government: Enabled by Technology)'를 발표하였으며, 세부시행전략으로는 ① 사용자 중심의 서비스(user-centric services), ② 자원 및 서비스 공유(shared services), ③ 정부 전문성 확대(professionalism) 등을 제시하였다.[25]

이 '기술기반의 정부혁신전략'을 통해 영국은 2007~2011까지 최우선적으로 공공 서비스에 대한 기술투자 및 업무혁신을 통해 국민과 기업에 대한 공공 서비스를 확대하여 제공하려고 하고 있으며, 2011년 이후에는 기술기반의 공공 서비스 제공에 더욱 큰 변화가 야기될 것으로 예측하고 이에 대응하여 새로운 기회를 제공할 것을 밝히고 있다.[26] 그리고 2007부터 2011년까지 공공서비스 전달의 참여 주체를 시민 또는 기업 중심으로 변모시키려는 것과 공유 서비스 프레임워크에 대한 지원 강화를 위해 투자하여 급진적인 변화에 따르는 환경에 대비할 계획을 세워 추진해오고 있다.[27]

IT Issues Weekly, 한국정보사회진흥원, 2009, 2-3면.

24) 한국정보사회진흥원 전자정부기획팀, "전자정부 해외 동향 : 영국의 전자정부 현황", 전자정부 포커스 제5권, 한국정보사회진흥원, 2007, 36면.

25) 류현숙 외, 앞의 책, 93면.

26) EC IDABC(2008), eGovernment in United Kingdom (v.9). http://epractice.eu 2009.12.23 방문.

27) 한국정보사회진흥원 전자정부기획팀, 앞의 주 24), 39면.

(3) 캐나다

캐나다 전자정부는 1999년 10월 정부 온라인 전략을 공식적으로 발표하고, 34개의 정부부처에서 온라인으로 전환함으로써 전자정부 서비스를 시작하였다. 이 전략은 캐나다를 전세계에서 가장 네트워크화 된 국가로 만들기 위한 국가정보화계획으로서, 산업부가 주도하고 공공과 민간의 파트너십을 기반으로 추진되었으며, 6개의 핵심전략을 골자로 하였다. 또한 전략의 이행을 위해 정보격차 문제가 발생할 수 있음을 고려하여 정보통신 인프라 구축에 역점을 두었다.

2008년 8월에는 전자정부의 추진방향 및 전략을 제시한 '온라인 정부계획(GOL: Government On-Line)'을 발표하였다. 이 계획은 가장 많이 이용되는 정부 서비스 130개를 2005년까지 온라인으로 제공하는 것을 목표로 하였으며, 서비스 접근성 향상, 서비스 품질 및 응답성 향상, 온라인 업무처리 신뢰성 구축이라는 3대 목표를 기반으로 일관성 있게 추진되었다.[28)]

국가재정위원회사무국 내에 조직된 최고정보책임자 지부(CIO branches)는 2003년까지 정부 차원의 기획조정, 프레임워크 제공 및 진전사항 검토 등 기능적인 측면에서 주도적인 역할을 담당하였으나, 2003년 이후 상당부분의 기능이 공공사업과 행정 서비스국(Public Works and Government Services Canada)으로 이관되었다. 2000년 설립된 정부온라인 사업 추진실(GLO Initiative Office)은 참여부처들의 전자정부 추진을 위한 예산 승인, 위험 관리 및 추진사항 등을 감독 및 지원하는 기능을 한다.[29)] 그리고 캐나다 공식 전자정부 사이트에서는 사이트 이용자 누구나 개인 계정을 만들 수 있으며, 로그인을 위한 아이디(epass)는 20여개의 정부 사이트에서 통합적으로 이용이 가능하다. 또 제공되는 컨텐츠는 카테고리별, 알파벳순, 키워드 순으로 분류되며, 사용자 누구나 자신의 필요에 맞게 재구성이 가능하고 신규 컨텐츠 또는 카테고리 생성시 이메일을 통해 사용자에게 알려주는 기능도 제공하고 있다.[30)]

---

28) 행정자치부, 2006 전자정부사업 연차보고서, 행정자치부, 2006, 349-351면.
29) 류현숙 외, 앞의 책, 90-91면.
30) 박현진・박선주, "전자정부 해외 동향 : 주요 선진국가의 전자정부 '개인화 서비스' 현황", 전자정부 포커스 제3권, 한국정보사회진흥원, 2008, 73면.

(4) 일본

1990년대 초반 일본의 경제는 거품 호황이 붕괴되기 시작하면서 위기에 직면하여 경기침체가 지속되며 연평균 성장률이 2%에도 훨씬 못 미치는 최악의 상황을 맞이하였고, 이러한 상황은 거의 10여 년 동안 회복할 기미가 보이지 않았다. 이에 일본 정부는 2000년대에 들어와서 침체된 경제의 새로운 원동력으로 IT 기술 중심의 국가 개혁을 추구하는 이른바 'IT 혁명'을 추진하게 되었다. 일본 정부는 급변하는 시대의 미래 국가 경영 방향을 IT 기반의 구조개혁에 초점을 맞추고 산업육성 및 경제 활성화를 위한 국가 종합전략을 채택하여「고도정보통신 네트워크 사회형성 기본법(IT기본법)」을 제정하고, 'e-japan 전략' 등을 추진하면서 정보화 사회를 위한 터전을 마련, 세계 최고수준의 정보통신 고도화를 달성하고 국민의 정보 활용능력의 향상 및 전문적 인재의 교육 양성을 목표로 추진하고 있다.[31)]

한편, 일본의 전자정부는 1995년부터 시행되어 온 '행정정보화 추진 기본계획'으로부터 시작되었으며, 2000년 내각에 고도정보통신 네트워크사회 추진전략본부(IT 전략본부)를 설치하고, IT 기본전략(基本戰略)을 시행함으로써 본격화되었다. IT기본전략에서는 5년 내에 세계 최첨단의 IT국가 실현을 목표로 하여 중점정책 분야로서 ① 초고속 네트워크 인프라 정비 및 경쟁 정책, ② 전자상거래 원칙과 새로운 환경정비, ③ 전자정부의 실현, ④ 인재육성 강화 등을 제시하였다. 일본은 IT전략을 통해 전자정부를 행정내부나 행정과 국민·사업자간에 이루어지고 있는 업무를 온라인화하여 정보 네트워크를 이용해 부처 횡단적, 전국가적 정보를 공유·활용하는 새로운 행정을 실현하는 것으로 정의하면서, IT화를 향한 중장기적 투자를 실시함과 동시에 업무개혁, 부처간 중복업무의 정리 및 제도 등의 재검토 등을 통해 행정의 간소화 및 효율화, 국민·사업자의 부담 경감 등을 실현하는 것을 목표로 하였다.

2003년에는 전자정부구축계획(電子政府構築計劃)을 발표하였으며, 각 부처별로 정보화총괄책임자(CIO) 연락회의를 설치하였다. 2006년에는 'IT신개혁전략(新改革戰略)이 발표되었는데, 이 계획에서는 초기 전자정부의 목

31) 김주원, "일본 전자정부 추진동향 및 시사점 : 행정정보화를 넘어 국가경쟁력 강화로", NIA IT 이슈 & 트렌트 제8호, 한국정보사회진흥원, 2008, 3면.

표가 제대로 달성되지 못했다고 평가하였고, 그 세부시행계획으로서 업무·시스템 최적화 계획, 온라인 이용 촉진을 위한 행동 계획 등을 통해 신뢰성 및 안전성이 확보된 전자정부를 실현할 것을 천명하고 있으며, 이와 함께 전자정부 사업에 대한 보다 체계적인 평가와 관리의 필요성을 피력하였다.

2007년에는 전자정부구축계획의 개정을 통해 2010년까지의 전자정부 사업 추진계획을 제시하였다. 이 계획에서는 비용 대비 효과의 극대화를 위해 PDCA(Plan, Do, Check, Act) 사이클에 의한 공정관리체제를 확립하고, ① 신청·신고 등 수속의 온라인화에 의한 편리성 및 서비스 향상, ② 업무·시스템 최적화를 통한 행정운영의 간소화 및 효율화, ③ 정부 전체적으로 업무·시스템의 공통화 등을 통한 한층 업그레이드된 최적화, ④ 정보시스템의 고도화 및 안전성·신뢰성 확보, ⑤ 원스톱 행정서비스를 위한 제2세대 전자행정 서비스 기반의 표준모델 구축 등을 2010년까지 달성할 것을 목표로 제시하였다.[32]

또한 일본 전자정부의 차세대 전자행정서비스의 목표는 첫째, 이용자 입장에서의 서비스 제공 둘째, 행정사무의 최적화 추진 셋째, 기업활동의 활성화 넷째, 국민과 행정의 신뢰 강화라는 목표를 설정하고, 국민중심의 궁극적인 전자사회의 실현을 통해 전자정부 서비스의 질적 향상과 효율화로 신뢰를 강화한다. 그리고 행정서비스, 행정관리의 개인정보 접근 이력, 업무 프로세스, 프로젝트의 진척상황 등을 가시화하고 투명성을 확보함으로써 국민중심의 전자행정 서비스의 질을 높이는 전자사회 실현을 기대한다.[33]

(5) 스웨덴

스웨덴의 전자정부는 1997년 정부 온라인화(Government eLink; GeL) 프로젝트로부터 시작되었다. 이 프로젝트는 정부 부처간 또는 정부와 국민간의 안전한 정보교환을 위한 준비 작업이었다. 1999년에는 정부전산화의 내용을 포함한 국가 IT전략(An Information Society for all)을 발표하였으며, 2000년에는 정부 부처간 협의체인 '공공 e포럼(현재의 Verva)'을

32) 류현숙 외, 앞의 책, 91면.
33) 김주원, 앞의 책 22면.

설치하였다. 2005년에는 스웨덴을 세계적 수준의 정보국가로 진입시키기 위한 IT전략(From an IT policy for society to a policy for an information society)을 발표하였으며, 유럽 국가 중 두 번째로 생체인식 전자여권 제도를 도입하였다. 또한 2006년에는 스웨덴의 범국가적 전자정부 사업의 추진을 주도하는 스웨덴 정부혁신협의회(Verva)를 설치하고, 공공 e포럼의 기능을 대체시켰다.

그리고 2008년 1월에는 새로운 전자정부 추진계획인 '현대적 전자정부 구현을 위한 액션플랜(Action Plan for a modern eGovernment)'를 발표하였다. 이 계획을 통해 스웨덴은 2010년까지 선별적으로 추진할 전자정부 정책을 수립·발표하였으며, 이를 통해 세계 최고의 전자정부 추진국으로서의 위치를 탈환하는 것을 목표로 하고 있다. 구체적인 시행계획으로는 ① 전자식별(e-Identification)을 통한 통신 및 정보교환의 안전성 및 효율성 구현, ② 정보 접근성의 확대, ③ IT 표준 확보 등이다.

스웨덴의 전자정부는 재경부(ministry of finance) 내의 지방정부 및 재정국(local government and financial market)의 주도 아래 추진되고 있다. 이 과정에서 정부혁신을 위한 전문가들로 구성된 정부혁신협의회는 자문위원회로서의 역할을 하며, 지방정부별 전자정부 추진위원회가 실질적으로 전자정부 사업을 시행하고 있다.[34]

한편, 스웨덴은 'UN의 전자정부 조사 2008'에서 전자정부 준비지수 부문에서 1위를 하였으나 범정부(NEA)는 초기단계로 2006년부터 정부 기관간 상호 운영성 및 서비스 질적 제고에 초점을 두기 시작했다. 그리고 행정개발부(Verva: Swedish Administrative Development Agency)는 공공행정서비스의 질적 변화를 위해 상호운영성 관련 아키텍처 및 프레임워크 타당성 조사를 수행하였으나 사업추진은 아직 미진하며, 정부 분권적 성향에 따라 각 행정기관이 개별적으로 전자정부를 추진하고 있고, 전자정부의 조정역할이 부재한 실정이다.[35]

(6) 싱가포르

싱가포르 전자정부는 1980년대부터 강력한 정부주도의 정책추진과 민간

34) 류현숙 외, 앞의 책, 96면.
35) 최향미, 앞의 책, 21면.

과의 공동투자 노력을 기반으로 아시아권에서는 가장 먼저 시작되었다. 1980년에는 정부전산화사업(Civil Service Computerization Programme: 1980~1999)을 추진하여 업무 자동화 및 문서업무 감축을 통한 부처 및 기관내부 업무처리의 효율성 향상을 도모하였다. 그리고 2000년에 들어서는 제1차 전자정부계획(1st eGovernment Action Plan(eGAP I): 2000~2003)과 제2차 전자정부계획(eGAP Ⅱ): 2003~2006)을 추진하였다.

2006년에는 이용자를 만족시키고 IT를 이용하여 전국민을 연결한다는 목표로 'iGov2020'이라는 새로운 마스터플랜과 정보통신 10개년 계획(iN2015)을 발표하였다. iGov2020은 지난 2003년부터 추진해온 제2차 전자정부계획을 발전시킨 것이며, iN2015는 2015년까지 IT부문의 역량강화를 위해 발표한 국가정보화계획이다. iGov2010의 추진목표는 ① 이용자(국민 및 일반사업자) 10명 중 8명 이상이 전자정부서비스에 만족하도록 할 것, ② 이용자 10명 중 9명 이상이 전자정부서비스를 다른 사람에게도 이용하도록 권장할 수 있도록 할 것, ③ 이용자 10명 중 8명 이상이 정부정책 및 이니시어티브에 기반하여 제공되는 정보의 투명성과 유용성에 만족할 수 있도록 할 것 등이다.

싱가포르의 IT산업과 전자정부 정책은 정보통신문화부(MICA: Ministry of Information, Communication and the Art)와 정보화진흥원(IDA: Information Development Authority)이 주관하여 추진하고 있다. 특히 정보화진흥원은 정부의 최고정보책임자로서 국가 정보화, 전자정부 정책 기획 및 정보화 촉진과 통신규제 기능의 효과적 통합을 위한 규제업무를 담당하고 있다.

2. 전자정부 구축의 성과와 미래

가. 전자정부의 성과

우리나라는 지난 수년간 '세계 최고 수준의 열린 전자정부' 구현이라는 비전하에 전자정부 로드맵을 수립하고, 중점과제를 선정하여 범정부적으로 추진한 결과 행정기관 간 경계 없는 온라인 서비스가 가능해져서 안방 민원시대를 열었고, 다양한 기업지원 서비스를 통해 기업활동에 우호적인

환경도 조성하였다. 무엇보다 행정업무의 투명성과 효율성을 높여 정부기관에 대한 국민의 신뢰성을 제고하는 등 다양한 성과를 이루어내었다.[36]

또한 우리의 전자정부는 국제사회에서도 높은 평가를 받고 있다. 앞서 기술한 바와 같이 우리나라는 전자정부 분야에서 세계적인 선도국가로서 평가받고 있다.

그 동안 정부는 지속가능한 정부혁신 인프라를 조성하여 행정의 투명성과 협업을 위한 온-나라 시스템(On-nara BPS)을 개발하여 전 부처 및 시・도에 확산하고, 2007년 회계연도부터 성과기반의 선진 회계제도(복식부기, 프로그램 예산 등)를 도입해 실시간 통합재정관리체계(디지털 예산회계)를 개통하였다. 그리고 국민에게 다가가는 전자정부 서비스 확대를 위하여 발급빈도가 높은 40여종의 행정정보를 행정・공공・금융기관간에 공유하여 민원인이 제출하는 구비서류를 대폭 감축하여 민원행정을 개선하였으며, 기업활동의 도우미로서 정부서비스 지원체계 정비로 기업행정의 단일창구(G4B)를 구축하여 창업부터 폐업까지 산업 활동 전반에 대한 행정지원체계의 기반을 마련하였다. 또 전자정부의 성공적 구현을 위한 기술적・제도적 기반을 강화하여 정부자원의 효율적 관리를 위해 2개의 정부통합전산센터 구축과 48개 부처 시스템의 성공적 이전 등 통합운영체계를 마련하였다. 이러한 성과를 토대로 부처별・단위업무별 정보화는 세계 일류 브랜드로 발돋움 하였다. 그리고 전자조달 '나라장터'에서는 약 44조원의 계약이 전자입찰로 진행되고 매일 18만 명이 방문하는 세계적 브랜드(전자입찰률 92.3%)로 되었다.[37]

그러나 이와 동시에 그 동안 부처 간, 기관간의 상이한 기술적용이나 시스템의 호완성이 미흡하거나 정보의 공유가 잘 이루어지지 않아 업무 효율성이 생각만큼 진전되지 않았으며, 이에 따른 국민들의 불편도 나타나게 됨으로써 만족도도 기대만큼 향상되지 않았다.[38] 특히 문제가 되는 것은 정보보안, 표준화 등 전자정부의 인프라가 취약하며, 개인정보보호에 대하여는 성과보다는 피해의 목소리가 더 높다고 할 것이다.

---

36) 행정안전부・한국정보사회진흥원, 앞의 주 7), 1면.
37) 행정자치부, 앞의 주16), 11-15면.
38) 류현숙 외, 앞의 책, 52-53면.

나. 전자정부의 미래와 기대효과

전자정부는 국민과 함께하는 세계 최고 수준의 디지털 정부라는 미래의 비전과 목표를 세워 수요자 중심의 맞춤형 서비스 제공, 시스템에 의한 정부혁신 가속화, 사회안전 실현을 위한 예방 대응체계 강화, 지속가능한 전자정부 발전기반 마련 등을 추구하였다. 또 전자정부의 비전과 목표를 달성하기 위하여 거버넌스형 추진체계 구축, 프로세스 혁신 및 제도정비, 성과관리 체계강화, 전자정부 인적역량 강화, 글로벌 리더십 강화 등의 전략을 수립하여 추진 중에 있다.[39]

전자정부 로드맵에서 제시된 전자정부 비전은 '세계 최고 수준의 열린 전자정부 구현'이다. '세계 최고 수준'이란 최근의 국가정보화 성과를 바탕으로 전자정부를 세계 최고 수준으로 성숙시키는 것을 의미한다. 그리고 '열린 전자정부'란 정부운영의 투명성을 바탕으로 국민의 참여를 활성화하는 것을 의미한다. 특히 투명성을 강조함으로써 정부의 정책 의도, 내용, 과정 등에 대한 정보를 충분히 공개하여 국민이 잘 인식하도록 하고, 정부와 국민 사이에 정보 비대칭이 없는 상태를 구현하고 이를 통하여 국민의 알 권리와 정보 접근성, 인력과 행정·재정 등 자원의 효율적 배분, 부패방지를 통한 깨끗하고 신뢰받는 행정을 촉진하는데 그 목표를 두고 있다.[40]

이러한 전자정부의 실현으로 인한 전자정부의 변화된 모습을 기대해 보면, ① 국민이 즐겨 찾는 서비스, ② 기업에게는 기업경쟁의 도우미가 되고, ③ 공무원은 업무 시간이 즐겁고, ④ 외국의 정부가 벤치마킹 하고 싶은 대상이 되는 것이다. 또 공유된 서비스로 부처간 장벽이 없는 협업 서비스, 온-나라 중심의 정부업무 자동화와 유비쿼터스 서비스를 통해 휴대단말기를 통한 다양한 서비스 채널 및 개인맞춤형의 지능화된 서비스를 제공할 수 있게 된다. 사회적 서비스로는 사용자인 국민 중심 서비스와 지자체와 연계한 통합서비스[41]로 정치·경제·사회·문화 등 모든 면에서 세계 최고의 전자정부가 기대된다.

---

39) 행정자치부, 앞의 주 16), 24면.
40) 행정안전부·한국정보사회진흥원, 앞의 주 7), 24면.
41) 행정자치부, 앞의 책, 29면.

3. 전자정부 구축이 개인에게 미치는 영향

가. 전자정부와 정보화의 역기능

전술한 바와 같이 전자정부 구축이 앞으로 우리에게 긍정적인 측면에서 많은 영향을 미칠 것으로 기대된다. 그리고 놀라운 정보사회의 발전으로 인하여 새롭게 등장한 전자정부는 정보통신기술을 기반으로 하여 정부업무의 전자적 처리와 유기적 연계로 행정의 효율성과 투명성을 제고하고, 국민과 기업이 원하는 정보와 서비스를 언제 어디서나 쉽게 접근하고 이용할 수 있도록 하는 것을 목표로 한다. 그런데 이러한 전자정부의 핵심적 내용이 되는 새로운 행정 시스템은 지금까지의 행정 시스템과는 전혀 다르다. 왜냐하면 새로운 행정 시스템에서는 서류전달이 아니라 컴퓨터 전산망의 연결을 통하여 정보교환이 행해지고 있기 때문에 국가기관 상호간에 업무와 과제를 구분하거나 특별히 정보협조를 구할 필요성이 없어지기 때문이다. 정보사회에서 행정조직이 발전된 현대 정보기술을 이용할 때 나타나는 장점은 무엇보다도 한 기관에서 다른 기관으로 '막히지 않는 정보의 흐름'을 확보하는 것이며, 이를 통하여 국가행정의 많은 절차들이 투명해지고, 효율적으로 국민에게 봉사할 수 있게 된다. 즉 이러한 정보통신기술은 무엇보다도 비용 절감, 신속한 결정 보장, 행정절차의 합리화에 기여하지만 이것이 동시에 개인정보의 침해 또는 정보자기결정권의 침해로 연결될 수 있다는 데에 결정적인 문제점이 있다.[42]

정보사회에서 중앙정보은행이 개인마다 고유번호를 부여한 상태에서 이들에 관한 각종 자료를 통합하여 수집·처리한다면, 이것이 바로 전산망 연결을 통하여 개인정보의 검색과 통합을 할 수 있다. 그렇다면 해커와 같은 외부인이 전산망에 침투하여 개인의 사생활을 침해할 수 있지만, 공무원에 의한 정보유출이나 전혀 다른 과제를 수행하는 국가기관이 법적인 통제 없이 개인정보를 함부로 검색·처리할 때 나타나는 사생활의 침해가 더 심각할 수도 있다.[43]. 그리고 공공부문에서 국민의 동의 없이 국가가 임의로 수집·보유한 개인정보를 공동이용할 때 개인의 인격에 심각한 타

42) 김일환, "민주, 법치국가의 발전과 사회통합", 2008 한국공법학회[공동]주최 국제학술대회, 한국법제연구원, 2008, 505면.

43) 김일환, "정보사회에서 개인식별번호의 수집 및 이용에 관한 헌법적 고찰", 성균관법학 제17권 제1호, 성균관대학교 비교법학연구소, 2005, 215면.

격을 가하는 역기능도 부인할 수 없을 것이다.

나. 개인정보보호 현황

우리나라의 최대의 개인정보 수집·보유자는 아마도 정부일 것이다. 우리나라의 개인정보보호 체계는 공공부문 개인정보보호와 민간부문 개인정보보호로 나뉘어 그 법적 근거 및 추진체계를 달리하고 있다. 공공부문 개인정보보호는「공공기관의 개인정보보호에 관한 법률」에 의거하여 공공기관이 보유하고 있는 개인정보를 관리하며, 민간부문 개인정보보호의 경우는「정보통신망 이용촉진 및 개인정보보호 등에 관한 법률」에 근거하여 중요 개인정보에 대한 보호가 이루어진다.

공공기관에서 수집·처리되는 개인정보보호를 위하여「공공기관의 개인정보보호에 관한 법률」에서는 공공부문의 개인정보보호 체계를 구성하고 있다. 이 법에 의하면 국무총리 소속하에 행정안전부장관을 위원장으로 하여 공공기관개인정보보호심의위원회를 설치하며, 이 위원회는 개인정보보호에 관한 정책 및 제도 개선, 정보처리의 이용 및 제공에 대한 공공기관간의 의견조정 등 공공기관의 개인정보보호에 관한 전반적인 사항을 심의한다.

민간부문에 있어서의 개인정보보호에 관한 일반법으로는「정보통신망 이용촉진 및 개인정보보호 등에 관한 법률」이 있으며,「신용정보의 이용 및 보호에 관한 법률」,「통신비밀보호법」,「정보통신기반 보호법」,「금융실명거래 및 비밀보장에 관한 법률」등에서도 개인정보보호에 관한 규정이 있다.[44]

다. 개인정보 침해 유형 및 현황

전자정부가 구축되면서 국민들은 한 번의 클릭으로 민원서류를 신청·발급받을 수 있는 전자민원시대가 되었다. 민간에 있어서도 인터넷을 통하여 안방에서 쇼핑도 할 수 있다. 하지만 이러한 편리성과 함께 고려해야 할 것은 어떻게 개인정보를 안전하게 보호할 수 있을 것인가의 문제이

44) 국가정보원, 2009 국가정보보호백서, 국가정보원, 2009, 14-15면.

다.

지난 2008년 2월 국내 최대 인터넷 오픈 마켓인 A업체가 중국 해커로부터 공격을 받아 1천만 명이 넘는 고객정보가 유출되는 사고가 발생하였다. 이어 7월에도 인터넷 포털 D업체에서 55만 명의 이메일 정보가 새어나갔고, 9월에는 1천 1백만 건에 달하는 L정유회사 고객 정보가 내부 직원에 의해 유출되는 사고가 잇따랐다. 이로 인해 개인정보에 대한 보안관리 문제가 전 국민의 관심사로 떠올랐다.[45)]

침해 유형별은 신용정보와 같은 정보통신망법 적용 대상 이외에 개인정보 침해, 주민등록번호 등 타인의 정보의 훼손·침해·도용, 기술적 조치 미비로 인한 누출, 이용자 동의 없는 개인정보 수집 등을 들 수 있다.

이와 같은 개인정보침해가 급증하는 것은 날로 더 발전해가는 정보통신기술과 전자정부 구축으로 인한 행정정보의 공동이용에 큰 원인이 있다고 생각할 수 있다. 따라서 전자정부의 성공은 개인정보가 오·남용되지 않고 해킹이나 유출 등의 위험으로부터 안전하다는 신뢰를 줄 수 있느냐에 달려 있다고 할 수 있다.

제2절 전자정부의 규범적 고찰

1. 전자정부 구현의 취지와 기본이념

정부는 21세기 지식정보화시대를 맞이하여 정보기술과 정부의 업무처리 혁신을 결합하여 정부경쟁력의 향상과 대민서비스의 개선이라는 전자정부의 비전 구현을 뒷받침하기 위해「전자정부법」을 제정하였다.[46)] 이 법은 행정업무의 전자적 처리를 위한 기본원칙·절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것을 목적으로 하고 있다.

또한 급변하는 정보화시대에 전자정부가 추구하는 비전과 목표는 산업

45) 위의 책, 21면.
46) 행정자치부, 2007 전자정부법의 이해와 해설, 2008, 7면.

사회에서 오랫동안 불친절·고비용의 행정서비스를 받아온 국민에게 정보통신기술의 장점을 충분히 활용하여 보다 적은 비용으로 편리한 행정서비스를 최대한 제공하려는 고객지향적인 목표를 추구하고 있는데, 이것이 전자정부의 구현 취지가 된다.

정보통신은 인간의 사회활동에서 가장 큰 제약요인인 시간적·공간적 한계를 극복하는 데 결정적으로 기여하는 기술이다. 컴퓨터와 통신망의 발전은 누구나, 언제나, 어디서나 정보자원을 교환할 수 있도록 해준다. 따라서 세계화·시장화·민주화 등 거대 물결에 적응하고 생존하기 위해 이러한 정보통신기술이 지니는 장점을 적극 활용하여 기업의 생산성은 물론, 국민에 대한 행정서비스의 효율성과 투명성을 제고[47]시키는 것이 전자정부구현의 이념이라고 할 수 있다. 하지만 전자정부의 목표는 결코 효율성과 생산성 제고에만 국한되지는 않는다. 전자정부가 태동하게 된 근본적인 배경이 정부가 국민의 신뢰를 상실해 가고 있다는 위기의식이었던 만큼 전자정부는 정부에 대한 국민의 만족도를 높이는 것을 궁극적인 목표로 삼는다.[48]

2. 전자정부의 법적 근거

가. 헌법

전자정부의 구현은 헌법적으로도 여러 가지 논의를 불러오고 있다. 우선 통치구조와 관련하여 직접민주주의 가능성을 제시함으로써 전통적인 대의제의 원리에 변화와 도전을 요구하고 있으며, 실질적인 법치주의 구현에도 이바지하는 정부로 자리 잡게 된다.[49] 이와 같이 전자정부가 정치적 지배의 성격을 변화시키고 있다. 현행 헌법은 입헌주의를 지배의 기본이념으로 채택하고 있다. 입헌주의란 주권자인 국민의 총의를 바탕으로 국가권력의 범위와 한계를 헌법에 규정하고 국가권력의 작용이 국민의 자

47) 전자정부특별위원회, 앞의 주 2), 31면.
48) 정보통신부, 전자정부사업이 지방자치단체 국제화사업에 미치는 영향에 관한 분석, 정보통신부, 2002, 28-29면.
49) 미래사회연구포럼, 개인의 사생활, 국가적 감시, 그리고 규범, 미래사회연구포럼, 2007, 109면.

유와 권리를 최대한 보장하는 방향으로 이루어져야 한다는 원리이다. 입헌주의는 공동체의 정치적 지배가 민주주의 원리에 의해 이루어지도록 요구한다.

우리 헌법도 제1조에서 우리의 국가형태가 민주공화국임을 천명하는 한편, 정치공동체의 주권이 국민에게 있고 모든 지배권력의 근원이 국민임을 선언하고 있다.[50]

이러한 점에서「전자정부법」제2장에서 전자정부의 운영 및 구현원칙으로서 전자적 처리의 원칙, 행정정보공개의 원칙, 국민 편익 중심의 원칙, 업무혁신 선행의 원칙, 전자적 처리의 원칙, 행정기관 확인의 원칙, 행정정보공동이용의 원칙, 개인정보보호의 원칙, 소프트웨어 중복개발방지의 원칙, 기술개발 및 운영외주의 원칙 등을 정하고 있다. 이것은 전자정부가 사이버 공간에 구축된 정부이지만 그 역시 실재하는 또 하나의 현실이라는 것을 의미하고 있다. 따라서 전자정부에 대해서도 역시 하나의 구획된 세계로서 존재하여야 할 당위성을 부여하지 않으면 안된다. 그것은 우리 헌법의 기본원리인 민주주주와 법치주의의 헌법원리로부터 나오는 원칙과 질서라고 하겠다.

이러한 관점에서「전자정부법」에서 말하는 전자정부의 구현 및 운영원칙 중 국민 편익 중심의 원칙, 행정기관 확인의 원칙 등은 국민주권원리를 규정하고 있는 헌법 제1조 제2항에서 그 근거를 구할 수 있다. 따라서 전자정부는 국민주권주의를 기초로 하는 민주주의 헌법 원리에 합치되어야 한다. 이들 원칙이 비교적 실세계의 국민주권주의를 전자정부 운영의 원칙으로 가감 없이 규정한 것이라면, 이를 사이버 공간에 적합하게 변용한 것이 업무혁신 선행의 원칙, 전자적 처리의 원칙, 소프트웨어 중복개발방지의 원칙, 기술개발 및 운영외주의 원칙 등이라 할 수 있다.[51]

나. 법률

1)「전자정부법」

---

50) 김종철, "전자정부와 개인정보보호의 조화 -이념적 측면을 중심으로-", 세계헌법연구 제12권 제2호, 국제헌법학회 한국학회, 2006, 73-75면 참조.

51) 강경근, 앞의 주 6), 127면.

(1) 개설

「전자정부법」은 행정기관 업무의 전자적 처리에 관한 기본법이며, 행정정보공동이용의 근거가 되는 최초의 법률이다. 2001년 3월 28일 제정된 이 법은 행정업무의 전자적 처리를 위한 기본원칙·절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것을 목적으로 하고 있다.

이 법은 행정기관 업무의 전자적 처리에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 적용되는 전자정부에 관한 일반법인데(법 제2조), 제1장 총칙, 제2장 전자정부의 구현 및 운영 원칙, 제3장 행정관리의 전자화, 제4장 대민 서비스의 전자화, 제5장 문서업무의 감축, 제6장 전자정부사업의 추진, 제7장 보칙 등 54개조로 구성되어 있다.

그리고 행정기관은 전자정부의 구현을 촉진하고 지식정보화시대의 국민의 삶의 질을 향상시키도록 이 법을 운영하고 관련 제도를 개선하여야 하며, 행정기관은 당해 기관의 전자정부의 구현 및 운영과 관련하여 행정혁신과 전자정부의 구현을 위한 사업간의 연계, 전자화 대상업무의 처리과정 혁신, 정보통신망을 통한 업무수행 및 행정서비스의 제공, 소속 공무원에 대한 정보통신기술 활용능력의 제고 및 검정, 전자정부의 운영과 관련한 국민 불만사항에 대한 확인 및 신속한 개선 업무를 수행할 책무가 부여되어 있다(법 제5조). 또한 공무원은 담당 업무를 전자적 처리에 적합하도록 개선하는데 최대한의 노력을 기울여야 하고, 담당 업무의 전자적 처리를 위하여 필요한 정보통신기술 활용능력을 갖추어야 하며, 전자적으로 업무를 처리함에 있어서 국민의 편익을 행정기관의 편익보다 우선적으로 고려하여야 할 책무가 있다.

(2) 전자정부의 구현 및 운영 원칙

「전자정부법」제2장은 전자정부의 구현 및 운영 원칙으로서 국민편익 중심의 원칙, 업무혁신 선행의 원칙, 전자적 처리의 원칙, 행정정보공개의 원칙, 행정기관 확인의 원칙, 행정정보공동이용의 원칙, 개인정보보호의 원칙, 중복투자방지의 원칙, 기술개발 및 운영 외주의 원칙을 들고 있다. 그리고 국회·법원·헌법재판소·중앙선거관리위원회 및 행정부는 이 원

칙들을 실현하기 위하여 필요한 시책을 수립·시행하여야 한다.

① 국민편익중심의 원칙 : 행정기관의 업무처리과정은 당해 업무를 처리하는데 있어서 민원인이 부담하여야 하는 시간과 노력이 최소화되도록 설계되어야 한다.

② 업무혁신 선행의 원칙 : 행정기관은 업무를 전자화하고자 하는 경우에는 미리 당해 업무 및 이와 관련된 업무의 처리과정 전반을 전자적 처리에 적합하도록 혁신하여야 한다.

③ 전자적 처리의 원칙 : 행정기관의 주요 업무는 전자화되어야 하며, 전자적 처리가 가능한 업무는 특별한 사유가 있는 경우를 제외하고는 전자적으로 처리되어야 한다.

④ 행정정보공개의 원칙 : 행정기관이 보유·관리하는 행정정보로서 국민생활에 이익이 되는 행정정보는 법령의 규정에 의하여 공개가 제한되는 경우를 제외하고는 인터넷을 통하여 적극적으로 공개되어야 한다.

⑤ 행정기관 확인의 원칙 : 행정기관은 특별한 사유가 있는 경우를 제외하고는 행정기관간에 전자적으로 확인할 수 있는 사항을 민원인에게 확인하여 제출하도록 요구하여서는 아니된다.

⑥ 행정정보공동이용의 원칙 : 행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다.

⑦ 개인정보보호의 원칙 : 행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다.

⑧ 중복투자방지의 원칙 : 행정기관은 전자정부 사업을 추진함에 있어서 다른 행정기관이 보유한 행정정보자원과의 상호연계 및 공동이용 등을 통하여 중복투자가 되지 아니하도록 필요한 조치를 하여야 한다.

⑨ 기술개발 및 운영 외주의 원칙 : 행정기관은 전자정부의 구현에 필요한 기술개발 및 운영에 있어서 당해 사업이 민간부문에 맡길 수 없거나 행정기관이 직접 개발 또는 운영하는 것이 경제성·효과성 또는 보안성 측면에서 현저하게 우수하다고 판단되는 경우를 제외하고는 민간부문에 그 개발 및 운영을 의뢰하여야 한다.

(3) 행정관리의 전자화

「전자정부법」제3장에서는 행정관리의 전자화에 대하여 규정하고 있는데, 행정기관의 문서는 원칙적으로 전자문서를 기본으로 하여 작성·발송·접수·보관·보존 및 활용되어야 한다. 먼저 전자공문서는 당해 문서에 대한 결재가 있음으로써 성립하며, 개인, 법인 또는 단체가 본인임을 확인할 필요가 있는 전자문서를 행정기관에 송신하고자 하는 경우에는「전자서명법」에 따른 공인전자서명 또는 다른 법령에 의하여 본인임을 확인하기 위하여 인정되는 전자적 수단을 이용하여 송신하여야 하고, 전자공문서에는 행정전자서명을 사용한다.

그리고 행정기관은 민원사항의 처리를 위하여 필요한 행정정보, 통계정보·문헌정보 등 행정업무의 수행에 참고가 되는 행정정보,「공공기관의 개인정보보호에 관한 법률」에 의하여 다른 기관에 제공할 수 있는 처리정보,「국가정보화 기본법」에 따른 국가정보화전략위원회가 행정기관간 공동이용이 필요하다고 인정하는 행정정보를 공동이용하여야 한다.

또한「전자정부법」은 행정정보취급·이용자의 금지의무로서 ① 행정정보의 처리업무를 방해할 목적으로 행정정보를 변경하거나 말소하는 행위, ② 행정정보를 변경하거나 말소하는 방법 및 프로그램을 공개·유포하는 행위, ③ 행정기관에서 처리하고 있는 행정정보를 누설하는 행위, ④ 행정기관에서 처리하고 있는 행정정보를 권한 없이 처리하는 행위, ⑤ 행정기관에서 처리하고 있는 행정정보를 권한 없이 타인으로 하여금 이용하게 하는 행위, ⑥ 거짓 그 밖의 부정한 방법으로 행정기관으로부터 행정정보를 열람하거나 제공받는 행위를 들고 있다.

그리고「전자정부법」은 전자정부의 실현에 필요한 행정지식관리, 행정기관의 업무재설계, 전자공문서 등의 표준화, 정보통신망의 구축과 그 보안대책 수립·시행, 정보통신망을 통한 의견수렴, 전자적 업무수행 및 온라인 원격근무, 공무원 정보통신기술 활용능력의 제고, 원격교육훈련 등에 관한 규정을 두고 있다.

(4) 대민 서비스의 전자화

「전자정부법」제4장에서는 대민 서비스의 전자화에 관하여 규정을 하

고 있다. 즉 전자적 민원처리, 구비서류의 전자적 확인, 비방문민원처리, 공인전자서명 등에 의한 신원확인, 전자적 고지·통지, 행정정보의 전자적 제공, 전자적 급부제공과 같은 대민 서비스를 규정하고 있다.

그리고 전자적 대민서비스에서 보안확보를 위하여 행정안전부장관이 국가정보원장과 사전협의를 거쳐 전자적 대민서비스와 관련된 보안대책을 마련하고, 중앙행정기관과 그 소속기관 및 지방자치단체의 장이 이 보안대책에 따라 당해 기관의 보안대책을 수립·시행하도록 하고 있다. 그리고 이 보안대책과 관련한 사항을 심의하기 위하여 행정안전부장관 소속하에 전자정부서비스보안위원회를 설치하고 있다.

(5) 문서업무의 감축

「전자정부법」제5장은 전자정부의 구축을 조장하기 위하여 문서감축을 규정하고 있다. 먼저 행정기관은 의사결정의 쇄신과 전자화, 민원신청의 전자화, 행정정보 제공의 전자화, 행정정보의 공동이용, 문서대장의 전자화 등의 방법으로 그 기관이 취득·작성·유통·보관하는 종이문서 등을 최대한 감축하여야 한다.

이를 위하여 중앙사무관장기관의 장은 문서업무감축계획을 작성하고, 행정기관의 장에게 통보하여야 하며, 행정기관의 장은 이 계획에 따라 매년 자체 집행계획을 수립·시행하여야 한다.

(6) 전자정부사업의 추진

「전자정부법」제6장에서는 전자정부사업의 추진에 관한 규정을 두고 있다. 중장기 전자정부사업계획의 수립, 전자정부사업의 지원, 전자정부사업의 사전협의, 전자정부사업의 종합평가, 시범사업의 추진, 정보화시스템의 보급·확산, 한국지역정보개발원의 설립, 전자정부의 국제협력 등을 규정하고 있다.

(7) 보칙

「전자정부법」제7장 보칙에서는 권한의 위임·위탁, 산하기관 등의 정보화에 관하여 필요한 시책 강구, 이 법 위반행위에 대한 벌칙, 벌칙 적용에서 행정정보를 제공받는 기관의 종사자에 대한 공무원 의제 등을 규정

하고 있다.

2)「행정절차법」

「행정절차법」은 행정절차에 관한 공통적인 사항을 규정하여 국민의 행정참여를 도모함으로써 행정의 공정성·투명성 및 신뢰성을 확보하고 국민의 권익을 보호함을 목적으로 한다.

「행정절차법」문서의 송달은 우편·교부로 하는 것 이외 송달받을 자가 동의하는 경우 정보통신망 이용 등의 방법에 의하도록 하고 전자우편주소로 송달할 수 있도록 하고 있다(법 제14조).

컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송신·수신 또는 저장된 정보로 정의되는 전자문서로 처분을 신청하거나 행정청이 전자문서의 방식으로 처분을 할 수 있으며, 청문을 전자문서로 통지할 수 있다(법 제17조, 제24조, 제31조 제5항).

그리고 행정청이 의사결정과정에 국민의 여론이나 전문가의 의견을 듣기 위하여 일반 공청회와 병행하여서 정보통신망을 이용한 전자공청회를 실시할 수 있도록 하고 있다(법 제38조의2).

또한「행정절차법」제8조에서는 행정응원을 규정하고 있다. 즉 행정청은 ① 법령 등의 이유로 독자적인 직무수행이 어려운 경우, ② 인원·장비의 부족 등 사실상의 이유로 독자적인 직무수행이 어려운 경우, ③ 다른 행정청에 소속되어 있는 전문기관의 협조가 필요한 경우, ④ 다른 행정청이 관리하고 있는 문서(전자문서 포함)·통계 등 행정자료가 직무수행을 위하여 필요한 경우, ⑤ 다른 행정청의 응원을 받아 처리하는 것이 보다 능률적이고 경제적인 경우에는 다른 행정청에 행정응원을 요청할 수 있도록 하고 있다. 이 조항은 행정정보공동이용의 법적 근거가 될 수 있다. 행정청은 이 규정에 따라 필요한 서류나 전자화된 문서를 제공해주도록 요청할 수 있다. 이러한 행정응원이란 도움을 구하는 기관의 과제수행을 가능하게 하거나 쉽게 하기 위하여 다른 국가기관에 문의하고 찾아주는 국가기관의 활동을 말한다.[52] 따라서 행정응원은 이를 구하거나 제공하는 기관에게 그 관할이나 권한의 확대나 이동을 뜻하지는 않는다. 그렇다면 도움요청이 없는 자발적인 행정응원은 법에 특별히 규정되어 있지

52) Paul Stelkens / H. J. Bonk / Michael Sachs, Verwaltungsverfahrensgesetz, C. H. Beck. (1993), pp.242-48.

않는 한 허용되지 않으며, 기관 내에서 지원행위는 원칙적으로 행정응원이 아니다. 그렇다고 한 기관 내에서 기관내부간 협조가 무제한적으로 허용되는 것이 아니라 업무에 필요하고 사항적 관할 영역 속에 있으며 사항결정을 위하여 필요한 경우에 허용된다.

이러한 행정응원은 현존하는 관할과 권한 내에서만 보충기능을 가진 것으로서 그 내용에 따라 정보제공뿐만 아니라 다양한 사실행위 또는 그 외 다른 행위도 포함된다. 이러한 행정응원은 원칙적으로 개개의 경우 청구하고 요청하며 허용되어야만 한다. 따라서 장기간 또는 지속적인 협력이나 공동의 전자정보처리시스템운영은 더 이상 행정응원으로 표현될 수 없다. 그러나 협력형태를 위해서는 이에 관한 또 다른 법적 근거를 필요로 한다.[53]

3) 「국가정보화기본법」

(1) 개설

2009년 5월 22일 전부 개정된「국가정보화기본법」은 국가정보화의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정함으로써 지속가능한 지식정보사회의 실현에 이바지하고 국민의 삶의 질을 높이는 것을 목적으로 하며, 국가정보화의 추진을 통하여 인간의 존엄을 바탕으로 사회적, 윤리적 가치가 조화를 이루는 지식정보사회를 실현하고 이를 지속적으로 발전시키는 것을 기본이념으로 한다. 그리고 국가정보화의 추진에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따르도록 함(법 제5조)으로써「국가정보화기본법」이 국가정보화추진에 관한 일반법으로서의 성격을 가지고 있다고 할 수 있다.

「국가정보화기본법」에서는 국가정보화란 국가기관, 지방자치단체 및 공공기관이 정보화를 추진하거나 사회 각 분야의 활동이 효율적으로 수행될 수 있도록 정보화를 통하여 지원하는 것을 말한다고 정의하고 있다.

이 법은 제1장 총칙, 제2장 국가정보화 정책의 수립 및 추진체계, 제3장 국가정보화의 추진, 제4장 국가정보화의 역기능 방지, 제5장 연차보고 등, 제6장 정보통신기반의 고도화 등 51개조로 구성되어 있다.

53) 김일환, 앞의 주 10), 512면.

(2) 국가정보화 정책의 수립 및 추진

「국가정보화기본법」에서는 정부가 국가정보화의 효율적, 체계적 추진을 위하여 5년마다 국가정보화기본계획[54]을 수립하여야 하며, 이 기본계획에 따라 중앙행정기관의 장과 지방자치단체의 장은 매년 국가정보화시행계획을 수립·시행하여야 한다(법 제6조 및 제7조).

그리고 국가정보화 추진과 관련된 사항을 심의하기 위하여 대통령 소속으로 국가정보화전략위원회를 설치하는데, 이 위원회는 기본계획 및 시행계획의 수립, 국가정보화 정책이나 사업 추진의 조정, 지식정보자원의 지정, 정보문화의 창달 및 정보격차의 해소를 위한 사업의 우선순위 결정, 중장기 지식정보자원 관리계획 등을 심의한다. 특히「전자정부법」에서 이 위원회의 심의사항으로 정한 사항을 심의하도록 하고 있는데(「국가정보화기본법」제10조 제8호),「전자정부법」에서는 국가정보화전략위원회가 행정기관간 공동이용이 필요하다고 인정하는 행정정보를 행정기관이 공동이용하도록 하고 있다(「전자정부법」제21조 제1항 제4호).

그리고「국가정보화기본법」에서는 국가기관과 지방자치단체의 국가정보화 시책의 효율적인 수립·시행과 국가정보화 사업의 조정 등의 업무를 총괄하는 정보화책임관을 임명하도록 하고 국가정보화 사업의 총괄조정, 지원 및 평가, 국가정보화 정책과 기관 내 다른 정책·계획 등과의 연계·조정, 정보기술을 이용한 행정업무의 지원 등의 업무를 담당하도록 하였다(법 제11조).

(3) 국가정보화의 추진

「국가정보화기본법」제3장에서는 분야별 정보화의 추진과 지식정보자원의 관리 및 활용에 관하여 규정하고 있다.

국가기관 등은 행정 업무의 효율성 향상과 국민 편익 증진 등을 위하여

54) 기본계획에는 ① 국가정보화 정책의 기본 방향 및 중장기 발전방향, ② 행정, 보건, 사회복지, 교육, 문화, 환경, 과학기술 등 공공 분야의 정보화, ③ 제16조에 따른 지역정보화, ④ 산업·금융 등 민간 분야 정보화의 지원, ⑤ 제2호부터 제4호까지의 사항과 관련된 분야별 정보보호, 국가정보화 기반의 조성 및 고도화, ⑥ 정보문화의 창달 및 정보격차의 해소, ⑦ 개인정보 보호, 건전한 정보통신 윤리 확립, 이용자의 권익보호 및 지적재산권의 보호, ⑧ 정보의 공동활용 및 표준화, ⑨ 국가정보화와 관련된 법령·제도의 개선, ⑩ 국가정보화와 관련된 국제협력의 활성화, ⑪ 국가정보화와 관련된 재원의 조달 및 운용, ⑫ 그 밖에 국가정보화 추진을 위하여 필요한 사항 등이 포함되어야 한다(법 제6조)

행정, 보건, 사회복지, 교육, 문화, 환경, 과학기술 등 소관 업무에 대한 공공정보화를 추진하여야 하며(법 제15조), 국가기관과 지방자치단체는 지역주민의 삶의 질 향상과 지역 간 균형발전, 정보격차 해소 등을 위하여 하나 또는 여러 개의 지역·도시에 대하여 행정·생활·산업 등의 분야를 대상으로 하는 지역정보화를 추진할 수 있다(법 제16조). 그리고 정부는 산업·금융 등 민간 분야의 생산성 향상과 부가가치 창출 등을 위하여 기업의 정보화 및 정보통신기반의 구축·이용 등 민간 분야의 정보화에 필요한 사항을 지원할 수 있다(법 제17조).

국가정보화의 추진을 통하여 창출되는 각종 지식과 정보가 사회 각 분야에 공유·유통, 공공정보화 추진에 필요한 민간투자 유치와 민간사업자와 민간사업자단체에 필요한 지원, 정보통신응용서비스 이용 등의 활성화와 우수한 콘텐츠의 개발 촉진 시책을 규정하고 있다.

특히 정부는 국가정보화를 효율적으로 추진하고 정보의 공동활용을 촉진하며 정보통신의 효율적 운영 및 호환성 확보 등을 위하여 표준화를 추진하여야 하며(법 제21조), 국가기관과 지방자치단체가 구축한 정보통신망의 효율적인 운영과 정보의 공동활용을 촉진하기 위하여 정보통신망간 상호연동에 필요한 시책을 마련하도록 하여(법 제22조) 전자정부에서 필요로 하는 행정정보공동이용의 기반을 구축하도록 하였다.

그리고 국가기관과 지방자치단체는 지식정보자원을 효율적으로 관리하도록 하고(법 제25), 이 지식정보자원의 개발·활용 및 효율적인 관리를 위하여 지식정보자원의 수집, 보존 및 전송, 지식정보자원의 공동활용, 그 밖에 지식정보자원의 개발·활용 및 효율적인 관리를 위하여 필요한 사항 등과 관련된 표준화를 추진하도록 하였다(법 제26조).

(4) 국가정보화의 역기능 방지

「국가정보화기본법」제4장에서는 정보이용의 건전성·보편성 보장과 정보이용의 안전성 및 신뢰성 보장을 규정하고 있다.

국가기관과 지방자치단체는 모든 국민이 국가정보화의 편익을 누릴 수 있도록 정보문화의 창달 및 확산 시책을 마련하여야 하며(법 제29조), 인터넷 중독의 예방 및 해소, 정보격차 해소 시책의 마련, 장애인·고령자 등의 정보 접근 및 이용 보장, 정보격차의 해소와 관련된 기술 개발 및

보급지원, 정보통신제품의 지원, 정보격차해소교육의 시행 등을 규정하고 있다.

그리고 국가기관과 지방자치단체는 정보를 처리하는 모든 과정에서 정보의 안전한 유통을 위하여 정보보호를 위한 시책을 마련하여야 하며, 정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 마련하여야 한다(법 제37조). 그리고 정보보호시스템에 관한 기준 고시, 개인정보 보호 시책의 마련, 이용자의 권익 보호 등, 지적재산권의 보호 등을 규정하고 있다.

(5) 연차보고 등

「국가정보화기본법」에서는 정부가 매년 국가정보화의 동향과 시책에 관한 보고서를 정기국회 개회 전까지 국회에 제출하여야 하도록 하고 있으며(법 제43조), 사회 각 분야의 정보화에 대한 지표를 조사하고 개발하여 보급하도록 하고 있다(법 제44조).

그리고 방송통신위원회는 광대역통합정보통신기반의 원활한 구축과 이용촉진을 위하여 필요한 때에는 홍보, 국제협력, 기술개발 등 그 업무를 전담할 기관을 분야별로 지정하고, 공공기관과 일정한 비영리기관 등이 이용하는 초고속정보통신망을 구축·관리하거나 이 전담기관으로 하여금 구축·관리하게 할 수 있도록 하였다.(법 제48조 및 제49조).

다. 요약 및 분석

「전자정부법」은 행정기관 업무의 전자적 처리에 관한 일반법의 성격을 가지고 있으며, 전자정부의 구성 및 운영에 관한 전반적인 사항을 규율하고 있다. 특히 전자정부법은 행정정보공동이용의 원칙에 대하여 규정하고 있다. 즉, 행정기관이 수집·보유하고 있는 행정정보를 다른 행정기관과 공동이용하여야 하며, 또 다른 기관이 보유하고 있는 행정정보를 제공받을 수 있는 경우에는 따로 수집하여서는 아니된다고 규정하고 있다. 또한 행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니 된다고 하면서 그 개인정보의 수집의 범위나 공유·보유·관리에 대한 구체적인 규정은 없어

행정정보공동이용으로 인한 침해가 예상된다.

「행정절차법」도 전자정부의 구축에 있어서 중요한 역할을 하고 있다. 처분의 신청과 행정청의 처분 및 청문의 통지를 정보통신망에 의한 전자문서로 할 수 있도록 하여 전자문서의 활용을 개방하고 있으며, 행정응원의 형식을 빌어 행정정보공동이용도 가능하도록 하였다.

한편 국가정보화추진에 관한 일반법으로서의 성격을 가지고 있는「국가정보화기본법」은 우리나라 정보화에 있어서 근간이 되는 가장 기본법이다. 특히「전자정부법」에 의한 전자정부 구현을 위한 각종 계획을 심의하는 절차를 규정하고 있으며, 국가정보화기본계획의 수립, 정보의 공동활용, 정보통신망간 상호연동, 광대역통합정보통신기반의 원활한 구축과 이용촉진 등에서 전자정부의 구축과 밀접한 관련이 있다고 생각한다.

이러한 법률들에서는 국가의 정보화와 전자정부의 구현을 위한 방침과 내용을 규정하고 있다는데 대하여 큰 의의를 둘 수 있으나, 상대적으로 전자정부의 역작용을 예방하는 장치를 마련하는데 소홀하고 있다고 생각한다.

3. 전자정부법제에 관한 비교법적 고찰

가. 미국

1) 전자정부 관련 주요법령

미국에서의 전자정부 관련 법령으로는 1980년「정부문서업무감축법」을 제정하여 정보자원관리를 위한 기본정책틀을 마련하였으며, 이후 1993년「정부성과결과법」,1996년「정보기술개혁법」,1996년「전자정보자유법」, 1988년「정부업무문서폐지법」, 1999년「전자적공개제공법」, 그리고 2002년「전자정부법」을 제정하였다.「전자정부법」은 전자정부를 겨냥한 최초의 포괄적 입법으로 특히, 전자정부 구축을 위한 추진체계 및 이에 따른 각 행정부처의 책임과 역할을 명백히 밝힌 법제라고 할 수 있다. 주요내용을 살펴보면 다음과 같다.

2) 전자정부 추진체계 및 주요 내용

이 법은 국민 중심의 전자정부를 보다 통합적으로 추진하고 행정기관의 협력 및 민간부문과 정부 사이의 협력을 증진함으로써 국민의 권리를 보다 충실히 보장하기 위하여 ① 예산관리처 내에 신설한 전자정부국의 국장을 둠으로써 연방정부의 리더십을 효과적으로 발휘하여 전자정부 서비스 및 업무를 개발하고 촉진한다. ② 인터넷 등 정보기술의 이용을 촉진하여 국민의 정부참여 기회를 확대한다. ③ 관련업무 통합에 의한 대민 서비스의 질을 향상시키는데 필요한 전자정부 서비스의 제공 및 업무의 능률과 효과를 제고할 수 있는 내부적 전자정부 업무절차의 이용과 관련하여 기관간 협력을 촉진한다. ④ 정부의 업무능력 제고를 통해 기관의 사명과 프로그램의 성과목표를 달성한다. ⑤ 정부기관 대내외에 인터넷 및 신기술의 사용을 촉진함으로써 국민 중심의 전자정부와 서비스를 제공한다. ⑥ 기업 및 그 밖의 정부기관들의 비용과 업무 부담을 줄인다. ⑦ 정책입안자들의 보다 전문화된 의사결정을 촉진하다. ⑧ 다양한 경로를 통한 양질의 정부정보 및 서비스 이용을 촉진하다. ⑨ 연방정부의 투명성과 책임을 강화한다. ⑩ 공공 및 민간단체의 모범 사례를 적절히 활용하여 정부기관의 업무집행을 변화시킨다. ⑪ 개인의 프라이버시 보호, 국가안보, 기록보존, 장애인의 이용 등에 관한 법률 및 그 밖의 관련 법률에 따라 정부정보와 서비스에 대한 접근의 용이성을 추구한다.

또한 이 법에서는 전자정부를 “정부가 국민, 단체 및 그 밖의 정부기관의 정부정보 및 서비스에 대한 접속 및 이들에 대한 정부정보 및 서비스의 제공・원활화 또는 정부업무의 효과, 효율성, 서비스 질 향상 등의 개선을 목적으로 일정한 절차와 함께 웹 기반 인터넷 프로그램과 그 밖의 정보기술을 이용하는 것”(제3601조(3))으로 정의하고 있다.

전자정부 추진체계와 관련하여서는 정보자원 및 기술 관리를 포함하여 전자정부의 효율적 구현이라는 관점에서 예산관리처장 직속으로 전자정부국을 두어 범정부적인 정보자원 및 기술관리 등 전자정부 관련 업무를 총괄하여 전담하도록 하였다. 그리고 정보화책임관협의회를 행정부 내에 두고 있다. 협의회의 업무는 정부 정보자원관리정책과 기준에 대한 권고안을 개발해 처장에게 제시하는 업무, 정보자원관리에 관한 경험, 아이디어, 모범사례 및 혁신방법 등의 공유, 정보기술을 이용한 정부의 업무 능력 향상을 위한 복수기관 관련 사업 및 그 밖의 혁신적 발상의 파악, 개발 및 조정업무에 있어 국장을 보좌하는 업무, 기관의 정보관리를 위한 공통

적 성과지표의 개발 및 이용촉진업무, 정보기술 표준에 관한 권고안을 개발하고 상업적 표준의 적절한 이용을 극대화하기 위하여 표준기술원 및 국장과의 협력업무, 정보자원관리 관련 채용, 교육, 분류, 전문적 개발 작업의 필요성을 평가하고 피력하기 위하여 인사관리처와의 협력업무, 연방기록법이 연방 정보자원관리 활동을 얼마나 효율적으로 규율할 수 있는지 평가하기 위하여 국민문서보관소장과 협력하는 업무 등이다(제3602조(f)).[55]

3) 프라이버시 영향평가

「전자정부법」은 국민 중심의 전자정부를 구현하는 과정에서 개인정보 및 프라이버시가 충분히 보호될 수 있도록 프라이버시영향평가를 실시할 것을 규정하고 있는데(제208조), 그 내용을 보면 다음과 같다.

(1) 기관의 책임

각 기관은 필요한 범위 내에서 프라이버시 영향평가를 수행하고, 당해 기관간의 결정에 따라 정보화책임관 또는 그에 상당하는 공무원이 프라이버시 영향평가를 검토하도록 하며, 가능한 범위 내에서 검토하여 기관 웹사이트, 연방관보 게재 또는 여러 수단을 통하여 프라이버시 영향평가를 공개하고 난 후(제208조(c)), 신원확인이 가능한 정보를 수집, 유지·관리 또는 유포하는 정보기술의 개발이나 조달 또는 정보기술을 이용하여 수집, 유지·관리 또는 유포되는 정보 또는 연방정부의 기관, 그 대행기관 또는 직원을 제외한 10인 이상의 자에 대하여 신원확인 문제가 제기되거나 보고요건에 신원확인이 들어있는 경우, 특정 개인의 물리적 또는 온라인 접속을 허용하고, 신원확인이 가능한 정보 등 새로운 정보들을 수집개시를 하여야 한다(제208조(b)). 여기서 민감한 정보는 보안상의 이유 또는 평가에 포함된 기밀 또는 민감한 정보나 개인정보를 보호하기 위해 이를 변경하거나 배제할 수 있다.

(2) 프라이버시 영향평가의 내용

예산관리처장은 프라이버시 영향평가의 필수요건들을 구체화한 지침을

55) 황종성 외, 전자정부법 개정방안 연구, 한국정보사회진흥원, 2008, 43-44면.

기관들에 시달하여야 한다. 그 요건은 ① 평가되는 정보시스템의 규모, 당해 시스템에서 신원확인이 가능한 정보의 민감성, 당해 정보의 무단 공개로 초래되는 위험 등에 관하여 프라이버시 영향평가가 이루어지게 하고, ② 프라이버시 영향평가는 수집할 정보, 당해 정보를 수집하는 이유, 당해 정보의 용도, 정보공유의 대상, 수집되는 정보 내용과 이를 공유하는 방식과 관련하여 개인에게 제시할 동의 기회 또는 고지, 정보보안 방안, 기록체계가 미합중국 제5편 제552a조(통칭 프라이버시보호법)에 따라 생성되는지의 여부 등이다(제208조(b)(2)).

(3) 처장의 책임

예산관리처장은 프라이버시 영향평가의 수행과 관련된 기관 정책과 지침을 개발하고, 범정부적으로 프라이버시 영향평가 과정의 구현을 감독하며, 처장이 적절하다고 판단하는 바에 따라 기존 정보 시스템이나 신원확인이 가능한 정보의 계속적 수집에 대한 프라이버시 영향평가를 기관이 수행하게 한다(제208조(b)(3)).[56]

3) 미국 전자정부법제 시사점

미국의「전자정부법」과 우리나라「전자정부법」을 비교해볼 때 우리나라「전자정부법」은 전자정부를 “정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다”(법 제2조 제1호)고 정의하여 행정의 효율성 또는 기능이나 역할에 치중하는 반면, 미국의「전자정부법」은 국민이 보다 더 정부와 친숙해질 수 있도록 배려함과 동시에 개인정보의 보호를 위해 프라이버시 영향평가제를 두고 운영하고 있어 전자정부 운영의 효율성보다 개인의 프라이버시 보호에 더 중점을 두고 있다는 점에서 보다 개방적이라는 느낌이 든다.

그리고「전자정부법」은 전자정부의 비전을 제시한 점, 전자정부 추진체계의 확립, 재원의 안정적 지원책 마련, 정보보호 정책체계의 정비, 인센티브 제공으로 민간참여를 유도한 점 등은「전자정부법」을 미국 보다 먼저 제정하여 운용하고 있는 우리나라의 법제에도 많은 시사점을 던진다

56) 위의 책, 48-49면.

고 하겠다.[57]

나. 프랑스

1) 전자정부 관련 주요법령

프랑스에는 우리나라의「전자정부법」과 같은 전자행정구현을 위한 일반적 성격의 법률은 없다. 다만 전자정부구현의 기반이 되는「전자서명에 관한 법률」,「전자서명에 관한 법률 시행령」,「정보공개에 관한 법률」 및「개인정보보호에 관한 법률」등이 제정되어 있다. 프랑스에서는 전자정부라는 말 대신에 전자행정(Administration èlectronique)이라는 용어를 쓴다. 그것은 행정의 전자화가 주로 행정부 내의 행정기관 및 대국민행정을 대상으로 하여 추진되고 있기 때문이다.[58]

전자행정에 관한 주요 법제로는 첫째, 전자행정의 안전성과 관련하여 2000년 3월 13일「정보기술에의 입증법의 적응 및 전자서명에 관한 법률 제2000-230호[59] (이하「전자서명법」이라함)」과 2001년 3월 30일 민법전 제1316-4조의 적용을 위해 제정된「전자서명에 관한 명령제2001-272호[60] (이하「전자서명법 시행령」이라 함)」를 들 수 있다.[61]

둘째, 전자행정절차와 관련하여 전자서식에 관한 명령서, 행정서식의 인터넷 제공에 관한 1999년 2월 2일 명령, 2000년 6월 16일 이 명령 시행규칙, 1999년 12월 31일 인터넷상에서의 행정절차에 대한 지원에 관한 훈령 등을 들 수 있고 행정절차를 규정하는 1978년 법률[62] 과 1994년 조세법전 (Code Général des Impôts) 등이다.[63]

---

57) 위의 책, 51면.

58) 프랑스법제에 관해서는 박균성, 프랑스에서의 전자정부구현을 위한 법제 동향, 한국법제연구원, 2001, 76면.

59)「Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JO 14 mars 2000」

60)「Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique」

61) 박균성, 프랑스의 전자정부법제, 한국법제원, 2001, 53-54면

62)「Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal」

63) 행정절차를 규정하는 1978년 법률에서는 전자적 방식에 의해 신고 또는 신청을 하기 위하여 특정기간 또는 일정한 기간을 준수하여야 하는 국민은 모두 문서의 우송뿐만 아니라 발송일을 증명할 수 있는 전자적 방식에 의해 신고선 또는 신청서를 제출하고 있다. 또 1994년 조세법

셋째, 정보공개법령에 관해서는 1978년「행정과 공중의 관계개선조치에 관한 법률」이 2000년 4월 12일 개정된 법률[64]과 1978년 7월 17일 법률 제78-753조의 집행을 위해 제정되었고 행정문서의 공개방식에 관한 2001년 6월 6일 명령 제2001-493호 등이 있다.[65]

넷째, 개인정보보호에 관하여는 1978년에 제정된「정보처리, 축적 및 자유에 관한 법률(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)」은 1992년, 1994년, 2000년에 개정되었다.[66]

2) 전자정부 관련 법제의 특징

프랑스에서는 우리의「전자정부법」에 해당하는 일반 법률이 제정되어 있지 않지만, 전자행정을 집행함에 있어서 개인정보를 보호하기 위한 법률이 비교적 잘 정비되어 있다.

프랑스는 서유럽의 다른 국가들과 비교하여 상대적으로 정보화가 늦은 편이지만, 1998년 이후부터 매우 의욕적이고 계획적으로 정보화를 추진하고 있으며, 행정의 전자화도 사회정보화의 한 내용으로 적극 추진되고 있다. 프랑스에서의 전자행정은 정보통신기술을 이용하여 행정서비스를 현대화를 하고 국가와 지방자치단체간의 행정활동의 효율성을 제고하며 행정기관과 이용자 사이의 질을 높이는 것을 목표로 하고 있다.[67]

전의 개정으로 모든 기업의 행정에 대한 신고는 계약에 의해 정해진 조건에 따라 전자적 수단에 의해 행해질 수 있다: 박균성, 프랑스에서의 전자정부구현을 위한 법제 동향, 78-79면.

64)「Loi n° 2000-321 du 12 avril 2000 Article 7 JORF 13 Avril 2000」

65) 한국정보사회진흥원, 앞의 주 17), 52면.

66) 박균성, 프랑스에서의 전자정부구현을 위한 법제 동향, 80-81면: 1992년 개정에서는 인종 또는 정치적·철학적 또는 종교적 의견 및 종합소득 또는 인간의 품성을 직접 또는 간접으로 드러내는 개인정보를 관계인의 명시적 동의 없이 정보를 처리할 수 없고 또한 정보 처리된 형식으로 보관할 수 없다. 다만, 공익을 위하여 국사원의 동의를 받은 명령에 의한 위원회의 제안 또는 동의를 받은 경우에는 그러하지 아니하다(제31조). 1994년 개정법에서는 특히 의료정보에 관하여 규율하고 있다. 개인의 치료를 위해서는 정보의 처리가 허용되고, 보건분야에서의 연구를 위해서는 일정한 조건하에서 개인정보의 자동처리가 허용되지만 정보처리는 국가정보처리·기본권위원회의 허가를 받아야 하고, 개인을 식별할 수 있는 정보를 송부할 때에는 코드화하여 보내도록 규정하고 있다(제40-1, 40-2, 40-3조). 의료정보의 보호와 이용에 관하여는 1999년과 2000년에 관련규정의 개정이 다시 있었다. 2000년에 개인정보보호법이 다시 보완·개정되었는데 개정된 주요내용은 다음과 같다. ① 정보가 수집·처리되는 목적의 실현에 필요한 기간 이상으로 정보는 원칙상 개인정보의 형식으로 보관될 수 없으며, 다만 역사적·통계적·과학적 목적의 처리를 위해서만 그 기간 이상으로 보관될 수 있다. 이와 같이 보관될 정보의 선택은 기록물에 관한 1979년 1월 3일 법률 제79-18호의 제4-1조에 규정된 조건에 따라 이루어진다(제28조 제1항).

프랑스에서는 아직도 행정절차가 우편, 전화 또는 민원창구를 통하여 행하여지는 경우가 많은데, 그 이유는 인터넷을 통한 전자행정방식은 기존의 전통적인 행정방식을 대체하는 것이 아니라 새로운 행정방식으로 추가되는 것으로 이해되기 때문이다. 그리고 행정객체의 신원확인 등을 위하여 더 효과적인 경우도 있고, 다른 한편으로 모든 국민이 전자행정방식에의 접근이 가능하지 않은 상황에서 전자행정방식만을 인정하는 것은 행정에서의 국민의 평등권을 침해하기 때문이다. 즉, 프랑스의 행정목표는 전통적 행정방식을 인정하면서 전자행정방식의 장점을 극대화하는 것이다.[68]

또 정보공개와 관련하여 행정기관이 공개하여서는 아니 될 정보를 제공하거나 잘못된 정보를 제공한 경우, 또는 국민의 권익을 보호하기 위하여 정보를 제공하여야 함에도 불구하고 제공하지 않은 경우 정보제공담당자의 민・형사상 책임과 국가배상책임의 문제가 제기된다.[69]

살펴본 바와 같이 프랑스에서는 전자행정에 관한 일반 법률을 제정하지 않고, 필요할 때마다 제정하는 방식을 취한다. 그 이유는 ① 일반 법률을 제정할 만큼 대국민전자행정에 대한 법적 문제가 아직은 발생하지 않는다는 점, ② 아직 큰 문제도 드러나지 않았는데 굳이 정보접근이 어려운 자들을 고려하여 전통적 방법과 전자적 방법을 혼용하면서 단계적으로 시행해도 된다는 여유로움, ③ 또한 현재의 행정운용에 있어서 정부행동계획이나 훈령을 통해서도 충분한 제도적 근거가 되기 때문이다.

다. 일본

1) 전자정부 관련 주요법령

일본에서도 프랑스 경우처럼 전자정부의 전자행정을 규율하는 일반법인「전자정부법」은 제정되어 있지 않지만, 전자정부구현을 위한 관련 법률들은 다수 있다. 예를 들면「서면교부 등에 관하여 정보통신기술이용을 위한 관련 법률의 정비에 관한 법률」,「상업등기법의 일부를 개정하는 법률」,「전자서명 및 인증업무에 관한 법률」,「전자정보처리조직에 의한

67) 박균성, 프랑스의 전자정부법제, 7면.
68) 박균성, 프랑스에서의 전자정부구현을 위한 법제 동향, 72면.
69) 박균성, 프랑스의 전자정부법제, 82면.

등기사무처리의 원활화를 위한 조치 등에 관한 법률」,「총무성설치법」,「고도 정보통신네트워크 사회형성기본법」(이하「IT기본법」이라함),「정부 액세스 행위의 금지 등에 관한 법률」,「정보공개법」,「전기통신회선에 의한 등기정보의 제공에 관한 법률」,「행정기관이 보유하는 전자계산기처리에 관련한 개인정보의 보호에 관한 법률」,「개인정보보호법」등이 있다.[70]

2)「고도정보 통신네트워크 사회형성 기본법 (IT기본법)」의 주요내용

「고도정보통신네트워크 사회형성 기본법 (IT기본법)」의 목적은 정보통신기술의 활용으로 세계적 규모로 발생하고 있는 급진적이고, 대폭적인 사회경제구조의 변화에 적절히 대응하는 것이다. 고도 정보통신 네트워크 사회의 형성에 관한 기본이념 및 시책 정책에 대한 기본방침을 정하고 국가 및 지방공공단체의 책무를 명확하게 하며, 고도 정보통신 네트워크 사회 추진전략본부를 설치함과 동시에 고도 정보통신 네트워크 사회의 형성에 관한 시책을 신속하고 중점적으로 추진하여 국민의 민주주의, 국민생활과 문화의 발전 및 공공복지 증진에 이바지하는 것을 목적으로 하고 있다(법 제1조).

제정 목적에서 보듯이 이 법은 국가 정보화를 한 차원 업그레이드 시킬 수 있는 기반을 마련하는 것이다. 즉, 국가정보화의 체계적 추진을 위한 입법의 일환이다. 이 법률은 전자정부 구현을 위한 각종 심의·결정하는 절차들을 규정하고, 고도 정보통신 네트워크 사회를 형성하기 위해 모든 국민이 정보통신기술의 혜택을 향유할 수 있는 사회를 실현하기 위해 인터넷, 기타 고도 정보통신 네트워크를 정보격차 없이 누구나 쉽게 접할 수 있는 기회를 제공하며, 이 기회를 통해 개개인의 능력을 최대한 발휘하여 정보통신기술의 혜택을 골고루 향유하는 것을 기본으로 한다.

그리고 법 제25조 내지 34조에서는 고도 정보통신 네트워크 실현을 위한 행정조직에 관한 전반적인 사항을 규정하고 있는데, 고도 정보통신 네트워크 사회의 형성에 관한 시책을 신속하게, 그리고 중점적으로 추진하기 위해 내각에 고도 정보통신 네트워크 사회 추진전략 본부를 두고, 본부원은 본부장 및 부본부장 이외의 모든 국무대신, 교육, 문화, 과학 및

70) 박균성, 프랑스에서의 전자정부구현을 위한 법제 동향, 76면.

산업의 각 분야에서 식견을 가진 자 중에서 내각총리대신이 임명하는 자로서 충당하고, 본부에 관한 사무는 내각관방에서 처리한다고 규정하고 있다.

이 법률은 'IT혁명'에 정확하게 대응하고 IT의 활용에 의해 발생하는 지식창조적인 사회에 어울리는 다양한 국민생활과 활력 있는 경제사회를 실현하기 위한 기본적 구조를 정하고 있다고 볼 수 있다.

특히 이 법률은 전자정부, 전자자치체의 추진(행정의 간소화, 효율화, 투명성의 향상), 공공분야의 정보화를 기본방침으로 함으로써 전자정부의 실현에 대한 의지를 담고 있다고 할 수 있다.[71]

4. 전자정부에서 개인정보보호 문제

일반적으로 전자정부와 개인정보보호와의 관계를 설명해 주는 이론이나 모형은 존재하지 않는다. 그러나 정보의 안전(information security)에 신뢰성이란 요소를 추가하여 온라인 환경에서의 신뢰를 구축함에 있어서 프라이버시·개인정보보호가 매우 중요하다는 데 대해서는 폭넓은 공감대가 형성되어 있다. 프라이버시는 신뢰의 전제조건(precondition for trust)이며 신뢰는 다시 프라이버시에 영향을 미친다. 이 점은 전자정부와 개인정보보호에 대해서도 마찬가지로 적용된다. 앞서 지적하였듯이 개인정보가 오·남용되지 아니하고 해킹이나 유추 등의 위험으로부터 안전하다는 신뢰를 줄 수 있느냐 하는 것이 전자정부의 성공을 좌우하는 관건이 된다. 이와 같이 개인정보의 충분한 보호가 전자정부의 성패를 좌우하는 핵심적 성공요인의 하나라는 것, 그리고 전자정부의 활성화의 선결조건을 이룬다는 것은 널리 공유되고 있는 생각이다.[72]

더 나아가 정보통신기술의 필요성과 중요성이 커질수록 그와 결부된 새로운 잠재적 위험도 커지고, 그만큼 정보사회의 역기능으로부터 개인을 보호하는 문제도 절실한 과제가 되고 있다. 정보화에 따를 생활상 편익의

71) 김재광, "일본의 전자정부 구현을 위한 법제 고찰", 한국법제원, 2001, 138면.

72) 홍준형, "전자정부와 개인정보보호 -정보사회의 권리장전을 위하여-", 정보과학회지 제22권 제11호, 학국정보과학회, 2004, 69면; 김성태, 전자정부 -이론과 전략, 법문사, 2003, 29면; OECD. (2003a). The e-Government Imperative(OECD e-Government Studies: http://www1.oecd.org/publications/e-book/4203071E.PDF).

증진이나 경제성·효율성 등과 같은 긍정적 결과 못지않게 그로 인한 위험과 불안감도 커지고 있다. 따라서 전자정부의 존속을 보장하고 안전을 확보하기 위한 행정법적 대응이 요구된다.

언급한 바와 같이「전자정부법」제11조는 행정정보의 공동이용을 명시하고 있지만, 그 범위나 구체적인 사항은 전혀 규정하고 있지 않다. 개인정보도 당연히 전자정부가 보유하고 있는 행정정보이고, 또 공용이용의 대상임이 분명함에도 불구하고, 이와 같이 무방비한 상태로 행정정보의 공동이용의 편리성에만 초점을 맞추고 있는「전자정부법」은 개인정보의 침해로 이어지게 된다.

제3절 행정정보공동이용과 헌법적 논의

1. 행정정보공동이용 개관

가. 행정정보공동이용의 의의

행정정보공동이용은 정부 및 공공기관이 업무수행의 목적으로 보유하고 있는 행정정보를 다른 행정기관 또는 공공기관, 공공부문과 민간부문, 기관·기업·개인 사이에 정보시스템을 통하여 공동으로 활용하는 것을 의미한다. 따라서 이러한 정보공동이용은 해당정보에 접근, 해당정보의 공유, 해당정보의 사용을 포함한다. 전자정부의 구현·발전을 위하여 핵심적 요소가 바로 '행정정보의 공동이용'이다. 정보시스템을 통한 행정정보의 공동이용은 정보전달의 신속성·정확성 확보, 지리적·시간적 한계의 극복, 종이문서 사용 절약 등의 경제적 효과가 발생하므로 전자정부 구현에 있어서 이상적이며 필수적인 수단이라 할 수 있다.[73]

「전자정부법」제2조 제4호에서는 행정정보공동이용을 행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것으로 밝히고 있다.

여기서 말하는 행정기관이란 국회·법원·헌법재판소·중앙선거관리위

73) 행정자치부, 앞의 주 4), 63면.

원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관 및 국무총리 소속기관을 포함한다. 이하 같다) 및 그 소속기관, 지방자치단체를 말하므로, 건강보험공단, 국민연금관리공단 등 공공기관이 작성·관리하고 있는 자료는 행정정보에 해당하지 아니한다.

이러한 행정정보를 제공받아 이용하는 자는 행정기관에 국한되며, 그 제공은 반드시 전자적 방식을 통해 이루어져야만 한다. 행정정보를 공공기관 이외의 민간부문, 예컨대 금융기관이 제공받아 활용하는 경우에 개인정보침해의 위험성은 매우 크다고 할 수 있다.[74] 그러나 행정정보 공동이용은 행정기관뿐만 아니라 국민의 편의적 측면에서 공공기관 또는 금융기관까지 확대하는 것이 당연한 논리이고, 이에 따른 개인정보침해에 대비하여 그 정의 및 범위가 확정되어야 한다.

나. 행정정보 공동이용의 필요성

전자정부는 정보통신기술을 기반으로 하여 정부업무의 전자적 처리와 유기적 연계로 행정의 효율성과 투명성을 제고하고, 국민과 기업이 원하는 정보와 서비스를 언제 어디서나 쉽게 접근하고 이용할 수 있도록 하는 것을 목표로 한다.[75] 따라서 행정정보를 공동이용하고, 동일한 정보의 중복수집을 금지하며, 행정기관 사이에 확인할 수 있는 민원서류의 제출요구를 금지하기 위하여「전자정부법」에서 규정하고 있는 것이 바로 행정정보공동이용의 원칙이다.[76]

결국 정보통신망에 의한 행정정보의 공동이용은 컴퓨터 시스템과 네트워크를 활용한 공동이용방법으로 정보전달의 신속성·정확성 확보, 지리적·시간적 한계의 극복, 종이문서 사용 절약 등의 효과가 있으므로, 전자정부구현을 위하여 이상적이며 필수적인 수단이라 할 수 있다.[77]

---

74) 권건보, 행정정보 공동이용과 개인 정보보호, 전자정부법제연구. 제1권 제2호, 행정자치부, 2006, 51면.

75) 강경근, 행정정보의 공동이용에 따른 법적 과제, 한국법제연구원, 2001, 10면.

76) 행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다.

77) 김일환, "전자정부구축에 따른 행정정보공동이용의 방식과 유형에 관한 고찰", 성균관법학 제19권 제1호, 성균관대학교 비교법연구소, 2007, 10면.

또한 행정정보공동이용은 정부기관의 능률성을 향상시킨다. 정부기관이 업무에 필요한 다양한 행정정보와 자료를 신속하고 정확히 입수·활용함으로써 조직의 능률성을 기할 수 있고, 부처간 협조를 통하여 부처이기주의를 극복할 수 있으며, 복잡하게 얽혀있는 타 부처와 상호 조정과 신속한 협조로 필요한 문제를 쉽게 해결할 수 있다. 나아가 데이터베이스를 저장해두고 공공기관간에 상호 활용함으로써 국민과 기업에 동일한 정보를 반복적으로 요구하지 않음으로써 서류제출 등의 부담을 경감하게 하여 국민의 편의를 도모한다.[78]

또한 국민의 정보접근의 평등과 정책결정에 대한 국민의 참여 강화를 고려해 보면 공동이용되는 정보가 다양한 목적으로 사용됨에 따라 다원적인 정보수집에 의하여 발생할 수 있는 사안별, 개인별 편차를 줄이고 이로써 평등의 원칙이 충실히 실현될 수도 있다.[79]

다. 행정정보공동이용의 분류

1) 분류의 필요성

행정정보를 공동이용함에 있어서 반드시 그 이용하는 정보를 먼저 분류할 필요가 있다. 그동안 행정정보 공동이용의 방식과 분류에 대한 연구가 법학에서 충분히 논의되지 않았지만 앞으로는 이에 관한 연구가 체계적으로 이루어져야만 한다.

왜냐하면 공동이용되는 행정정보 중에 개인정보에 해당하는 행정정보가 포함되어 있기 때문에 개인정보에 해당하는 행정정보를 공동이용하는 것은 곧 정보주체의 기본권인 자기정보관리통제권의 침해로 이어지기 때문이다. 개인정보가 공공행정기관간에 공동이용되면서 자신에 관한 정보의 수집과 이용에 대한 정보주체의 동의의 범주를 초월하거나 법률의 취지에 벗어나 개인정보가 이용될 수 있는 위험을 가중시키게 된다.[80]

결국 행정정보 공동이용을 통하여 각 행정기관이 보유하고 있는 정보를 제공받은 것은 새로운 개인정보를 수집하는 것과 다를 바 없다. 따라서

78) 강경근, 행정정보의 공동이용과 기본권, 아·태공법연구 통권 제10호, 아세아·태평양공법학회, 2002, 108-109면.
79) 한국전산원, 행정정보공동이용을 위한 법제전략 연구, 한국전산원, 2005, 12면.
80) 정부혁신지방분권위원회, 전자정부로드맵, 정부혁신지방분권 로드맵, 2003, 299면.

전자정부 구현 과정에서 필수적으로 나타나게 되는 개인정보의 공동이용이 그 정당성을 입증해야 하는 기본권 제한임을 분명이 인식하고 이에 따른 법제정비를 강구하는 것이 중요한 과제로 대두된다.[81]

행정정보공용이용의 대상이 되는 행정정보는 개인정보에 해당되는 행정정보와 개인정보에 해당하지 않는 행정정보로 나누고 있다.

2) 개인정보에 해당하는 행정정보

(1) 개인정보에 해당하는 행정정보의 분류

첫째, 공동이용되는 행정정보가 개인정보에 해당하느냐에 따라서 개인관련성 있는 행정정보와 개인관련성이 없는 행정정보(또는 물적 정보의 공동이용과 인적 정보의 공동이용)로 구분할 수 있다.

둘째, 개인정보에 해당하는 행정정보의 공동이용은 다시 민감한 개인정보의 공동이용과 비민감개인정보의 공동이용으로 구분할 수 있다.

셋째, 개인정보에 해당하는 행정정보의 원래 수집된 목적 외의 이용여부에 따른 분류, 즉 개인정보에 해당하는 행정정보를 원래 수집한 목적범위 내에서 공동이용 하는 경우와 원래 수집한 목적의 범위를 넘어서서 이용하는 경우로 나눌 수 있다.

(2) 정보이용주체에 따른 분류

행정정보 공동이용주체에 따른 분류는 정보의 이용자가 공공기관 또는 민관기관이냐에 따라 행해질 수 있고, 이는 다시 공공부문에서 행정기관 내에서 해당기관 부서간(행정기관 내부간)과 해당기관과 유사한 업무를 담당하는 유관기관(행정기관 상호간) 공동이용으로 구분할 수 있다. 또 해당기관과 다른 업무를 담당하고 있는 기관 및 행정기관과 다른 국가기관간(행정기관과 다른 기관 국가기관 및 공공기관 상호간 공동이용) 공공이용으로 구별할 수 있다. 또 공공부문과 민간부분간 공동이용 및 민간기관간 공동이용으로도 구분한다.[82]

3) 개인정보에 해당하지 않는 행정정보

행정정보공동이용은 정보공개의 여부, 이용방식, 이용대상의 종류, 이용

81) 김일환, 앞의 주 77), 16-17면.
82) 위의 논문, 16면.

용도의 유형에 따라 구분할 수 있다. 그리고 공동이용의 형태에 따라서 크게 온라인으로 하는 경우와 그렇지 않은 경우를 구분할 수 있으며, 최종용도에 따라 대국민 서비스, 정책결정, 기관의 내부관리로 구분할 수 있다. 그리고 물적 정보와 인적 정보, 공동이용의 주체에 따른 분류, 공동이용의 정도에 따른 분류, 공동이용의 형태에 따른 분류, 데이터의 가공 여부에 따른 분류, 서비스방식에 따른 분류 그리고 정보시스템 연계·통합방식에 따른 분류 등으로 나누어지기도 한다.[83]

2. 행정정보공동이용의 실제

가. 행정정보공동이용의 현황

1987년부터 시작된 제1차 행정전산망사업에서 행정정보공동활용을 위한 행정정보 관리체계 구축을 기본목표로 설정한 이래 행정정보공동이용을 위한 데이터베이스 구축은 지속적으로 강조되어왔다.[84] 행정정보공동이용은 유관기관간 정보를 공동으로 활용함으로써 재활용에 따른 중복투자를 방지하고, 주요정책의 수립에 필요한 정보를 지원하며, 범정부적 차원에서 부처별로 보유하고 있는 정보를 공동으로 활용하며, 나아가 대민서비스를 개선하기 위하여 추진되었다.

정보공동이용은 주로 ① 주민등록정보, ② 부동산정보, ③ 기업정보, ④ 세금정보, ⑤ 자동차정보 등 5대 분야를 중심으로 논의되었다. 구체적으로는 주민등록정보는 주민등록관리시스템에서, 부동산정보는 지적행정시스템, 필지중심토지시스템, 지적정보센터와 건축행정정보시스템, 토지관리정보체계시스템, 산업입지전산시스템 및 부동산등기정보시스템을 각각 활용하였다. 그리고 자동차정보는 자동차관리시스템, 이륜차관리시스템, 유관망관리시스템을 활용하였고, 기업정보의 경우는 대법원 사업정보등기시스템, 세금정보는 국세청 국세통합정보시스템을 각각 활용하였다.

이 중에서 주민등록정보는 행정안전부, 국토해양부, 국세청, 관세청, 경찰청 등 다음 <표 2>에서 보는 바와 같이 70여개 기관에서 활용되고 있

83) 이에 관한 자세한 설명은 위의 논문 12면 이하 참조.
84) 권건보, 앞의 주 74), 52면.

다. 그리고 부동산 정보는 개별공시지가, 거래정보, 개발부담금내역정보, 용도·지부관리 및 지식정보의 민원인 요구와 행정기관의 과세자료로 이용되고 있다. 또한 자동차정보는 차량기본정보, 소유자정보, 차량번호, 제원 및 자동차등록원부, 차적정보에 관련된 경우와 자동차등록통계자료, 저당·압류 등 민원인 요구정보가 있고, 그 외 자동차등록통계, 차동차세완납증명 등을 발급하고 있다.[85] 하지만 올해부터는 공동이용대상이 더 늘어날 전망이다. 행정안전부는 수요자 맞춤형 행정정보공동이용체계 기반 구축 사업이 완료됨에 따라 2010년 1월 4일, 서비스를 1차 개통해 행정정보공동이용 대상 민원 구비서류를 81종으로 확대하고, 구비서류를 제출하지 않아도 되는 행정정보공동이용 기관도 전체 행정기관인 59개 공공기관, 16개 시중은행 및 1개 교육기관 등 391개 기관으로 확대한다. 이번에 새로 추가되는 서비스 및 그 내용은 건강보험증, 건강보험자격득실확인서 등 2종의 공공기관 정보를 처음으로 포함하는 등 5개 기관이 보유하고 있는 10종을 추가해 총 81종(행정기관 정보 79종, 공공기관 정보 2종)의 구비서류를 공동이용하게 된다.

<표 2> 행정기관 및 공공기관의 공동이용 대상 행정정보

순	공동이용 대상 행정정보	보유기관
1	「국가유공자 등 예우 및 지원에 관한 법률」 제6조에 따른 국가유공자 및 그 유족 등의 확인에 관한 국가유공자등록 정보	국가보훈처
2	「특수임무수행자 지원에 관한 법률」 제6조 및 제19조에 따른 취업지원대상자 여부의 확인에 관한 취업지원대상자증명 정보	
3	「여권법」 제4조에 따라 발급한 여권에 관한 정보	외교통상부
4	「해외이주법」 제6조에 따른 해외이주신고에 관한 정보	
5	「재외동포의 출입국과 법적 지위에 관한 법률」 제7조 제5항에 따른 국내거소신고사실증명에 관한 정보	법무부
6	「출입국관리법」 제88조 제1항에 따른 출입국에 관한 사실증명 정보	
7	「출입국관리법」 제88조 제2항에 따른 외국인등록사실증명에 관한 정보	
8	「부동산등기법」 제14조 및 제41조의2 제1항 제4호에 따라 작성된 외국인부동산등기등록의 증명에 관한 정보	
9	「인감증명법」 제4조에 따른 개인 인감증명에 관한 정보	행정자치부
10	「상훈법」 제2조에 따른 상훈수여의 증명에 관한 정보	
11	「주민등록법」 제7조에 따른 주민등록표에 관한 정보	
12	「지방세법」 제38조 제2항에 따른 지방세 납세증명서에 관한 정보	

85) 이에 관한 자세한 설명은 행정자치부, 전자정부법의 이해와 해설: 「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률」, 행정자치부, 2001; 권건보, 앞의 주 74), 53면.

13	「지방세법」 제196조의3에 따른 자동차세의 납부의무가 있는 자에 대한 과세증명에 관한 정보	
14	「지방세법」 제195조에 따른 토지의 재산세과세대장에 관한 정보	
15	「지방세법」 제195조에 따른 건축물의 재산세과세대장에 관한 정보	
16	「지방세법」 제195조에 따른 주택의 재산세과세대장에 관한 정보	
17	「지적법」 제2조 제1호가목에 따른 토지대장에 관한 정보	
18	「지적법」 제2조 제1호가목에 따른 임야대장에 관한 정보	
19	「지적법」 제2조 제1호가목에 따른 지적도에 관한 정보	
20	「지적법」 제2조 제1호가목에 따른 임야도에 관한 정보	
21	「산업집적 활성화 및 공장설립에 관한 법률」 제16조에 따른 공장등록에 관한 정보	산업자원부
22	「광업법」 제43조에 따른 광업원부에 관한 정보	
23	「대외무역법」 제14조 제2항에 따른 수입승인에 관한 정보	
24	「석유 및 석유대체연료 사업법」 제10조에 따른 석유판매업의 등록에 관한 정보	
25	「국민기초 생활 보장법」 제2조 제2호에 따른 국민기초생활 수급자에 관한 정보	보건복지부
26	「장애인복지법」 제29조에 따른 장애인등록에 관한 정보	
27	「오수·분뇨 및 축산폐수의 처리에 관한 법률」 제24조의2에 따른 축산폐수배출시설설치허가 및 신고에 관한 정보	환경부
28	「폐기물관리법」 제24조 제2항에 따른 사업장폐기물배출 신고에 관한 정보	
29	「국가기술자격법」 제13조에 따른 국가기술자격증에 관한 정보	한국산업인력공단
30	「건설기계관리법」 제3조 제3항에 따른 건설기계등록증에 관한 정보	건설교통부
31	「건설기계관리법」 제7조에 따른 건설기계등록원부에 관한 정보	
32	「건설산업기본법」 제9조에 따른 건설업의 등록에 관한 정보	
33	「건설기계관리법」 제13조 제4항에 따른 건설기계검사증에 관한 정보	
34	「건설기계관리법」 제21조에 따른 건설기계사업의 신고에 관한 정보	
35	「건축법」 제8조 제1항에 따른 건축허가에 관한 정보	
36	「건축법」 제18조 제2항에 따른 건축물 사용승인서에 관한 정보	
37	「건축법」 제29조에 따른 건축물대장에 관한 정보	
38	「건축사법」 제23조에 따른 건축사 업무의 신고에 관한 정보	
39	「토지이용규제 기본법」 제10조 제1항에 따른 토지이용계획확인서에 관한 정보	
40	「부동산가격공시 및 감정평가에 관한 법률」 제11조에 따른 개별공시지가에 관한 정보	
41	「자동차관리법」 제7조에 따른 자동차등록원부에 관한 정보	
42	「자동차관리법」 제8조 제2항에 따른 자동차등록증에 관한 정보	
43	「자동차관리법」 제48조 제1항에 따른 이륜자동차의 사용신고에 관한 정보	
44	「주택법」 제29조 제1항에 따른 주택 또는 대지의 사용검사에 관한 정보	
45	「선박법」 제8조에 따른 선박국적증서에 관한 정보	해양수산부
46	「선박법」 제26조의2에 따른 선적증서원부에 관한 정보	
47	「선박안전법」 제9조 제1항에 따른 선박검사증서에 관한 정보	
48	「수산업법」 제8조에 따른 어업면허에 관한 정보	
49	「어선법」 제13조에 따른 어선의 등록에 관한 정보	

50	「해양오염방지법」 제23조 제1항에 따른 폐기물 위탁처리자의 신고에 관한 정보	
51	「소득세법」 제76조, 「부가가치세법」 제18조 및 제19조에 따른 세액의 납세사실에 관한 정보	국세청
52	「소득세법」 제4조에 따른 거주자의 소득금액 증명에 관한 정보	
53	「부가가치세법」 제5조에 따른 휴업사실에 관한 정보	
54	「부가가치세법」 제5조에 따른 폐업사실에 관한 정보	
55	「국세징수법」 제6조에 따른 납세증명서에 관한 정보	
56	「법인세법」 제111조 및 「부가가치세법」 제5조에 따른 사업자등록에 관한 정보	
57	「관세법」 제248조 제1항에 따른 수출입신고에 관한 정보	관세청
58	「병역법」 제5조 제3항에 따른 병적관리에 관한 정보	병무청
59	「도로교통법」 제80조에 따른 운전면허에 관한 정보	경찰청
60	「특허법」 제185조에 따른 특허원부에 관한 정보	특허청
61	「실용신안법」 제18조에 따른 실용신안등록원부에 관한 정보	
62	「디자인보호법」 제37조에 따른 디자인등록원부에 관한 정보	
63	「상표법」 제39조에 따른 상표원부에 관한 정보	
64	「부동산등기법」 제14조에 따른 건물등기부에 관한 정보	대법원
65	「부동산등기법」 제14조에 따른 토지등기부에 관한 정보	
66	「부동산등기법」 제41조의2에 따른 부동산등기용등록번호에 관한 정보	
67	「상업등기법」 제5조에 따른 법인등기부에 관한 정보	
68	「상업등기법」 제11조에 따른 법인의 인감에 관한 정보	
69	「호적법」 제10조 및 제124조의4에 따른 호적부에 관한 정보	
70	「호적법」 제14조에 따른 제적부에 관한 정보	

나. 행정정보공동이용의 절차 및 방법

1) 행정정보공동이용의 절차

(1) 행정정보공동이용계획 및 수립

「전자정부법」과 시행령에서 규정하고 있는 행정정보공동이용의 절차는 다음과 같다. 먼저 중앙사무관장기관의 장[86]은 행정기관이 전자적으로 생산·유통·저장하고 있는 행정정보를 조사하여 목록을 작성하여 행정기관에 배포하고, 행정기관이 공동이용을 필요로 하는 정보에 대한 수요를

86) 중앙사무관장기관의 장이라 함은 국회 소속기관에 대하여는 국회사무총장, 법원 소속기관에 대하여는 법원행정처장, 헌법재판소 소속기관에 대하여는 헌법재판소사무처장, 중앙선거관리위원회 소속기관에 대하여는 중앙선거관리위원회사무총장, 중앙행정기관 및 그 소속기관과 지방자치단체에 대하여는 행정안전부장관을 말한다(전자정부법 제2조 제3호).

조사할 수 있다. 또 행정안전부장관은 조사를 위하여 필요하다고 인정하는 경우에는 행정기관에 필요한 자료의 제출을 요청하거나 행정정보의 공동이용실태를 확인할 수 있으며, 조사결과에 따라 행정정보공동이용계획을 수립하고 정보화전략위원회의 심의를 거쳐 이의 시행에 필요한 조치를 할 수 있다. 행정안전부장관은 행정정보공동이용계획을 수립하는 때에는 ① 행정기관의 정보파일 보유현황 및 구축계획, ② 공동이용하고 있거나 또는 공동이용할 필요가 있는 정보파일의 명칭·보유기관·이용목적·이용범위·이용기간 및 소요예산 등의 현황, ③ 행정정보의 제공거절 또는 행정정보의 제공중단·이용금지 등의 경우 해당 정보파일의 명칭·보유기관·제공요청기관·이용범위·거절사유·이용금지사유 등의 현황 등을 고려하여야 한다.

(2) 행정정보제공의 요청 및 제공

행정기관의 장은 그 소관업무를 수행함에 있어서 다른 행정기관이 보유·관리하는 행정정보를 이용할 필요가 있는 경우에는 그 보유기관에 대하여 이용목적을 밝혀 해당 행정정보의 제공을 요청할 수 있는데, 이 제공요청은 필요한 최소한의 범위에 한정하여야 한다. 그리고 행정정보의 제공요청을 받은 행정기관의 장은 정당한 사유가 없는 한 행정정보공동이용센터를 통하여 해당 행정정보를 제공하여야 한다.

(3) 행정정보의 제공중단 등

행정기관의 장은 일정한 사유가 있는 경우에는 해당 기관에 대하여 행정정보의 제공을 중단하거나 이미 제공한 행정정보의 반환 및 그 이용의 금지를 요구할 수 있다. 그 사유는 ① 행정정보를 제공받은 기관이 행정기관의 장이 정한 행정정보의 이용목적, 이용범위, 그 밖의 행정정보의 이용·관리에 관하여 조건을 이행하지 아니함으로써 소관업무의 수행에 지장을 초래한 경우, ② 행정정보를 제공받은 기관이「전자정부법」제22조의3에서 정한 행정정보취급·이용자의 의무를 위반한 경우, ③ 그 밖에 행정정보의 제공을 중단하거나 이미 제공한 행정정보를 회수하고 그 이용을 금지하여야 할 불가피한 사유가 생긴 경우이다.

행정기관의 장이 행정정보의 제공중단 또는 이용금지를 하고자 하는 경

우에는 그 행정정보를 제공받고 있는 기관에 대하여 제공중단 또는 이용금지 10일전까지 그 사유를 명시하여 통지하여야 한다. 다만, 급박하거나 불가피한 사유가 있는 경우에는 그러하지 아니하다.

이러한 행정정보의 이용금지를 요구받은 기관의 장은 해당 행정정보를 복제 또는 복사하거나 부본 등의 형태로 계속 보유 또는 이용하여서는 아니 된다.

2) 행정정보공동이용의 방법

행정기관이 행정정보를 공동이용하기 위하여 정보통신망으로 다른 행정정보의 보유기관에 행정정보를 송신하는 방법은 ① 행정정보의 송·수신 과정에서 행정정보가 훼손·변조 또는 유출되지 아니하도록 행정전자서명 및 이에 상응한 보안기술을 적용하는 송신방법, ② 송신 중에 정보가 유출되더라도 행정기관 또는 해당 정보주체에게 위험이 보다 적은 송신방법, ③ 행정정보의 송신에 사용되는 정보통신망 회선 및 전송구간을 선택할 수 있는 경우 회선을 최소화하고 전송구간을 최단화하는 송신방법 등을 사용해야 한다.

그리고 행정기관 또는 공공기관 등은 다른 행정기관이 보유·관리하는 행정정보를 정보통신망을 통하여 제공받거나 이용하고자 하는 경우에는 그 행정기관과 공동이용에 관하여 협의를 한 후 행정정보공동이용센터와 ① 정보통신망·정보시스템·정보보호시스템의 구성방법 및 내용, ② 행정정보의 제공방법 및 정보전달체계, ③ 정보통신망의 연계에 따른 비용분담, ④ 그 밖에 정보통신망을 통한 행정정보의 공동이용을 위하여 사전에 협의가 필요한 사항을 협의하여야 한다.

다. 행정정보공동취급자와 이용자의 의무

「전자정부법」의 목적을 달성하기 위하여 공무원은 담당 업무를 전자적 처리에 적합하도록 개선하는데 최대한의 노력을 기울여야 하며, 담당 업무의 전자적 처리를 위하여 필요한 정보통신기술 활용능력을 갖추어야 한다. 그리고 공무원은 전자적으로 업무를 처리함에 있어서 국민의 편익을 행정기관의 편익보다 우선적으로 고려하여야 한다.

또한 행정정보취급·이용자는 누구든지 행정정보를 취급·이용함에 있어서 ① 행정정보의 처리업무를 방해할 목적으로 행정정보를 변경하거나 말소하는 행위, ② 행정정보를 변경하거나 말소하는 방법 및 프로그램을 공개·유포하는 행위, ③ 행정기관에서 처리하고 있는 행정정보를 누설하는 행위, ④ 행정기관에서 처리하고 있는 행정정보를 권한 없이 처리하는 행위, ⑤ 행정기관에서 처리하고 있는 행정정보를 권한 없이 타인으로 하여금 이용하게 하는 행위, ⑥ 거짓 그 밖의 부정한 방법으로 행정기관으로부터 행정정보를 열람하거나 제공받는 행위를 하여서는 아니된다. 이를 위반한 경우 징역 또는 벌금형의 처벌을 받게 된다.

라. 행정정보공유추진단

정부는 인터넷 민원서류 위·변조 문제 및 행정업무의 기반이 되고 국민생활과 가장 밀접한 주민등록증명과 관련 민원업무의 개선을 위한 방안으로 행정정보공유추진단을 구성하였다. 이와 같은 행정정보공유센터 구축을 전자정부 역점사업으로 추진키로 한 데 이어 센터 및 행정정보공유시스템 구축계획을 구체화한 행정정보공유종합계획 수립에 착수하여 정보의 공유기반을 마련하였다. 또한 정보의 공유 및 확대를 위한 체계적 기반을 확보하기 위해「행정정보공유추진위원회 규정」을 2009년 12월 30일까지 한시법으로 제정했으나 규제개혁 중점과제로 추진 중인 행정정보공동이용 업무의 연속성과 안전성을 확보하고, 행정정보공동이용 중기전략계획을 원활히 추진하기 위해 2012년 12월 31일까지로 3년간 연장하였다. 이 규정의 주요내용은 다음과 같다.

먼저 행정기관간 행정정보의 공유를 확대하기 위한 사항에 관한 대통령의 자문에 응하기 위하여 국무총리 소속하에 행정정보공유추진위원회를 둔다. 이 위원회는 ① 행정정보의 공유를 확대하기 위한 정책의 수립·추진에 관한 사항, ② 행정정보의 공유를 확대하기 위한 법령·제도의 개선에 관한 사항, ③ 공유대상 행정정보, 행정정보의 공유 절차 및 공유대상 행정정보에 대한 접근권한 등 행정정보의 공유에 필요한 사항, ④ 행정정보의 공유를 확대하기 위한 업무흐름의 재설계, 정보화추진 전략의 수립 및 시스템의 개발에 관한 사항, ⑤ 행정정보의 공유 현황에 대한 확인·

점검에 관한 사항, ⑥ 그 밖에 행정정보의 공유를 확대하기 위하여 필요한 사항 등을 심의 한다. 그리고 행정정보공유추진단은 ① 위원회의 심의안건 작성 등 회의 준비에 관한 사항, ② 위원회의 기능과 관련된 조사·연구 및 점검에 관한 사항, ③ 그 밖에 위원회의 업무 지원에 관한 사항 등의 사무를 처리한다.

이러한 정보공유추진으로 기대되는 효과는 다음과 같다. 첫째, 국민들이 체감하는 전자정부 서비스 질이 한층 더 높아지고 기관간에 정보의 흐름이 원활해지면 정부의 대국민 방문요청 횟수가 줄어들고 불필요한 서류를 제출하지 않고도 기관들 상호간에 업무를 처리하여 국민들이 편익을 제공받게 될 것이다.

둘째, 신속·정확한 정보교류로 정책수립의 적시성을 확보하여 생산성이 향상된다.

셋째, 이미 구축되어 있는 행정데이터베이스를 최대한 재활용함으로써 비용절감과 중복투자방지가 기대된다.

3. 행정정보공동이용 방법상의 문제점

가. 컴퓨터를 통한 개인정보공동이용의 위험성 문제

정보통신기술의 발달에 따라서 컴퓨터에 의한 자동정보처리는 엄청난 처리속도 및 상상을 초월하는 연결가능성을 낳는다. 그래서 자동화된 정보처리를 통하여 공간적으로 떨어져 있는 다른 정보에 순식간에 접근할 수 있으며, 그 결과 정보가 원래 저장되었던 목적과는 다른 목적으로 이용될 위험성 및 자동 정보결합 가능성이 높다.[87]

나. 개인정보 수집과정에서의 문제점

1) 수집근거의 문제

개인정보를 공동이용함에 있어서 수집제한의 원칙이 지켜져야 한다. 이에 관해서는「공공기관의 개인정보보호에 관한 법률」제4조 제1항에서 공

87) 미래사회연구포럼, 개인의 사생활, 국가적 감시, 그리고 규범, 미래사회연구포럼, 2007, 121-122면.

공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다고 규정하고 있다.

하지만 명확한 법적인 근거 없이 개인정보를 수집·관리하는 경우가 많이 있다. 따라서 개인정보공동이용에 있어서 데이터 주체의 인지나 동의에 의한 개인정보의 수집의 원칙이 침해될 위험이 확대된다. 더 나아가 정보의 주체로부터 직접 수집하기보다는 다른 파일이나 타 조직이 구축해 놓은 개인정보를 활용하는 것을 특징으로 하기 때문에 이러한 동의를 얻기가 어려울 뿐만 아니라 형식화될 위험이 상존하다.[88]

2) 수집목적의 구체성 문제

개인정보는 수집당시에 그 목적이 구체화되어야 하고 목적의 범위 내에서만 사용되어야 한다. 그러나 행정정보공동이용의 경우에는 목적 구체성의 원칙을 위반할 위험이 있다. 공동이용을 전제로 하지 않는 정보시스템의 경우 수집된 개인정보는 관련 업무의 특성에 맞게 정리·분류·관리하게 된다.

일반적으로 컴퓨터로 처리하게 되면 정보를 표준화·일반화함으로써 정보와 사실간 괴리를 확대하게 되고, 이러한 괴리는 행정정보공동이용에 의하여 더욱 심화될 수 있다.

다. 행정정보 중에 있는 개인정보의 관리상의 문제

1) 개인정보자료 질의 문제

행정정보공동이용의 자료로 활용되는 개인정보를 공공기관에서 관리하는 경우, 개인정보의 질이 확보되지 못하면 의사결정의 오류가 발생하게 된다. 특히 행정정보공동이용에서 개인정보가 부정확하고 질이 낮을 경우 의사결정과정에서 오류가 기하급수적으로 반복되는 폭포화현상이 발생하게 된다.

2) 개인정보자료의 안전성 확보문제

공공기관에서 보유·관리하는 개인정보자료는 그 상실이나 부당한 접

88) 박홍윤, 공공기관 개인정보의 공동이용에 있어서 문제점과 정책적 과제, 정보통신부, 2002, 80면.

근, 파괴, 이용, 수정 또는 공개와 같은 위험으로부터 적절한 안전장치에 의하여 보호되어야 한다. 하지만 개인정보를 공동이용하는 경우 공동이용 시스템이 가지는 네트워크화, 분산 시스템의 운영, 사용자 중심의 시스템 운영, 온라인에 의한 데이터의 처리 등에 의하여 데이터의 안전성 문제는 지속적으로 증가될 수 있다.

라. 개인정보의 이용에 있어서의 문제점

1) 이용제한의 문제

행정정보공동이용은 본래 이용제한이 아니라 이용의 활성화에 있기 때문에 개인정보를 보호하기 위한 이용제한의 원칙과는 상반되는 목적을 가진다. 행정정보공동이용 시스템의 구축으로 개인정보의 이용률이 높아지면 그 만큼 남용의 위험성[89]도 커지기 때문에 이용제한의 필요성이 크다고 할 수 있다.

2) 비맥락적 의사결정과 도식적 정보처리의 문제

비맥락적 의사결정은 데이터가 가지는 의미를 정확하게 파악하지 못하고 의사를 결정하는 것을 의미한다. 행정정보에 포함되어 있는 개인정보를 공동이용함에 있어서 그 정보들을 표준화시킬 수밖에 없는데, 그럴수록 개인정보의 특성은 무시되고 사회적인 스키마(skimmer)에 의지하는 결정을 하게 된다. 특히 프로파일링에 의하여 창출되는 정보는 사실정보가 아닌 판단정보의 특성을 가지기 때문에 주관적인 해석의 가능성이 높아진다.

그리고 개인정보의 공동이용은 전후사정을 무시한 채 부분적 또는 불완전한 정보의 사용으로 특정 개인에 대한 잘못된 판단을 초래하여 정치적·경제적 활동에 치명상을 입히는 경우가 발생할 수도 있다. 더 나아가 틀린 정보 또는 특정 시점에 국한된 정보를 이용하여 특정인을 잘못 인식하도록 만들어서 개인의 명예를 실추시키고 신용을 잃게 만드는 경우가 많이 발생할 수도 있다.[90]

89) 위의 책, 95면.
90) 위의 책, 98-99면.

마. 개인정보 관리체제에 대한 문제

1) 공개의 원칙에 따른 문제

개인정보 데이터의 개발, 활용, 정책들은 일반에게 공개되어야 한다. 이를 위해서는 개인정보 데이터의 존재와 성격 그리고 주요한 이용 목적 및 데이터의 관리통제자를 명확히 하고 권한과 책임의 소재를 명확히 해야 한다.

그러나 개인정보를 공동이용하는 경우에 개인들은 자기의 정보가 조직에서 어떻게 이용되고 있는지를 확인하기는 어렵다. 그리고 정보관리체계가 기본적으로 복잡한 구조를 가지고 있기 때문에 집행 또는 처리과정에서 권한이나 책임의 근거를 명확히 하는 것은 어렵고 그만큼 개인정보의 침해가능성이 크다고 할 것이다.

2) 개인참여 원칙에 대한 문제

정보의 주체는 정보의 관리자나 통제자로부터 자신과 관련된 자료를 얻거나 그 밖의 자신에 대한 정보를 데이터 통제자가 가지고 있는지를 확인할 권리를 가지고 있다. 그러나 개인정보의 전산처리로 인하여 조직이 개인에 대하여 보다 많은 권력을 행사할 수 있게 하고 결정이 내려진 맥락을 이해할 수 없도록 하기 때문에 개인은 결정이 이루어진 뒤에야 비로소 부당한 처리가 있었음을 알게 되거나 또는 알지 못하고 지나갈 수 있다. 그리고 공동이용에서 개인은 통제 대상조직을 식별하는 것이 용이하지 않으므로 개인정보의 오류에 대하여 수정·정정·삭제권의 행사가 어렵다. 더욱이 이들 과정이 여러 개의 조직과 연결되어 있으므로 권리행사의 과정이 복잡하여, 많은 시간과 비용을 수반하게 된다.

3) 책임의 원칙에 따른 문제

행정정보공동이용에 있어서 개인정보를 공동으로 이용하고 목적 이외의 이용이 증대함으로 컴퓨터 결과를 바탕으로 한 결정의 책임을 명확하게 하기가 쉽지 않다. 특히 네트워크화로 인하여 기밀정보에 대한 어느 한 조직의 책임은 감소되고 책임을 다른 조직이나 컴퓨터에 전가시키게 되는 경향이 커질 수 있다.

한편, 행정정보공동이용과 관련한 법률들에서는 개인정보보호의 원칙

에 대한 예외조항을 지나치게 많이 규정하고 있어 사실 공공기관에서의 개인정보보호는 기대하기 어렵다.

현실적으로 컴퓨터 매칭, 프로파일링(profiling), 신원조회 등이 많이 이루어지고 있어, 개인의 기본권인 자기정보관리통제권을 침해할 위험이 많다고 할 수 있다. 실제로 국가정보원, 경찰, 검찰과 국세청이 행정정보 공동이용 관련 법률 및 개인정보보호 관련 법률들의 예외적인 조항에 의해 사실상 무제한적으로 행정정보를 이용할 수 있다고 생각된다.

4. 행정정보공동이용 절차상의 문제점

「전자정부법」제11조에서 행정정보공동이용의 원칙을 규정하면서, 제21조 제1항 제3호에서「공공기관의 개인정보보호에 관한 법률」(이하「개인정보보호법」이라 함) 제10조 제3항[91]의 규정에 의하여 다른 기관에 제공할 수 있는 '처리정보'도 공동이용의 대상이 된다고 명시하고, 있어 개인정보도 공동이용의 대상이 된다고 할 수 있다.

개인정보보호에서 다른 기관에 제공할 수 있는 사유가 매우 폭넓게 설정되고 있어서 결과적으로 공동이용이 매우 용이해지는 문제가 있다. 특히 제3항 제2호에서 "처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 제20조[92]에 따른 공공기관개인정보보호심의위원회의 심의를 거

91)「공공기관의 개인정보보호에 관한 법률」제10조제3항 보유기관의 장은 제1항의 규정에 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다. ① 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, ② 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 제20조에 따른 공공기관개인정보보호심의위원회의 심의를 거친 경우, ③ 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, ④ 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우, ⑤ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 이용하게 하거나 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, ⑥ 범죄의 수사와 공소의 제기 및 유지에 필요한 경우, ⑦ 법원의 재판업무수행을 위하여 필요한 경우이다.

92) 위원장은 행정안전부차관으로 하고, 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자 중에서 위원장의 추천으로 국무총리가 임명 또는 위촉한다.

친 경우"라고 규정하고 있는데 이는 이 법이 개정되기 전, 이 법 제2항 제2호에서 규정하였던 "처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 제20조에 따른 공공기관개인정보보호심의위원회의 심의를 거친 경우"보다는 다소 차이가 있지만, 역시 큰 차이는 없다고 하겠다. 따라서 이 규정은 자칫 행정기관 상호간에 큰 걸림돌 없이 개인정보를 공동이용할 수 있도록 하고 있다.

물론「개인정보보호법」제10조 제2항에서 정보주체나 제3자의 권리와 이익을 부당하게 침해할 우려가 있으면 공동이용을 제한하고 있다. 하지만 각 행정기관의 활동 가운데 법률에서 정하는 소관업무의 수행이 아닌 것이 거의 없다. 또 어떤 정보가 공유되지 아니하면 소관 업무를 수행할 수 없는 경우인지도 명확하지 않다. 따라서 이 규정 역시 명확성의 결여라고 보인다. 또 제20조에 따른 공공기관개인정보보호심의위원회의 심의를 거친 경우라고 하는데, 위원장은 행정안전부차관으로 하고 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자 중에서 위원장의 추천으로 국무총리가 임명 또는 위촉하고 있는데 그 위원회가 심의한 기준에 신빙성이 있을지 의문이다. 공공기관의 직원이야 말할 것도 없지만 학식과 경험이 풍부한 자의 기준이 명확하지 않다. 이러한 문제들에 비추어 볼 때 행정정보공동이용에 있어서 개인관련 정보의 공동이용 부분에 대해서는 허용조건을 보다 엄격하게 규정하여 국민의 기본권인 자기정보관리통제권을 확고하게 보장하여야 한다.

5. 개인정보의 침해 위험성

행정정보공동이용이 활성화되면 행정정보 중에 있는 개인정보의 침해문제가 심각하게 부각될 수 있다. 일반 행정정보에 개인정보가 포함되어 통합될 경우 실로 다양하고 방대한 정보가 축적되므로 악의적 목적을 가지고 정보에 접근할 경우 심각한 피해가 발생한다. 예컨대 해커들이 공공기관의 컴퓨터에 침입하여 개인정보를 빼내어 악용하는 경우 등이다.

「개인정보보호법」은 개인정보의 수집에 있어 공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를

수집하여서는 아니된다고 규정하고 있지만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 예외로 규정하고 있어 정보주체의 동의가 없더라도 제공할 수 있도록 하고 있어서 개인정보의 침해위험성이 아주 크다고 할 수 있다.

그리고 한 번 수집된 개인정보는 유출 혹은 남용될 가능성을 배제할 수 없고, 개인정보에 접근할 수 있는 자가 많아질수록 그 만큼 개인정보의 유출이나 남용으로 인한 개인정보의 침해가 증가할 수밖에 없다.

6. 행정정보공동이용의 개선방안

전술한 바와 같이「전자정부법」은 행정업무의 전자적 처리를 위한 기본원칙·절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것을 목적으로 전자정부의 전자행정에 관한 일반법으로 제정되었다. 그러나 전자행정에 관한 모든 사항을 규율하고 있는 것도 아니고, 추상적인 원칙 규정과 세부적인 절차규정이 혼재되어 있어, 기본법으로서의 면모가 미흡하다고 할 수 있다. 따라서 현행「전자정부법」을 전자행정에 관한 일반법의 성격으로 다시 전반적인 내용을 개정할 필요가 있다.

「전자정부법」제11조의 행정정보공동이용의 원칙에서 행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다고 규정하고 있는데, 이 조항에 근거하여 행정정보가 공동이용되고 있으므로 이 조항이 기본법의 성격을 가진다고 할 수 있다. 그렇다면 행정정보공동이용을 위해 이러한 추상적인 내용을 구체화할 개별법이 신설되어야 한다.

전자정부의 활성화를 위하여 첫째, 전자정부 고도화단계에서 기존의 개별부처 중심의 사업이 다수 부처간에 연계·통합사업으로 확산되고 있고, 다수의 공공기관들에서 운영하는 정보시스템간의 연계 및 통합이 확산됨에 따라 정보시스템의 복잡성 내지 중복성이 증가되고 있어 통합적 정보자원관리체계를 구축할 필요가 있다.

둘째, 전자정부 표준화와 관련하여 전자정부 시스템의 유기적인 연계·통합 시스템체계가 요구된다. 통합체계를 통하여 행정정보공동이용이 이루어져야 하며, 이러한 정보시스템의 상호연계 행정정보가 공동이용할 때는 이에 사용되는 데이터, 코드, 시스템 등이 규정된 기준에 따라 구축되어야 한다.

셋째, 행정정보공동이용의 활성화를 위해서는 행정의 효율성, 국민 권리실현의 안전성·신속성, 데이터구축 비용의 절감, 중복투자방지 등에 필요한 제도와 효율성 극대화를 위해 규율체계를 마련함이 바람직할 것이다.

넷째, 전자정부 보안성과 관련하여 현행「전자정부법」제12조에서 개인정보의 보호에 관해서는 원칙을 정하고 있으나, 일반정보의 보안에 관한 규정이 없는 실정이다. 날로 발전해가는 정보통신기술과 법령간의 격차가 발생할 경우 침해행위에 대한 우려와 규제의 공백이 발생할 우려가 있다. 따라서 개인정보보호의 강화와 일반정보의 보안성을 위한 규정이 필요하다.

다섯째, 개인정보강화와 관련하여「전자정부법」제12조에서 행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니 된다고 규정하고 있으나 이는 일반적 추상적 규정일 뿐이다. 이에 관해서는 현행「전자정부법」에 규정하는 것보다는 행정정보공동이용에 관한 법률을 제정하여 구체적인 내용, 방법, 절차, 범위 등을 설정하는 것이 필요하다.

여섯째, 정보의 수집, 특히 개인정보의 수집·활용·보유와 관련하여, 전자행정을 실현하기 위하여 가장 우선적으로 실행되어야 하는 것이 정보의 수집일 것이다. 물론 여기에는 개인정보의 수집은 말할 나위도 없다. 그런데 현행 법률에서는 일반정보의 수집과정은 물론 개인정보의 수집과정에 대해서 구체적인 언급이 없다. 따라서 일반정보는 차치하고라도 개인정보의 수집에 관해서는 명확한 목적, 사용처, 한계 등을 상세히 규정하여야 한다. 수집·보유하고 있는 개인정보를 이용하지 않는 동안의 잠재적 위험, 수집당시의 목적과 연계성 확인, 공동이용방법 이외의 대안적인 방법은 없는지에 대한 분석, 공동이용을 정당화하기 위한 비용·편익 등을 분석할 필요가 있다.

일곱째, 행정정보의 범위와 관련하여「전자정부법」에서는 행정정보라 함은 행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전

자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것을 말한다고 하여 정보의 공동이용 범위를 설정하고 있으며, 행정기관은 ① 민원사항의 처리를 위하여 필요한 행정정보, ② 통계정보·문헌정보 등 행정업무의 수행에 참고가 되는 행정정보, ③「공공기관의 개인정보보호에 관한 법률」제10조 제3항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보에 대하여 공동이용을 할 수 있도록 하고 있다. 그런데 여기서 말하는 모든 정보가 공동이용대상의 범위에 해당하지도 않는다. 또 민원사항의 처리를 위하여 필요한 행정정보라고 하는데, 민원사항의 처리를 위하여 필요한 행정정보에 대한 기준설정이 문제이다. 다음으로 통계정보·문헌정보 등 행정업무의 수행에 참고가 되는 행정정보인데, 일반적으로 어떤 것이 통계정보나 문헌정보인지는 알 수 있으므로 크게 문제가 되지는 않는다. 그리고「공공기관의 개인정보보호에 관한 법률」제10조 제3항의 규정의 추상적인 표현들은 일부개정을 통하여 수정이 이루어져 크게 문제가 되지는 않는다. 그러나「국가정보화기본법」제12조 제2항 제2호에서 말하는 "행정정보공동이용에 관항 사항"에서는 공동이용의 대상은 정보화책임관협의회의 결정을 통하여 그 내용 및 범위가 확정되기 때문에 여전히 개인의 법적안정성과 예측가능성이 부족한 규정이다. 따라서 이러한 문제들을 해결하고 구체적인 대상과 범위를 확정할 수 있는 법률을 제정하는 것이 필요하다.

여덟째, 수집된 개인정보의 관리과정과 관련하여 ① 최신성, 정확성, 신뢰성을 담보할 수 있는 데이터의 질을 확보할 방안이 강구되어야 하고, ② 개인정보 중에서도 민감한 정보는 분리하여 특별 관리하여야 한다. 이를 위해서는 공공기관의 비밀분류에 대한 규정과는 다른 차원에서 개인정보의 등급제와 이에 상응하는 보호수준을 정할 필요가 있다. ③ 그리고 개인정보를 공동 활용함에 있어 관련 당사자의 사전 동의 또는 소명기회를 제공하는 절차적 제도가 규정될 필요가 있다.

아홉째, 개인정보의 이용에 대한 통제과정과 관련하여 공동이용에 관하여 행정안전부장관과 정보화추진위원회가 있고 개인정보보호와 관련하여서는「개인정보보호법」에서 공공기관의 컴퓨터 등에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의하기 위하여 국무총리소속하에 공공기관개인정보보호심의위원회를 둔다는 규정을 두고 있지만, 이들 기관은 개인정보의 이용에 대한 심의권한만 가지고 있어, 책임성 확보를 위한 기능

은 거의 없고, 단지 통보만 할 뿐 통제력은 거의 없다. 또 그나마 심의권한과 결정권한이 분리되어 있어 실효성이 확보되지 않음은 물론이고, 상호 이견이 발생할시 정책의 혼선이 우려된다. 따라서 개인정보보호를 위한 독립기관의 설치가 요구된다.

열째, 공개의 문제와 관련하여 개인은 조직의 정보활동에 참여하기 위해서 자신에 관한 정보가 어떠한 경로를 통하여 수집되고, 사용되어지며 유포되는지를 알 수 있어야 한다. 더 나아가 민주주의의 전제조건으로서 국민의 알 권리 보장과 정보공개청구권의 보장이 요구되며, 공개대상정보에 전자적 정보를 포함시키거나 전자적으로 공개된 정보를 획득할 수 있어야 한다.

특히「공공기관의 정보공개에 관한 법률」제7조에서 행정정보의 공표를 규정하고 있지만, 그 범위나 절차가 제한적이고 구체적인 기준이 마련되어 있지 않으며, 그 공표여부, 범위, 시기 등에 관한 구체적인 기준이 없어 공공기관의 재량사항으로만 규정되어 있어 실효성이 있다고 할 수 없다. 따라서 명확한 기준 설정이 요구된다.

열한 번째, 자기정보관리통제권과 관련하여 행정정보에 포함되어 있는 개인정보를 자기정보관리통제권의 제한과 한계라는 측면과 헌법적 측면에서 검토하고, 헌법 조화적 방안을 모색할 필요가 있다. 개인정보가 포함된 행정정보의 공동이용은 정부가 부여받은 수권임을 부인할 수 없다. 하지만 그 제한의 정당성도 필요최소한의 정도에서 정당화될 수 있다. 이러한 정당성을 부여받기 위하여 독립된 통합적인 개인정보보호기구를 설치하고 행정정보공동이용으로 인한 개인정보침해가 발생하지 않도록 사전, 사후 감독케 하는 것도 바람직한 방편이 될 수 있다. 또 앞서 언급한 미국의 경우처럼 개인관련 행정정보의 공동이용과 관련하여 사전영향평가제도의 도입을 하는 방안도 검토해 볼 필요가 있다.

제3장 전자정부하에서 행정정보공동이용과 개인정보보호

제1절 서설

행정기관은 행정의 주체로서 헌법과 법령에 따라 부여된 행정목적을 달성하기 위하여 사회 공공의 안녕과 질서의 유지에 필요한 조치를 하거나 행정의 대상이 되는 국민의 요구에 따라 행정의 수요자가 필요로 하는 서비스를 제공하는 등의 다양한 형식의 행정활동 행위를 하게 된다.[93]

그동안 국가는 각종의 국가목적에 필요한 자료를 조사하기 위하여 무수한 행정정보를 수집해왔으며, 그렇게 수집된 정보를 체계적으로 분류하여 보관하고 또 활용해오고 있다. 국민을 효과적으로 통치하는데 필요한 행정정보의 조사활동은 국가의 성립과 더불어 시작되었다고 할 수 있다. 국가의 유지와 존속을 위해서는 국민에게 국방과 조세의 의무를 부과하는 것이 필수적이었는데, 이것은 국민의 인구변동이나 소득상황에 대한 개략적 파악이 있을 때 가능하다.

근대사회에 있어서도 국가는 상비군의 구성원이 될 개인들의 신상을 파악하거나 개인의 기본적 인권을 정책과정에서 보장하기 위하여, 혹은 국가재정의 근간이 될 조세의 징수원을 확보하거나 관료에 의한 합리적인 국가경영을 위한 기초정보를 확보할 목적으로 시민들 개인에 관한 정보를 수집·처리하지 않으면 안 되었다. 이처럼 자율적인 존재로서 개인의 지위를 확보하기 위해 성립한 근대국가가 역설적으로 개인의 정보에 대한 국가의 통제력을 강화하는 방향으로 진행되어왔다고 할 수 있다.[94]

현대에 이르러 국가는 국방이나 외교 등 전통적인 행정업무 이외에도 경제적·사회적·환경적 위험이나 수요에 대처하기 위하여 교육, 사회, 안보 등의 영역에서 새로운 업무들을 적극적으로 수행해야 하는 상황에 처해 있다. 특히 사회복지국가의 이념은 개인의 후견인으로서 국가위상을

93) 심현정, "행정정보공동이용 제도에 대한 이해와 관련 법제의 발전방향", 법제 통권 제589호, 법제처, 2007, 87면.
94) 김종철, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론", 인터넷법률, 법무부, 2001, 26-27면.

보편화시켰으며, 그것은 국가로 하여금 개인의 일상생활에 대한 정보를 더욱 적극적으로 수집·처리하도록 하는 요인이 되었다. 특히 오늘날 대다수 국가가 행정의 효율성·공정성·과학화 등을 명분으로 하여 전자정부의 구축에 힘을 쏟고 있는 상황에서 개인정보의 관리능력이 전례 없이 강화되었다. 실제로 가족관계부나 주민등록, 토지대장, 금융거래의 내역, 부동산거래의 내역, 각종의 세무자료 등이 전산처리되면서 행정기관은 국민의 개인적 신상은 물론 경제적 사정까지도 상세히 파악할 수 있게 되었다.[95]

전자정부 구현의 취지와 핵심적인 기본이념을 간단히 두 가지로 요약하다면, 첫째, 정보기술을 이용한 정부혁신과 둘째, 정부가 국민을 정부의 고객으로 이해하는 고객지향적인 열린 정부라 할 수 있다.[96] 즉 국민을 정부의 고객으로 생각하여 국민의 편에서 여러 전자적 기술을 통하여 정부와 국민이 편리한 상호소통을 이루어보고자 하는 것이 전자정부 구현의 기본이념 중의 하나이다.[97] 이러한 전자정부의 기본취지의 이념하에 우리나라에서도 2002년 전자정부가 공식 출범함에 따라 전자정부 홈페이지를 개설하여 전자정부를 대표하는 허브 포털 사이트로 운영하고 있다.

이러한 전자정부의 구축에 따라 행정주체는 끊임없는 정보의 연결을 통하여 개인의 모든 일상적 정보에 대해서 낱낱이 파악할 수 있게 되었다. 이렇게 되면 정보주체는 자신의 정보가 누가, 어떤 목적으로 얼마만큼 처리·이용·전달하는지를 파악하기 곤란하고, 나아가 그러한 개인정보의 흐름을 자율적으로 통제하는 것이 불가능해질 수밖에 없다.[98] 또한 행정기관이 보유하고 있는 개인정보가 당초의 목적과 달리 이용될 경우 조사당시의 배경이나 기준 등을 충분히 인식할 수 없는 상태에서 자칫 개인에 관한 잘못된 인식과 평가에 기초한 행정작용이 이루어질 수 있고, 때로는 인격적 가치의 훼손 등과 같은 막대한 피해를 초래할 수도 있다.

이렇게 볼 때 행정정보공동이용의 활성화로 행정의 효율성과 편익성, 국민의 편익증대를 도모하는 것도 중요하지만, 그와 동시에 행정정보 가운데 개인관련성이 뚜렷하거나 민감성이 농후한 경우 그러한 정보의 공동

95) 권건보, 앞의 주 74), 49-50면.
96) 권기헌, 전자정부와 행정개혁, 커뮤니케이션북스, 1999, 171-172면.
97) 임지봉, "우리 전자정부법제의 현황과 개선방향", 국제헌법학회 한국학회, 2008, 248-249면.
98) 김일환, "개인정보보호법제의 정비방안에 관한 연구", 한국법제연구원, 1997, 118-119면.

이용에 일정한 제한을 가함으로써 개인정보의 침해라는 부작용을 최소화할 수 있는 방안을 함께 강구할 필요가 있다. 행정정보공동이용과 개인정보보호 중에 어느 한쪽을 일방적으로 강조하여 다른 한쪽을 희생시키는 형태보다는 서로 상충될 수 있는 두 가지의 법적 가치가 조화적으로 공존하는 가운데 각각의 기능을 극대화할 수 있는 방안을 모색하는 것이 가장 바람직할 것이다.[99]

이러한 기본적 인식하에 본장에서는 행정정보공동이용과 개인정보보호의 헌법적 기초를 고찰하고, 행정정보공동이용과 관련한 개인정보보호법제를 비교법적으로 고찰하여 문제점을 검토하고 그 개선방향을 모색하고자 한다.

제2절 전자정부와 개인정보보호의 실제

1. 개인정보공동이용과 개인정보보호

가. 개인정보의 개념과 유형

1) 개인정보의 개념

(1) 일반적인 개념

개인정보는 정보사회에서 보호가 필요한 정보의 하나로서 인식되고 있기 때문에 '개인정보보호'도 정보사회에 있어서 중요한 문제로 등장하고 있다.[100]

개인정보는 개인과 정보라는 용어가 합성된 단어로 이루어져 있으나, 이 가운데 전자는 일응 후자에 부가된 한정사의 의미로 이해될 수 있다 그런데 여기서 정보의 부분보다 개인의 부분에 논란의 소지가 엿보이고 있다. 정보(information)라는 개념의 규정이 그리 용이한 것은 아니지만 사전적으로는 사정이나 정황에 관한 소식이나 자료를 말한다.[101]

---

99) 권건보, 앞의 주 74), 51면.

100) 백윤철, "개인정보보호법(안)과 최근 입법동향 및 과제", 토지공법연구 제43집 제2호, 한국토지공법학회, 2009, 662면.

101) 민중 엣센스 국어사전, 민중서림, 2002, 2207면.

이러한 정보의 존재는 인류보다 더 오랜 역사를 가지고 있다고 할 수 있다. 인간이 생존하기 이전에 생물이 존재하면서부터 정보와 관련된 활동은 이루어져오고 있었다. 생물은 생존유지를 위해 끊임없이 외부로부터 그를 둘러싼 정황에 관한 소식을 얻고, 이를 식별·평가하여 외부환경에 대응하는 행동을 취해왔던 것이다. 그러다가 생물의 진화와 함께 정보의 개념도 복합화·고도화하여 인간의 경우에는 언어나 문자와 같은 고도의 정보매체가 생산되고, 마침내 정보는 인간이 사회생활을 유지하는데 필요불가결의 생활수단이 되었다.

정보는 무엇보다도 어떤 특정의 목적을 달성하기 위한 행동선택에 작용한다는 점에 그 효율성이 있으며, 논리적이고 예지적이라는 특징을 가지고 있다. 이러한 정보의 힘은 오늘날 정치·경제·사회·문화 등 모든 영역에서 일종의 권력으로 받아들여지고 있다.[102]

이러한 환경에서 논의의 대상이 되는 개인정보를 어떻게 정의하느냐가 매우 중요하다. 우선 개인정보는 개인을 특정할 수 있는 모든 정보로 정의할 수 있을 것이다. 개념에 관한 논의에서는 개인정보를 생존하는 사람에 대한 정보로 한정할 것인가 또는 법인의 경우도 포함할 것인가도 쟁점이 된다. 그러나 개인정보는 생존하는 자연인의 내면적 사실, 신체나 재산상의 특질, 사회적 지위나 속성에 관하여 식별되거나 또는 식별할 수 있는 정보의 총체를 일컫는 것으로 이해할 수 있다.[103]

한편, 레이먼드 왝스(Raymond Wacks) 교수는 개인정보를 개인에 관련되는 것으로 내밀하거나 민감하다고 여겨지기를 기대하고 그 결과 수집, 이용 또는 유통이 억제되거나 적어도 제한되기를 원할만한 사실, 통신 또는 의견이라고 정의하고 있다.[104] 그런데 이러한 정의는 법적 보호의 필요성에 대한 주관적 혹은 객관적 평가를 전제로 하는 것이라고 할 수 있다. 하지만 개인정보의 침해는 정보주체의 주관적 인식에 따라 다르게 평가될 수 있고, 같은 개인정보라 하더라도 그 처리방법이나 사용목적에 따라 그 결과가 달라질 수 있다. 따라서 개인정보의 개념을 선험적으로 확정하거나 그 종류를 명확하게 특정하는 대신 법적 보호의 범위를 가능한

---

102) 권건보, 개인정보보호와 자기정보통제권, 경인문화사, 2006, 8면.

103) 정영화, “인터넷상 개인정보보호 및 분쟁해결에 관한 연구”, 인터넷법연구 제1호, 한국인터넷법학회, 2002, 22면.

104) Raymond Wacks, Personal Information : Privacy and the Law, Oxford: Oxford University Press, p.26.(1989).

한 넓게 상정할 필요가 있다. 그렇다고 개인에 관한 일체의 사항을 개인정보로 파악할 경우 법적 보호의 대상이 되는 범위가 지나치게 확대되는 문제가 있다.

(2) 실정법상 개념

가) 외국의 경우

1995년 미국 클린턴 행정부가 창설한 정보인프라기획단(IITF: Information Infrastructure Task Force)이 제시한 개인정보의 제공과 이용에 관한 원칙(principles for providing and using personal information)에서는 개인정보(personal information)를 개인을 식별할 수 있는 정보(information identifiable to individual)로 정의하고 있다.[105] 그러나 연방입법에서는 정보의 내용이 각각의 법률제정 목적에 따라 세부적으로 정해져 있으므로 일반적인 정의를 찾기 어렵다. 다만「1998년의 아동 온라인 프라이버시보호법(Children's Online Privacy Protection Act)」에서는 개인정보를 개별적으로 식별 가능한 개인에 관한 정보로 정의하면서, 여기에는 성명, 주소, 이메일주소, 전화번호, 사회보장번호(social security number) 등을 포함한다고 규정하고 있다.[106]

영국의「1998년 데이터보호법(Date Protection Act 1998)」은 개인데이터(personal data)를 당해 데이터 및 데이터 관리자가 보유하고 있거나 보유할 가능성이 있는 데이터나 기타의 정보로부터 신원을 확인할 수 있는 생존하는 개인에 관한 데이터로 정의하고, 여기에는 개인에 대하여 표현된 의견이나 데이터관리자의 모든 지시사항, 그 사람과 관계있는 모든 타인에 관한 의견도 포함되는 것으로 규정하고 있다.

한편, 독일의「1990년 연방데이터보호법(Bundesdatenschutz-gesetz)」은 개인관련 데이터(Personenbezogene Daten)를 그 형식 여하를 불문하고 직·간접적으로 자연인의 신원을 확인할 수 있게 하는 정보로서 자연인 또는 법인에 의해서 처리되는 정보라고 정의하고 있다.

---

105) Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Washington D.C.October(1995),p.5. http://www.ntia.doc.gov/ntiahome/privwhitepaper.html, 2009.12.2. 방문.

106) 15 U. S. C. § 6501(8).

그리고 일본의 2003년「행정기관이 보유하는 개인정보의 보호에 관한 법률」은 개인정보를 생존하는 개인에 관한 정보로서, 당해 정보에 포함되어 있는 성명, 생년월일 기타의 기술 등에 의해 특정의 개인을 식별할 수 있는 것(다른 정보와 조합할 수가 있어서 그에 의하여 특정의 개인을 식별할 수 있는 것을 포함한다)으로 정의하고 있다.

또한 유럽연합(EU)의「1995년 개인정보보호지침(Directive 95/46/EC)」제1조에서도 개인정보를 자연인을 식별하거나 식별할 수 있는 모든 정보라고 정의하고 있다.[107]

나) 우리나라의 경우

전술한 바와 같이 일반적인 개인정보의 개념은 '개인에 관한 정보'를 뜻하지만, 법적 보호대상으로 고려되는 개인정보는 그보다 함의가 좁은 '개인 관련성'과 '식별 가능성'이란 두 가지 기준에 의해 제한되는 법기술적 개념이다.

먼저「공공기관의 개인정보보호에 관한 법률」제2조 제2호에서는 개인정보를 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보로 정의하고 있다. 물론 당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다. 즉, 개인정보는 '생존하는 개인을 식별할 수 있는 정보'로서 사망하였거나 사망으로 추정되는 자에 대한 정보는 보호대상이 아니라고 하겠지만, 사망자와 유족관계를 나타내는 정보는 유족에 대한 식별이 가능한 것으로 인정된다고 하겠다.[108]

그리고「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 제1항 제6호에 의하면, 개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보를 말한다고 규정하고 있다. 여기에는 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보도 포함된다.

또한「전자서명법」제2조 제13호에서도 개인정보라 함은 생존하고 있는

107) 권건보, 앞의 주 102), 15면.
108) 행정안전부, 공공기관 개인정보 보호 이해와 해설, 행정안전부, 2008, 23면.

개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다고 규정하고 있다.[109]

이러한 법률적 정의에 의하면, 개인정보는 성명·주민등록 및 그에 관한 사항과 같이 정보주체를 식별할 수 있는 정보뿐만 아니라 그 밖의 개인에 관한 정보라고 하더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 정보를 대상으로 하며, 개인에 관한 정보라고 하더라도 다른 정보와 용이하게 결합하여 해당 개인정보의 주체를 식별할 수 없다면 그것은 공공과 민간의 영역에서 법률상 보호되고 있는 개인정보로는 볼 수 없다고 할 것이다.[110]

이러한 법적 규정에 비추어 보면, 개인정보의 주체는 자연인이며, 법인이나 사자(死者)는 개인정보의 주체가 될 수 없다. 그리고 개인정보의 범위는 당해 개인을 직접 알아볼 수 있는 식별정보와 당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 비식별정보를 구분하고 있다. 이러한 현행 법률상의 개인정보는 헌법상의 개인정보자기결정권의 개념과는 일치되지 않는다. 즉, 헌법상 개인정보자기결정권에서 개인정보는 법률상 개인정보보다는 넓은 개념으로 이해하는데 반하여, 이들 법률에서는 좁은 개념으로 이해하고 있다.[111] 그리고 현행법상 개인정보의 주체를 자연인에 한정하고 있으나, 정보화시대에 있어서 개인정보의 침해는 자연인뿐만 아니라 법인에게도 발생하므로 개인정보의 법률적 개념의 주체를 확대시킬 필요가 있다.

2) 개인정보의 유형

---

109) 총무처, 축조해설 개인정보보호법, 총무처, 1994, 31면.

110) 이에 대하여 권건보 교수는 법률상 정의에 의할 때 개인정보는 직접식별개인정보와 간접식별개인정보로 대별하면서 "그 주인공이 누구인지 판명될 수 있다면 역시 개인정보라 할 수 있다"(권건보, "유비쿼터스 컴퓨팅 시대의 개인정보침해와 법적 대응방안", 공법연구 제32집 제5호, 164면)고 하는 반면, 정준현 교수는 "고도의 과학기술이 접목되어야 비로소 알 수 있다면 그것은 법상 보호되는 개인정보로 볼 수 없다"(정준현, "개인정보의 보호와 그 활용에 관한 소고", 토지공법연구 제43집 제2호, 한국토지공법학회, 2009, 718면)고 한다.

111) 백윤철, 앞의 주 100), 663면.

일반적으로 성명, 주소, 생년월일 등을 통해 특정의 개인을 식별할 수 있다. 따라서 성명, 주소, 생년월일 등의 요소가 포함되어 있는 정보는 특정 개인을 식별하는 정보에 해당한다고 할 수 있다. 또 그러한 요소가 원래부터 기재되어 있지 않았거나 기재되었다가 삭제·말소되었다고 하더라도 당해 정보 중의 다른 부분으로부터 특정의 개인이 추측된다거나 다른 정보와 결합함으로써 특정의 개인이 추측되는 경우 그러한 정보에 대해서는 특정의 개인이 식별될 가능성이 있다고 할 것이다. 따라서 사상, 신조, 종교, 양심, 가치관, 체력, 건강상태, 신체적 특징, 질병경력, 학력, 전과, 직업, 자격증, 소속정당이나 단체, 재무금융상태, 소득, 채권채무관계, 소유부동산 등도 개인정보에 해당될 수 있다.[112]

개인정보에 속하는 사항들을 구체적으로 유형화해보면, 개인의 일반정보(성명, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적), 가족정보(가족구성원의 이름, 직업, 생년월일, 주민등록번호, 출생지), 교육정보(최종학력, 출신학교, 성적, 자격증, 서클활동, 상벌상태), 병역정보(군번 및 계급, 제대유형, 주특기, 근무부대), 부동산 및 동산정보(소유주택 및 토지, 자동차, 저축현황, 현금카드, 주식 및 채권, 수집품, 고가의 예술품, 보석), 소득정보(연봉, 소득의 원천, 소득세 지불현황), 수익정보(보험가입 현황, 수익자, 회사의 판공비), 신용정보(대출잔액 등 지불현황, 저당, 신용카드, 담보설정 여부), 고용정보(고용주, 회사주소, 상관의 이름, 직무수행 평가기록, 교육기록, 상벌기록), 의료정보(가족 병력기록, 신체장애, 혈액형), 법적정보(전과기록, 구속기록, 이혼기록), 조직정보(노조가입, 정당가입, 클럽회원, 종교단체 활동), 습관 및 취미정보(흡연, 음주량, 여가활동, 도박성향, 비디오대여기록) 등으로 열거해 볼 수 있을 것이다.[113]

나. 개인정보공동이용의 개념과 목적

1) 개인정보공동이용의 개념

스넬런(Ignace Th. M. Snellen)[114]은 공공조직의 정보관리체계의 발전과

112) 권건보, 앞의 책, 18면.
113) 홍성찬·황인호, “프라이버시권에 있어서의 개인정보보호에 관한 연구”, 사회과학연구 제14권 제1호, 건국대학교 사회정책연구소, 2001, 23면.

정을 다섯 단계로 구분하여 설명하고 있다. 제1단계는 일상 업무나 단위 업무에서의 정보기술도입단계이고 제2단계는 단위업무간의 연결단계이며, 제3단계는 정부조직계층간 공동이용시스템을 구축한 통합적 운용단계이다. 그리고 제4단계는 주민이 직접 관공서를 방문하지 않고도 자신이 원하는 정보를 취득할 수 있는 네트워크 단계이고, 제5단계는 국가간 그리고 세계적인 네트워크 단계를 말한다. 개인정보공동이용은 전자정부의 행정정보공동이용의 개념에 포함되는 제3단계 이상의 단계에서 특징으로 나타나게 된다.

여기서 말하는 개인정보란 생존하는 개인에 관한 정보로서 해당정보에 의하여 개인을 식별할 수 있는 것을 말하며, 해당 정보만으로 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것은 개인정보에 해당한다. 그리고 행정정보공동이용이란 행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것이라 할 수 있는데, 전자는 개인정보이고 후자는 행정정보인데 후자인 행정정보는 전자인 개인정보를 포함하여 공동이용하고 있다고 할 수 있으며, 이와 같은 개인정보가 포함된 행정정보를 공동이용하는 것을 개인정보의 공동이용이라 정의 할 수 있다.

제2단계 이상에서는 단순한 정책의 집행이나 관리의 수단으로서 활용되던 개인정보가 의사결정 및 정책결정의 수단으로 활용된다. 이러한 정보의 공동이용은 정보통신기술의 발달에 의하여 조직간의 연계의 필요성이 더욱 확대되는 결과로 나타난다고 할 수 있다.

이러한 논의에 의할 경우 정보의 공동이용은 기존의 조직 내 정보체계를 두 개 이상의 조직에서 활용하거나 두 개 이상의 조직내 정보체계를 결합하여 운영하는 정보관리체계로 정의될 수 있다. 정보공동활용의 사전적 의미는 정부 또는 공공기관이 업무수행을 목적으로 보유 또는 관리하고 있는 정보를 부서와 부서, 기관과 기관, 공공부문과 민간부문, 그리고 기관·기업·개인 사이에 공동으로 활용하는 것을 의미한다.

「전자정부법」제2조 제4호에서도 행정정보공동이용이란 “행정기관이

114) Ignace Th. M. Snellen, "Information Strategy for Public Policy, "in Paul H. A. Frissen and Ignace Th. M. Snellen, Informatization Strategies in Public Administration, New York : Elsevier Science Publishers(1990), p.184.

보유・관리하고 있는 행정정보를 다른 행정기관 또는 공공기관 등이 정보시스템을 통하여 공동이용하는 것"이라고 정의하고 있다.

또 행정정보의 공동이용은 다른 기관이나 조직의 정보공개를 의미하며, 바로 이러한 공개를 바탕으로 정보를 공유하고 사용하는 것을 말한다. 정보의 공동활용은 그 대상에 따라 물적 정보의 공동활용과 인적 정보의 공동활용으로 구분될 수 있는 바, 이 때 행정정보에 포함된 개인정보가 공동이용될 때 개인정보의 공동이용이 되는 것이다.

물적 정보의 공동활용이라 함은 통계정보, 외무관련 문서와 학교시설관리, 문화기록 등과 같이 비인적 정보를 공동활용하는 것으로서 행정안전부의 주민등록정보와 같은 것을 공동활용하는 것을 의미한다.[115]

2) 개인정보공동이용의 목적

정보화사회에서 공공정보의 공동이용은 행정의 편의성, 경제성, 효율성, 투명성, 책임성 등을 가능케 하는 정책수단일 뿐 아니라 성공적인 국가경영을 위한 중요한 전략적 수단으로 인식되고 있다.

국가차원에서 개인정보를 공동이용하는 목적은 일반정보체계와 다를 바 없으나, 이러한 목적을 달성할 수 있도록 고도화시킨 것으로 이해될 수 있다. 특히 정보이용・접근가능성・이용가능성의 증대와 데이터 수집・저장・처리의 중복을 줄이는 것을 그 목적으로 한다.

개인정보의 공동이용은 공공기관의 정보의 수집・관리비용을 절감하여 경제적 이익창출 및 더 나아가 국민들에게 보다 양질의 서비스를 제공하여 줄 수 있는 기회를 증대시킬 수 있다.

또한 정책결정자에게 의사결정과 관련한 보다 나은 정보를 제공하여 줌으로써 합리적인 결정을 할 수 있게 한다. 정책과 관련하여 자동화된 정보시스템은 정책문제의 발견, 정책문제의 정의, 대안정보의 선택, 그리고 정책논의에 도움을 줄 수 있다.[116]

다. 개인정보공동이용을 위한 기본조건

전자행정에 있어서 개인정보 이외에 모든 정보의 공동이용을 위하여 정

115) 박홍윤, 앞의 책, 11면.
116) 위의 책, 13-14면.

보체계의 환경이 공동이용에 적합하게 성숙되어야 한다. 먼저 정치적인 차원에서 공동이용에 대한 이해관계자간의 합의가 이루어져야 한다. 오늘날 대부분의 공동이용 시스템이 구축되어 있어도 이용의 효율성이 저하되는 가장 중요한 요인은 정보의 공동이용에 대한 합의의 부재이다. 특히 부처이기주의 및 부처할거주의적인 관료제 내의 형태가 극복되지 않는다면 정보의 공동이용은 실효를 거두기 어렵다.

다음으로 정보의 공동이용은 이용의 경제적 타당성이 전제되어야 하고, 기술적인 조건이 충족되지 않으면 공동이용에 의하여 얻어지는 정보의 질과 정확성이 저하된다. 기술적인 차원에서 데이터베이스화된 개인정보를 공동이용하기 위해서는 첫째, 공동이용의 대상이 되는 조직은 각각 구체적 목적을 가지고 있는 조직정보체계가 있어야 한다. 개개의 조직은 자기들과 연관성이 있는 모든 개인정보를 단일 시스템으로 구축하여야 한다.

둘째, 몇 개 또는 모든 시스템이 하나 이상의 텔레커뮤니케이션을 통하여 연결되어야 한다. 즉 개별 시스템이 다양한 형태의 네트워크에 의하여 연결되어 데이터의 집권화가 되어야 한다.

셋째, 개인정보가 일관성 있고 통일되게 식별되어야 한다. 이 조건에 의하여 여러 기관의 개인정보가 커뮤니케이션 기술에 의하여 하나로 통합되게 된다. 즉 두 개의 시스템에 존재하는 개인정보를 일관성 있고 정확하게 연결시키기 위해서는 양자에 공통된 그리고 중복되지 않은 인자가 있어야 한다.[117]

2. 개인정보의 공동이용을 위한 응용기술

가. 컴퓨터 매칭

컴퓨터 매칭 또는 컴퓨터 연결(Computer Matching)이라 함은 데이터의 유사점과 차이점을 결정하기 위하여 두 개 이상의 컴퓨터 파일을 비교하는 것 또는 둘 사이의 유사점 또는 상이점을 색출하기 위하여 하나의 정보데이터베이스(database)와 다른 정보데이터베이스를 비교하는 컴퓨터의 이용[118] 혹은 범죄의 혐의자를 확인하기 위하여 무관계한 개인의 전산화

117) 위의 책, 14-15면.

된 파일을 연결시키는 것이라고 할 수 있다.[119] 미국의「1988년 컴퓨터 연결 및 프라이버시 보호법(The Computer Matching and Privacy Protection Act of 1988)」은 둘 이상의 자동화된 기록시스템 또는 기록시스템과 기록간의 컴퓨터에 의한 대조 혹은 둘 이상의 자동화된 기록시스템 또는 하나의 기록과 다른 기록과의 컴퓨터에 의한 대조를 의미하는 것으로 정의하고 있다.[120]

「컴퓨터 연결 및 프라이버시 보호법」은「1974년 프라이버시법」으로부터 연방정부가 정보의 수집목적에 합치될 경우에는 예외적으로 본인의 동의 없이도 개인정보를 활용할 수 있다는 통상적 예외규정을 악용한다는 비판을 배경으로 제정되었다.「컴퓨터 연결 및 프라이버시 보호법」은 연방기관이 보유하고 있는 개인기록을 무단으로 활용하는 것을 통제하기 위해「프라이버시법」을 개정하는 형식을 취하여 절차면에서의 통제는 가능하게 되었다. 그러나 컴퓨터 매칭의 허용여부에 대해서는 실질적 판단기준을 제시하지 못한다는 비판을 받는다.

그리고「컴퓨터 연결 및 프라이버시 보호법」과 관련하여 미국 하원은 정부기관이 컴퓨터 매칭에서 얻어진 정보의 진실성을 다른 방도로 증명하지 않는 한 증거에서 인정할 수 없다고 한다. 나아가 컴퓨터 매칭을 실시하기 전에 비용・효과 분석을 실시할 것을 요구함으로써 개인정보 활용에 엄격한 요건을 부과하였다.[121]

한편, 컴퓨터 매칭의 기본적인 절차는 먼저 하나 혹은 두 개의 개인정보 데이터베이스에서 필요한 레코드를 선택하고 여기서 불필요한 필드나 정보를 제거한 후, 두 개 이상의 데이터베이스를 매칭 알고리즘에 의하여 결합시키게 된다. 이와 같은 결합에서 가장 핵심이 되는 것이 통일된 식별인자이다. 매칭에 의하여 처음 나온 결과를 로 히트(raw hit)라고 한다. 로 히트로 된 자료에 대하여 일정한 추론과 필터링을 거쳐서 최종적

118) 박홍윤, 앞의 주 88), 16면.
119) Committee on Governmental Affairs United States, Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs, U.S.A. : G.A.O., (1983), p.4
120) The Computer Matching and Privacy Protection Act of 1987: Hearings on S. 496 Before the Subcomm. on Government Information Justice, and Agriculture of the House Comm. on Government Operations, 100th Cong., 1st Sess. ii(1987).
121) 이정희, “통신비밀보호법의 문제점과 개선방향에 관한 연구 : 도·감청을 중심으로”, 석사학위논문, 용인대 경영대학원, 2007, 19면 참조.

인 솔리드 히트(solid hit)를 얻게 되고 그 결과를 바탕으로 개개인에 대하여 의사결정을 행하게 된다. 이들의 정보는 다시 데이터베이스로 관리하게 된다. 이들 결과에 대해서는 질 분석을 하여 데이터의 정확성 등을 평가하는 데 활용되기도 한다.

이 기법은 특정 개인보다 일반 대중에 대한 감시기법의 차원에서 주로 활용된다. 이는 거대한 개인정보 데이터베이스에서 나오는 부당한 사기자(詐欺者) 등을 적발하는데 유용한 기법이 된다. 우리나라의 경우 컴퓨터 매칭은 1980년대 중반 이후부터 매우 광범위하게 사용되고 있다.[122]

이외에 컴퓨터 매칭은 정보관리에 있어서 데이터의 정확성과 신뢰성을 확보할 수 있는 수단이 되기도 한다. 그러나 이는 정보 프라이버시에 대하여 잠재적인 위협의 요인이 되기도 하여 이용에 있어서 적절한 통제가 요구된다. 특히 컴퓨터 매칭의 기법은 소비자 기업간, 그리고 국민과 국가간에 커다란 권력의 불균형을 가져온다. 특히 매칭에 의하여 개인과 그들의 행태에 대하여 잘못된 이미지를 형성할 위험이 상존한다는 비판을 받고 있다.[123]

나. 컴퓨터 프로파일링

컴퓨터 프로파일링(Computer Profiling)은 프로파일(Profile)을 작성하여 이용하는 것을 말한다. 정보시스템에서 프로파일링 기법은 큰 데이터베이스에서 특정한 항목의 조합을 찾는 검색기술이다.

개인정보의 활용과 관련하여 프로파일링은 특정한 대상집단과 밀접하게 연관된 특성을 확인하고, 이와 동일하거나 유사한 특성을 가지고 있는 사람들을 확인하기 위하여 데이터베이스를 검색하는 과정이다. 즉, 개인이 어떤 행동이나 성향과 관련된 것으로 알려진 특성을 가지고 있는지의 여부를 결정하는 과정이다. 프로파일링은 통계적으로 비슷하게 나타난 다른

122) 1980년 한국전력이 국민주를 공모했을 때, 청약자의 주민등록번호와 이름을 국세청의 1987년 납세자료와 매칭하여 무자격자 및 이중청약자를 적발해낸 것과 공공기관으로서는 지방행정기관에서 토지대장과 재산세·상속세 자료를 매치시켜 미과세자료를 색출하는 것 등이 대표적인 예이다. 또 컴퓨터 매칭의 기법은 보험재정의 건전화, 납세행정의 효율화 등에 의하여 공공자금의 절약이라는 유용한 효과를 가져 올 수 있다. 이에 의하여 국세청의 개인 소득파일에 대한 매칭 프로그램을 앞으로 더욱 확대될 전망이다.

123) 박홍윤, 앞의 책, 18-19면.

사람의 과거 행태를 기초로 특정한 개인들을 확인하는 것이다.

특히 데이터베이스로부터 지식발견(Knowledge Discovery in Databases: KDD)이라고 하는 데이터 마이닝(data mining) 기법의 발전은 이러한 프로파일링의 과정을 한 단계 높이는 결과를 가져오고 있다. 데이터 마이닝은 대규모의 데이터 내에 숨겨져 있는 고급 정보를 추출해서 의사결정, 예측, 예보에 응용하는 기법으로 최근 2000년대의 데이터베이스 응용기술로 주목을 받고 있는 기술 분야이다.

이러한 컴퓨터 프로파일링은 공공수요를 파악하고 민간기업의 목표광고의 기법을 활용하여 정책 및 업무의 효과성 제고를 할 수 있고, 경제적인 면에서 수입의 증대 및 공공비용의 절감효과를 얻을 수 있다. 이러한 경제적 효과에 의하여 이 기법은 국세청의 음성탈루 소득자에 대한 세무조사 등에 많이 사용된다.

이러한 점에서 공직자 재산변동 상황에 대한 DB화와 그 정당성에 대한 추적이 이루어질 수 있도록 시스템이 구축된다면 공직자의 부정부패를 억제하는 데 유요한 도구가 될 수 있다. 이외에 전산감사나 다양한 형태의 불법행위자의 적발 등에 활용성이 높은 것으로 알려지고 있다.[124]

다. 컴퓨터 신원조회 및 적격심사

컴퓨터 신원조회는 컴퓨터에 의한 다양한 형태의 신원조회 및 신원확인을 의미한다. 컴퓨터 신원조회(Computer Screening)는 하나 이상의 컴퓨터 레코드에서 비정상적인 유형을 확인하기 위한 컴퓨터 분석방법을 의미한다. 컴퓨터 신원조회는 내부규범에 의거하여 트랜잭션을 심사하거나 신분을 마스터파일에서 조사하는 방법이다. 이는 일정한 프로파일링의 결과를 마스터파일로 운영하는 경우에 유용하다. 예로 출입국관리에서 신원특이자의 검사, 은행의 대출에서 불량거래자의 조사 등 우리나라 시스템에서 가장 많이 사용되는 기법으로 종종 법이나 조직의 규범에 의거하여 의무적 행위로 규정하고 있다.

컴퓨터 프로파일링은 개인을 대상으로 할 수도 있고, 모든 트랜잭션에 대하여 법이나 조직의 규범에 의하여 의무적으로 하는 경우도 있다. 우리

124) 박홍윤, 앞의 책, 19-24면 참조.

의 경우에 경찰청의 수사업무 등에서 일상화된 정보처리 활동이라고 할 수 있다. 또한 여권전산망에서 여권신청자의 신청항목을 주민 데이터베이스에 보내어 그 항목의 진위여부를 yes/no로 회신 받는데 활용하고 있다.

이외에 미국에서 상용의 예를 보면「1982년 채무변제법(The Debt Collection Act, 1982)」에서는 연방정부에 대부를 신청하는 사람에게 그들의 사회보장번호를 제출할 것을 요구하고 있다. 그리고 이 번호는 해당 기관에서 납세 불이행 여부를 조사하기 위해 국세청(IRS: Internal Revenue Service) 파일로 신청자의 신용을 확인할 것을 규정하고 있다. 그리고「1984년 총괄범죄통제법」은 육아시설의 운영 및 고용인에 대하여 전국적인 범죄기록을 제공하여 주도록 하고 있다. 특히「적자감소법」은 특정 연방지원 사회보장 프로그램에 대하여 수혜자를 선정하기에 앞서 컴퓨터에 의하여 데이터 대조를 실행할 것을 규정하고 있다. 그러나 미국에서는 파일들을 연결하는 표준화된 통일식별부호가 완벽하지 않기 때문에 이들의 이용은 제한되어 있다.[125]

이러한 점에서 다른 외국의 경우도 통일된 식별인자는 데이터의 연계에 있어서 가장 큰 문제로 나타나고 있다.[126]

3. 개인정보공동이용의 실태

가. 공공기관의 개인정보 현황

우리나라에서 개인정보를 가장 많이 보유한 자는 아마도 정부일 것이다. 정부가 보유한 개인정보 파일의 기록은「공공기관의 개인정보보호에 관한 법률」제7조에 의하여 행정안전부장관이 년 1회 이상 관보 또는 인터넷 홈페이지 등에 게재하여 공고하여야 한다.

지난 2008년 국정감사에서 유정현(한나라당) 의원이 공개한 자료를 보면, 2007년 2만 315개 공공기관(중앙행정기관, 지방자치단체, 교육청 및 각급 학교, 정부투자기관 등을 포괄)에서 1360 종류의 개인정보파일 9만 2855개를 보유한 것으로 나타났다. 이는 2005년 1095개 기관에서 1078종

125) Computer Science and Telecommunications Board National Research Council, (1997), p.78-80.
126) 박홍윤, 앞의 책, 24-26면 참조.

류 1만 510개 개인정보파일을 보유한 것과 비교하면 무려 9배나 증가한 수치다.

또 공공기관이 보유한 개인정보파일의 일반적인 증가와 함께 생체정보와 같은 민감한 개인정보의 수집도 늘어나고 있다. 우리나라에서는 이미 1968년부터 일정 연령 이상의 전 국민을 대상으로 열손가락 지문을 수집하고 있는데, 이는 현재 전산화되어 경찰청에서 관리하고 있다. 나아가 국민을 대상으로 한 유전자 정보 수집도 늘어나고 있다. 지난 2004년 경찰청은 장기 미아를 찾는다는 명분으로 보호시설에 수용된 아동들과 미아 신고를 한 부모들에 대한 유전자 데이터베이스를 구축했으며, 경찰과 검찰은 범죄자의 유전자 데이터베이스 구축을 위해 오랫동안 법안 마련을 추진해왔다. 2006년에 발의한「유전자감식정보의 수집 및 관리에 관한 법률(안)」이 결국 17대 국회를 통과하지 못하자, 2009년 5월 26일 법무부는「DNA신원확인정보의 이용 및 보호에 관한 법률(안)」을 다시 입법예고했다.

개인의 화상정보를 수집하는 폐쇄회로텔레비전(CCTV) 설치도 급증하고 있다. 2002년 서울 강남구청과 강남경찰서가 CCTV 5대를 시범 설치한 이래로, 공공기관들은 앞다퉈 CCTV를 도입하기 시작했고, 2008년 5월까지 약 13만대의 CCTV가 공공기관에 의해 설치된 것으로 파악되고 있다. 2008년 2월 국무총리 산하 공공기관의 개인정보보호 심의위원회에서 검토된 공공기관 CCTV 관리실태 조사결과에 따르면 대다수 공공기관 CCTV에 줌·회전기능이 설치돼 있을 뿐 아니라 일부 CCTV는 당사자 몰래 음성 녹음까지 하는 등 관련법규(「공공기관의 개인정보보호에 관한 법률」)도 제대로 지켜지고 있지 않았다.

또 공공기관에서 수집한 개인정보의 공유도 확대되고 있다. 2006년에 구축된 행정정보공동이용 시스템은 현재 주민등록등·초본, 납세관련서류, 부동산 관련 서류 등 행정정보 71종을 공유하고 있다. 이 중 개인정보는 모두 44종이다. 정부는 2012년까지 공공기관이 공동이용하는 행정정보 수를 150종으로 확대하고, 공동이용기관도 50개에서 전체 공공기관으로 확대할 예정이라고 한다. 또한 공공기관뿐만 아니라 병원·학교·협회 등 민간기관도 공동이용 대상에 포함[127]시킨다고 한다.

---

127) 한겨레21, "악착같아라, 정부의 정보 폭식", 한겨레21. 통권766호, 2009, 22면.

나. 개인정보공동이용 현황

행정정보공동이용은 유관기관간 정보를 공동으로 활용함으로써 재활용에 따른 중복투자를 방지하고, 주요정책의 수립에 필요한 정보를 지원하며, 나아가 대민서비스를 개선하기 위한 목적으로 기관간 업무데이터베이스를 공동 활용하고 있다. 부처별로 보유하고 공동 활용하고 있는 5대 데이터베이스의 이용현황과 이용에 대한 수요현황은 다음 <표 3>과 같다.

<표 3> 5대 데이터베이스 정보공동이용의 실태현황

구분	관리시스템	주요이용정보	수요 요구 현황
주민정보 (행정안전부 주민과)	주민등록관리시스템(행정안전부 주민과)	실명확인, 주소조회 등	행정안전부, 국토해양부(표준공시지가), 국세청(과세기초자료), 관세청(관세사범단속), 경찰청(신원조회) 등 70개 기관
부동산 정보 (국토해양부, 행정안전부, 대법원)	지적행정시스템(행정안전부 지적과), 지적정보센터(행안부), 건축행정정보시스템, 토지관리정보체계시스템, 산업입지전산시스템(국토해양부), 부동산등기정보시스템(대법원)	개별공시지가, 종토세, 주택자료, 토지 소유현황 등	개별공시지가, 거래정보, 개별부담금 내역정보, 용도·지부관리 및 지적정보(토지대장, 지적도면, 임야도면 등)의 민원인 요구와 행정기관의 과세자료로 이용
기업정보(대법원,국세청)	대법원 상업등기시스템	사업자등록정보, 법인등록정보 등	병무청 등 5개기관 증가
세금정보 (국세청)	국세청 국세통합정보시스템	과세자료, 근로소득정보 등	금감위의 근로소득정보 등
자동차정보 (국토해양부)	자동차관리시스템, 이륜차관리시스템, 유관망관리시스템(건교부자동차관리과)	자동차등록원부, 차적정보 등 유관망개발후 시범운영 중	차량기본정보, 소유자정보, 차량번호, 제원 및 자동차등록원부, 차적정보에 관련된 경우와 자동차등록통계자료, 저당, 압류 등 민원인의 요구 정보가 있고 그 외 자동차동록 통계, 자동차세 완납증명 등을 발급

정보공동이용은 주로 ① 주민등록정보, ② 부동산정보, ③ 기업정보, ④ 세금정보, ⑤ 자동차정보 등 5대 분야를 중심으로 논의되었다.

정보공동이용의 유형별로 살펴보면, 첫째, 업무처리 공동이용의 예로서 국토정보센터가 행정안전부, 국토해양부, 농림수산식품부, 국세청 등의 행정기관에 공직자 재산등록심사와 대기업 소유 토지 등 토지현황 파악에 필요한 정보를 제공하는 것을 들 수 있다.

둘째, 민원 서비스 정보공동이용의 사례로는 여권발급전산망의 운영이 대표적이다. 여권발급전산망은 외교통상부, 행정안전부, 병무청, 경찰청 등의 관련 데이터베이스를 묶은 하나의 통합 시스템으로, 각 시·도청에서 여권발급 민원인에 대한 정보를 조회해서 즉시로 여권을 발급할 수 있다.

셋째, 결정지원 정보공동이용의 경우, 부처 내에 랜(LAN)을 구축하고 이를 통해 부서간에 필요한 통계자료 등을 공동이용하거나, 범정부적으로는 행정안전부 행정종합정보서비스(NATIS: National Administration Total Information Service), 통계청의 통계정보서비스(KOSIS) 등 온라인상으로 정책정보를 제공하는 것을 예로 들 수 있다.

넷째, 열린 정부 정보공동이용으로서는, 국무총리실 공보실이 알림마당이라는 통합데이터베이스를 설치하여 각 중앙은행기관에서 공보관실을 통해 공개되는 보도자료 등을 국민들에게 제공하고, 정부전산정보관리소가 보도자료·정부입찰·최신법령 등의 알림자료, 경제정보·정부간행물 등의 공공데이터베이스자료, 국가시험·민원사무 등의 민원자료, 행정자치부 중심의 정보데이터베이스자료를 일반국민에게 제공하는 것이 그 예이다.[128]

다. 개인정보공동이용의 문제점

2008년부터 2년 동안 국민건강보험공단이 총 1억 건이 넘는 개인정보를 다른 기관에 제공한 것으로 나타났다. 국가인권위원회가 연구를 의뢰해 조사한 개인정보 수집·유통 실태조사 보고서에 따르면 개인의 사적인 정보들이 정부와 기업에 집중되고 있으며 통신기기의 발달로 유출 위험도

128) 최진안, "전자정부구축에 따른 개인정보공동이용의 헌법적 고찰 -형사사법통합정보체계 구축사업을 중심으로-", 박사학위논문, 성균관대학교 중앙학술정보관, 2009, 39-40면.

갈수록 높아지는 것으로 드러났다. 특히 국민건강보험공단은 2008년부터 2년 동안 공단 내 각 부서에서 총 733회에 걸쳐 1억 건이 넘는 개인정보를 다른 기관에 제공한 것으로 나타났다.

이와 같이 공공기관의 개인정보 보유가 증가할수록 개인정보침해도 급격하게 늘어날 수 있다. 또한 개인정보에 접근할 수 있는 사람이 많아지면 그만큼 개인정보의 유출이나 남용 위험성이 증가할 수밖에 없다.

우리나라에서 개인정보를 위협하는 구조적인 문제 중 하나는 '주민등록번호'의 남용이다. 공공·민간 할 것 없이 주요 개인정보 데이터베이스를 위하여 주민등록번호를 수집하고 있으며, 이를 개인 식별 수단으로 사용한다. 따라서 주민등록번호만 알면 서로 다른 개인정보 데이터베이스의 정보를 통합할 수 있게 된다. 주민등록번호를 식별 수단으로 사용하는 데이터베이스가 많을수록 위험성은 더욱 커진다. 2005년 국가인권위원회 인권상황 실태조사에 따르면, 법정 서식의 47.1%, 공공기관 개인정보 파일의 80.4%에서 주민등록번호를 수집하는 것으로 드러났다. 민간에서 이용되는 서식조차 48.2%가 주민등록번호를 요구하고 있었다.

공공기관이 보유한 개인정보는 급증하고 있지만, 수집된 개인정보의 보호는 미흡한 상황이다. 2008년 11월 국민건강보험공단이 보유한 개인정보 70만여 건이 불법 유출된 사실이 밝혀진 바 있듯, 여러 기관이 공동으로 이용하는 개인정보 데이터베이스는 남용의 가능성에 항상 노출돼 있다. 주민등록번호를 포함한 개인정보의 대규모 유출사고가 잇달아 발생하고 있지만, 행정안전부는 주민등록번호 제도에 대한 근본적인 대책은 내놓지 않고 있다.

정부가 보유한 모든 개인정보 파일이「공공기관의 개인정보 보호에 관한 법률」에 따라 보유 현황이 공개되는 것도 아니다. 국가 안전이나 범죄 수사 등과 관련된 개인정보 파일의 공개는 이 법에서 예외로 인정하고 있기 때문에 경찰청의 범죄·수사경력자료 등은 보유 현황이 공개되지 않는다. 이와 같은 비공개 개인정보 파일의 경우 그 운영 및 관리가 적절하게 이뤄지는지에 대해 사회적 감시 자체가 어렵다.

특히 수사기관이나 정보기관은 자체적으로 보유한 개인정보에만 접근할 수 있는 것이 아니다. 사회 전반의 개인정보 데이터베이스 확대는 수사기관이나 정보기관 등 정부가 파악할 수 있는 개인정보의 폭과 깊이를 확대하고 있다. 금융거래 내역, 교통카드를 통한 이동 경로, 인터넷 이용 내역,

공공 및 민간의 CCTV 기록, 통화 내용 등 영장만 있으면 개개인의 삶 전반을 투명하게 들여다볼 수 있을 정도다. 비록 정부가 선의의 목적을 가지고 있더라도, 개인정보 수집이 과도하거나 관리 체계가 허술하다면 개인정보의 유출과 남용의 위협에서 자유로울 수 없다. 어쩌면 더 큰 위험은 수집된 개인정보가 국민을 통제하기 위한 수단이 될 수 있다는 점이다.[129]

개인정보공동이용의 처리과정에서 정보주체의 의사가 반영될 기회가 보장되지 않을 경우 개인은 은밀한 개인정보의 수집이나 부정확한 개인정보의 축적과 유통에 대해서조차 묵인할 수밖에 없다. 자신의 인적사항이나 생활상의 각종 정보가 자신의 의사와는 무관하게 집적되고 이용 또는 유통되는 상황에서 자신에 관한 정보에 있어서 조차 자율적 결정이나 자기통제의 가능성을 봉쇄당한다면 개인의 자유로운 인격발현이나 사생활의 형성은 기대하기 어렵게 된다. 이렇게 될 경우 개인은 정보의 주체가 아리라 단순한 정보객체로 전락하게 되고 말 것이다. 한편, 개인정보의 수집과 처리에 있어서의 국가적 역량이 현격히 강화되었다는 것은 국민 개개인에 대한 감시능력이 무한히 증대되고 있음을 의미한다. 개인의 일상적 생활상이 국가에 의해 낱낱이 파악될 수 있음에도 불구하고 은밀하고 교묘하게 이루어지는 정보의 처리로 말미암아 국민들 개개인으로서는 좀처럼 자신이 감시를 받고 있다거나 통제되고 있다는 것을 인식할 수 없다. 이러한 상태에서 개인은 혹시 자신이 감시당하고 있을지 모른다는 막연한 두려움을 느끼게 되고, 그러한 심리상태는 개인의 자유로운 일상생활을 위축시키는 결과를 가져올 수 있다. 이는 공동체생활에 있어서 개인이 공적 의사형성과정에 자유로이 참여하지 못하도록 하여 민주적 의견형성을 저해하거나 의사를 왜곡하는 결과를 초래할 수도 있다.[130]

129) 한겨레21, 앞의 주 124, 23면.
130) 권건보, 앞의 주 74), 54-55면.

제3절 개인정보보호에 관한 비교법적 고찰

1. 외국과 국제기구의 개인정보보호법제

가. 외국의 개인정보보호법제

1) 미국의 개인정보보호법제

(1) 미국법의 체계

일반적으로 미국은 불문법 국가이며 법원의 판결이 선례구속(先例拘束)의 원칙을 가지는 보통법체계 국가라고 알고 있다. 하지만 미국 의회는 엄격한 삼권분립 원칙하에 연간 수많은 법률을 제정하고 있으며, 대부분의 판결은 의회에서 제정된 법률이나 행정부의 명령을 해석하고 있는 제정법 체계를 가지고 있다.[131] 미국의 제정법은 특정 분야의 판례법을 변경하거나 판례가 규율하지 않은 새로운 법 분야를 형성하기 위하여 제정되는 것이 보통이다.

특히 오늘날과 같이 급변하는 미국 사회에서 제정법의 역할이 보다 강조되고 있으며, 정보보호와 같은 새로운 분야에서 미국 제정법은 보다 큰 의의를 갖는다고 할 수 있다. 이러한 제정법은 1차적 법원 중의 하나이다. 미국에서는 크게 1차적 법원과 2차적 법원으로 분류된다. 1차적 법원은 판사가 재판하는 경우 반드시 적용하여야만 하는 것으로 판례법, 제정법 및 관습법 등이 여기에 해당한다. 2차적 법원으로는 학설, 백과사전, 논문집, 교과서 및 참고문헌 등이 이에 해당하며 판사가 이를 적용해야 하는 구속력을 받지는 않는다.[132]

한편, 미국 연방수정헌법 제1조는 연방의회가 언론·출판의 자유를 제한하는 법률을 제정할 수 없도록 규정함으로써 명시적으로 표현의 자유를 보장하고 있다. 이에 반해 프라이버시권에 대해서는 명문의 규정을 두고 있지 않았다. 이러한 프라이버시권은 초창기에 재산권의 일종으로 혹은 신탁(trust)의 일부로 취급되어 점차 불법행위법에서 권리나 헌법상 인권으로 인식되어 갔다.[133] 다만, 보통법을 통한 보호는 포괄적이기는 하나

131) 김형남, 외, 미국법 강의, 세종출판사, 2001, 14-16면.
132) 이창범, 미국, 독일, 일본의 정보보호법 체계에 관한 연구, 한국정보보호진흥원, 2006, 13면.
133) 이민영, "미국의 언론보도와 프라이버시", 세계의 언론법제 개인정보보호와 언론 2008년 하권(통권 24호), 한국언론재단, 2008, 76면.

그 적용이 불확실하고 헌법을 통한 보호는 국가가 개인의 프라이버시를 제한하는 경우로만 한정되었다. 미국에서 아직 통일적인 개인정보보호법이 제정되지 않고 있는 데, 그 이유는 미국의 지리적, 역사적 상황 때문이기도 하다.[134]

(2) 개인정보보호체계 및 특징

미국은 개인정보보호에 있어서 국가기관 스스로가 정보 및 프라이버시 보호 문제를 다루어야 한다는 인식을 바탕으로 원칙적으로 당해 행정기관들이 프라이버시 관련 현안을 자체적으로 해결하는 방식을 취하고 있으며, 여러 개별법에 의해 그 용도에 따라 개인정보를 보호하는 부문별 접근방식을 채택하고 있다. 다만 연방기관의 개인정보와 관련해서는 관리예산처(OMB)가 이들 행정기관에 대한 감독기구의 역할을 수행하고 있다.[135]

그리고 공공부문에서 대통령 직속의 관리예산처(OMB)가 예산편성권을 집행수단으로 하여 강력하고 공정한 보호체계를 구축하고 있고, 민간부분에서는 일부 영역을 제외하고 소비자정보를 일반적으로 보호하고 감독하는 책임을 행정부로부터 독립된 기관인 연방거래위원회(FTC)가 맡고 있다. 물론 연방거래위원회는 소비자정보의 보호만을 위해서 특별히 설립된 기구는 아니다. 그러나 연방거래위원회는 공정거래질서를 확보하기 위해 주어져 있는 강력한 집행권한에 기초해서 시장에서 소비자정보의 오·남용으로 인한 중대한 프라이버시침해가 있는 경우 적극적인 보호기능을 수행하고 있다고 할 수 있다.

또한 연방거래위원회는 기업에 의한 소비자정보의 활용의 필요성과 가치를 충분히 인식하면서 산업계의 자율규제가 원만하게 작동되도록 지도와 감독을 행하고 있다. 연방거래위원회는 행정부로부터 분리된 독립규제위원회로서 7년 임기의 5인의 위원으로 구성되어 있다. 연방통신위원회(FCC)도 5년 임기의 5인의 위원으로 구성되어 있다.[136]

---

134) 김일환, “개인정보공동이용의 통제와 감독에 관한 비교법적 고찰 -미국과 독일의 법제를 중심으로-”, 헌법학연구 제13권 제2호, 한국헌법학회, 2007, 419면.

135) 황종성 외, 국외 개인정보보호법제 분석 및 시사점, 한국전산원, 2004, 128면.

136) 박문석, “사이버공간에서의 프라이버시권에 관한 비교법적 연구”, 박사학위논문, 영남대학교 대학원, 2009, 255면.

미국의 개인정보보호법제 특징은 첫째, 공적영역에서든 사적영역에서든지 간에 개인정보의 사용에 관한 법률과 명령은 비교적 많고 다양한 편이나 일반적으로 이들은 특정한 산업이나 경제영역, 그리고 종종 어떤 구체적 문제를 다루는 경향이 있다. 둘째, 이러한 개개 분야의 법률들은 개인정보의 수집에서 처리·삭제까지 일관되게 보호한다기보다는 특정한 정보사용자, 특정한 정보사용 문맥, 특정한 정보유형이나 개인정보의 특정한 사용에만 적용되며, 특히 개인정보의 수집, 사용, 저장보다는 이러한 정보의 공개만을 금지하는 경향이 매우 강하다. 셋째, 미국에서 개인정보는 국가나 독립된 위원회를 통한 통제와 감독을 통한 보호가 아닌 자신의 권리가 침해되었다고 생각하는 개개 시민이 법원에 소를 제기하여 구제 받는 사법적 구제책에 거의 의존하고 있다.[137]

이러한 특징으로 인하여 미국에서 개인정보보호는 일반적 원칙과 기준을 제시하는 종합적이고 포괄적인 기본법의 부재로 개인정보보호가 충분히 보장되지 않는다는 비판을 받고 있다.

(3) 개인정보보호법제의 현황

앞서 고찰한 바와 같이 미국은 개인정보보호에 대한 통일적·일반적인 법체계를 가지지 않고, 연방의회 및 주의회에서 특정분야에만 한정적으로 적용되는 개별입법만 제정하고 있다. 즉, 미국의 개인정보보호입법은 공공부문과 민간부문을 통합하지 않고 부분적·개별적으로 적용되는 법체계를 유지하고 있다. 구체적으로 살펴보면 다음과 같다.

공적영역에서의 개인정보에 관한 대표적인 개별 연방입법 중 연방정부의 기록에 대한 법률로는「1974년 프라이버시법(Privacy Act, 1974)」, 1988년의「컴퓨터 연결 및 프라이버시 보호법(The Computer Matching and Privacy Protection Act of 1988)」,「2002년 전자정부법(E-government Act, 2002)」등을 들 수 있다. 통신부문에는「전자통신 프라이버시법(Electronic Communications Privacy Act, 1986)」,「전화소비자보호법(Telephone Consumer Protection Act, 1999)」,「1994년 법집행통신지원법(Communications Assistance for Law Enforcement Act, 1994)」등이 있다. 그리고 민간부문에서 적용되는 개별입법으로는 「1970년 공정

137) 김일환, 앞의 주 131), 420면.

신용기록법(Fair Credit Reporting Act, 1970)」, 「1974년의 공정신용경리법(Fair Credit Billing Act, 1976)」,「1974년 가족교육권 및 프라이버시법(Family Educational Rights and Privacy Act」, 1976년 개정됨),「1977년 공정채권추심법(Fair Debt Collection Practices Act, 1977)」,「1978년 금융 프라이버시권에 관한 법(Right to Financial Privacy Act, 1978)」,「1988년 비디오 프라이버시보호법(Video Privacy Protection Act, 1988)」,「1994년 운전자 프라이버시 보호법(Driver's Privacy Protection Act, 1994)」, 「1996년 건강보험관리 및 책임에 관한 법률(Health Insurance Portability and Accountability Act, 1996)」,「1999년 아동 온라인 프라이버시 보호법(Children's Online Privacy Protection Act, 1999)」등을 들 수 있다.

이하에서는 개인정보보호와 관련하여 대표격인「프라이버시법」및 개인정보공동이용과 관련한「컴퓨터 연결 및 프라이버시 보호법」의 주요내용 및 개별입법들을 살펴보기로 한다.「컴퓨터 연결 및 프라이버시 보호법」은 앞에서 컴퓨터 매칭과 관련하여 잠시 언급한 바 있지만 여기서는 좀 더 구체적으로 검토하기로 한다.

(4) 세이프 하버 원칙

미국은 제정법이나 판례법 이외에도 개인정보보호를 위한 지침으로 세이프 하버 원칙(Safe Harbor Principles)을 정립하였는데, 이 원칙은 1988년 10월 25일 발효된「EU 개인정보보호지침」에서는 이 지침과 같은 적절한 수준의 개인정보보호 체계를 갖추지 못한 제3국에 대한 개인정보 국외 이전을 엄격히 제한하도록 하였는데, 이와 관련하여 미국은 자국의 항공사, 은행, 여행사 및 다국적 기업의 피해를 방지하기 위해 세이프 하버 원칙을 마련하고 EU와 협상 끝에 2000년 7월 합의하고 2001년 11월 1일부터 효력을 얻어 시행되고 있다. 이는 EU의 법률에 의한 개인정보의 보호방식이 아닌 자율규제의 원칙하에서 개인정보의 보호를 행하는 미국식 개인정보 보호방식을 의미한다.

세이프 하버 원칙은 기본적으로 유럽연합 회원국과 국제교류와 관련하여 유럽 시민들의 개인정보를 전달받아 개인정보취급의 적정성 여부를 판단한다. 특정한 목적을 가진 원칙이기 때문에 국제조약의 성격을 가지지는 않는다. 이 원칙에 따를 것인지의 여부는 전적으로 미국 기업들에게

달려 있는 것이다. 그러나 실질적으로 이 원칙에 따를 경우 유럽 위원회(European Commission)로부터 개인정보의 적정성(adequacy)을 확인받게 되는 결과가 되기 때문에 EU 회원국과 별도의 협의와 논의를 진행할 필요가 없이 적정성이 추정되게 된다. 따라서 현재 미국에서는 이러한 세이프 하버 원칙의 장점과 이점으로 인해 다수의 기업체가 참여하고 있다.[138]

세이프 하버 원칙은 고지, 선택, 정보제공, 접근, 안전성, 데이터 무결성, 집행의 총 7개의 원칙으로 구성되어 있다.

① 고지(Notice)

개인정보의 수집·이용목적, 용도, 정보를 제공하는 제3자의 유형, 문제제기 또는 권리행사시 접근방법 등에 대하여 고지하여야 한다.

② 선택(Choice)

개인정보가 제3자에게 제공되는지 여부 및 최초의 수집목적과 양립할 수 없는 다른 목적으로 정보가 사용될 것인지 여부에 대해 opt-out 방식의 선택권을 제공 또는 민감한 정보에 대해서는 opt-in 방식의 선택권을 제공하여야 한다.

③ 정보제공(Onward Transfer; Transfers to Third Parties)

개인정보의 위탁처리 등과 같이 제3자에게 개인정보를 제공할 경우, 당사자에게 고지함을 물론 선택권을 부여하여야 한다.

④ 접근(Access)

정보주체의 접근권과 정정·삭제요구권을 보장하여야 한다.

⑤ 안전성(Security)

개인정보를 손실, 오용, 권한 없는 접근, 변경, 파기로부터 보호하기 위한 합리적 예방조치를 취해야 한다.

⑥ 데이터의 무결성(Data Integration)

당초의 수집 및 이용목적에 부합한 개인정보의 이용, 정확성·완전성·최신성을 확보하여야 한다.

⑦ 집행(Enforcement)

원칙의 준수를 담보할 수 있는 구제수단과 분쟁해결절차, 제재수단이 확보되어야 한다.

---

138) 이창범·윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 164-65면.

(5) 미국의「프라이버시법」

「프라이버시법(privacy Act)」은 연방기관들이 보유하고 있는 기록들에 적용된다. 따라서「프라이버시법」의 적용범위는 기록(record)의 개념 정의에 따라 결정되는 바,「프라이버시법」에 따르면 기록이란 개인의 교육, 재정, 병력, 전과나 이력 등을 포함할 뿐만 아니라 기관에 의하여 보유되는 이름, 개인확인번호, 상징, 지문이나 목소리, 사진처럼 개인을 구체적으로 확인할 수 있는 다른 어떤 것을 담고 있는 개인에 관한 정보, 정보의 수집이나 분류를 말한다.[139] 문제는 「프라이버시법」이 일정 부분의 개인정보를 보호함으로써 개인의 프라이버시를 보호하고 있다고 하더라도 프라이버시나 프라이버시의 이익에 대한 정의를 내리고 있지 않다는 것이다. 또한 비록 연방법원이 헌법상 보장하고 있는 프라이버시권 및 「프라이버시법」에 근거하여 대부분의 사건에서 개인정보를 보호하고 있지만, 그것으로는 일관적이고 체계적인 개인의 정보를 보호하지 못하고 있다.[140]

이 법에서 제시하고 있는 개인정보의 보호의 원칙은 ① 개인은 자신에 관한 어떤 기록이 행정기관에 의하여 수집・보유・사용 또는 공표되는 것을 스스로 결정하는 것, ② 자신에 관한 기록은 자신의 승인 하에서만 이용이 가능하다는 것, ③ 연방정부가 보유하고 있는 자신에 관한 기록에 대하여 개인의 접근이 허용되어야 하고, 틀린 기록은 정정 또는 수정을 요구할 수 있다는 것, ④ 또 이러한 기록이 정확하고 적절한 관리를 하여 오・남용을 방지하는 원칙 등이다.

(6) 전자정부법과 프라이버시 영향평가

미국은 각종 전자정부 사업을 추진하는 과정에서 당해 사업이 프라이버시에 미치는 영향을 사전에 조사함으로써 전자정부사업에 따른 국가기관에 의한 프라이버시 침해를 최소화할 목적으로 전자정부법에 프라이버시 영향평가제도를 법제화하였다.[141]

---

139) 5 U.S.C. 522a(a)(4).

140) 김배원, 정부규제적 통합 개인정보 보호법에 관한 연구, 정보통신부, 2002, 42면.

141) 홍준형, 개인정보보호법제 정비를 위한 기본법 제정방안 연구, 한국전산원, 2004, 94면; 구병문 “캐나다 및 미국의 프라이버시 영향평가제도 분석과 국내전자정부 법제도의 도입방향 검토”,

「2002년 전자정부법(E-Government Act of 2002)」은 공공기관이 전자정부사업을 추진하는 경우에 그 전에 해당사업이 개인의 프라이버시에 미치는 영향을 분석·평가하여 그 보호대책을 마련할 것을 요구하는 프라이버시영향평가제도를 도입하였다. 이에 따라 2003년 9월에 관리예산처(OMB)는「전자정부법」의 프라이버시 영향평가 제도를 시행하기 위한 가이드라인을 공표하였다. 이에 따르면, 각 공공기관은 신원확인이 가능한 개인정보처리시스템을 개발하거나 조달하는 경우에 수집되는 개인정보의 종류와 항목, 수집목적과 용도, 개인정보를 제공하는 기관, 개인정보보호에 관한 사항 등과 관련하여 당해 시스템이 개인의 프라이버시에 미치게 될 영향을 평가하고 그 결과를 가능한 한 웹 사이트나 연방관보에 공개하여야 한다.[142]

이와 같은 대상에 대해 평가대상이 되는 정보체계의 규모, 당해 체계에서 신원확인이 가능하게 하는 정보의 민감성, 당해 정보의 무단공개로 초래되는 위험에 관하여 평가하게 되는데 평가 결과는 가능한 범위에서 공개하도록 되어 있다. 다만 공개하는 경우에도 보안상 이유로 또는 프라이버시 영향평가에 포함되어 있는 민감한 정보나 개인정보를 보호하기 위하여 공개에 관한 사항을 변경하거나 공개자체를 배체할 수 있도록 하고 있다.[143] 그리하여 당해 공공기관이 전자정부기금을 사용하고자 하는 경우에는 이 프라이버시영향평가의 결과를 관리예산처에 제출해야 하는 데, 이 제도는 전자정부사업의 추진에 따른 정부기관에 의한 개인정보 및 프라이버시 침해의 최소화 및 일반 국민의 권익과 기본권을 확보하는 데 그 의의가 있다.

(7)「컴퓨터연결 및 프라이버시보호법」

가) 성립배경

미국 연방정부는 1970년대 초반에 컴퓨터연결 프로그램을 개발하였는데, 이후 프로그램의 사용은 폭발적으로 증가하였다. 컴퓨터연결 프로그램은 둘 이상의 컴퓨터 기록에 담겨있는 기록을 대조하여 잘못된 기록이나

정보화정책 제10권 제3호, 한국전산원, 2003, 213-214면.

142) 구병문, 앞의 주 138), 256면; 최선희, "미국 전자정부법의 프라이버시조항 시행지침 발표", 정보통신정책(통권 제334호), 정보통신정책연구원, 2003, 33-38면 등 참조.

143) 홍준형, 앞의 주 138), 94면.

원하는 기록을 찾아내는 것이다. 연방기관들은 이러한 연결 프로그램을 통하여 정부의 보조금지급 프로그램에서 사기, 실수 또는 남용을 발견하기 위하여 사용하거나 정부보조금의 혜택을 받고자 하는 신청자의 자격심사 등을 결정하기 위하여 사용하였다.[144] 이러한 컴퓨터프로그램 연결로 인하여 연방복지프로그램에서 예산을 절약하고 비용을 절감할 수 있었다고 한다.

하지만 이러한 컴퓨터 연결 프로그램은 프라이버시 침해라는 논란을 크게 불러일으켰다. 컴퓨터 연결 계획은 카터 행정부시대에 건강·교육·복지를 담당하는 부처가 설치되면서 수립되었다. 이러한 카터 행정부의 계획을 레이건 행정부가 이어받음으로써 국가의 복지프로그램에서 사기, 낭비, 남용의 소지를 없애려는 구체적인 목표들을 계획하였다. 그리고 레이건 행정부시대에 정부의 통합과 효율성을 위하여 대통령자문위원회는 컴퓨터연결을 강력하게 주장하였고, 이러한 주장은 레이건 행정부시대에 만들어진 정책들에 상당한 정도로 반영되었다. 그런데 컴퓨터 연결을 통한 예산절감은 프라이버시 침해라는 기회비용 없이는 발생하지 않는다고 프라이버시 보호주의자들은 생각하였다. 결국 의회는 이러한 컴퓨터프로그램 연결사용의 급증으로 인하여 개인의 프라이버시가 위협받을 수 있다고 결론을 내렸다. 이에 따라 컴퓨터연결 프로그램을 통하여 그 기록들이 비교되는 개인의 프라이버시권을 보호하기 위하여 의회는「1988년 10월 18일 컴퓨터 연결 및 프라이버시보호법」[145]을 제정하였다.

이러한 컴퓨터연결과 관련된 두 가지 사례를 소개하면 다음과 같다.

첫째 사건[146]에서는 원고 라 재퍼스(Lra Jaffess)는 재향군인국(The Veterans Administration)으로부터 연금을 받을 뿐만 아니라 사회보장제도에 의해서도 보조금으로 받았다. 그런데 퇴역군인에게 지급되는 연금은 사회보장법에 의하여 지급되는 것을 포함한 다른 국가기관들로부터 받는 보조금에 따라 다르게 지급되도록 규정되어 있었다.[147] 그리고 이 법에 따라서 재향군인국이 지급하는 연금을 수령하는 사람들은 매년 그들의 소득변화를 신고해야만 했다. 그러나 원고는 사회보장법에 의하여 수령한

144) S. Rep. No. 516, 100th Cong. 2d Sess. 2 (1988).
145) 이에 관해서는 김일환, 앞의 주 131), 428-429면.
146) Jaffess v. Secretary, Dep't of Health, Educ. & Welfare.
147) 38 U. S. C. § 521 (1988).

액수를 재향군인국에 신고하지 않았다. 그런데 재향군인국은 건강·교육·복지부가 제공하는 사회보장연금을 받는 사람들의 기록과 재향군인국이 지급하는 연금을 수령하는 사람들의 기록을 컴퓨터로 연결·검토하였다. 컴퓨터를 통한 이러한 비교는 위 법률이 요구하는 신고의무를 이행하지 않은 사람들을 찾아내기 위한 것이었다. 이러한 연결을 통하여 재향군인국은 원고가 신고의무를 이행하지 않았음을 발견하게 되었다. 이에 따라서 재향군인국은 원고에게 연금액수를 감액하여 지급한다고 통지하였다. 원고는 이에 대하여 부당하다고 주장하면서 소를 제기하였으나 법원은 이를 받아들이지 않았다.

둘째 사건에서 1982년 교육부는 학자금을 대출하였으나 아직 변제하지 않은 학생들의 목록과 현직에 있거나 이미 퇴직한 연방공무원들에 대한 기록을 컴퓨터로 대조하였다. 교육부가 컴퓨터연결을 통하여 찾아낸 기록에 의하면 변제능력이 있음에도 불구하고 변제하지 않은 금액이 3천 4백만 달러에 달하였다.[148] 그런데「1982년 채무변제법(Debt Collection Act)」에 따르면 공무원이 연방합중국에 대하여 채무를 지고 있는 경우에 이를 변제하지 못하고 있는 경우에 해당 기관이나 다른 기관의 장에 의하여 확인된다면 정해진 기간 동안 매월 일정액을 개인의 월급에서 차압하도록 규정되어 있었다.[149]

나) 주요내용

「컴퓨터연결 및 프라이버시보호법」의 당초의 입법취지는 개인의 프라이버시보호와 정보감시문제에 초점을 맞추기보다는 적정한 행정절차, 행정비용 감소, 복지혜택의 분석 등을 포함하여 행정부가 실현하려는 목적을 위하여 제정되었으나, 어쨌든 이 법은 개인의 프라이버시보호를 위하여 관련기관들이 연결기록들을 사용하기 위해서는 해당 기관들의 서면 동의를 요구하고, 제안된 연결들에 관하여 연방관보(Federal Register)에 기록함으로써 시민들에게 사전 통지되어야만 한다. 또한 어떤 개인에 관한 기록과는 반대되는 기록들을 보유하는 연방기관들이 이러한 기록들의 정확성을 입증하고, 관련 개인들에게 이에 관하여 항변할 기회를 제공하지

148) Hearing before the Subcommittee on Oversight of Gov. Management of the Committee on Governmental Affairs, S. REP. No. 2756, 99th Cong. 2d Sess. 62 (1986).
149) 5 U. S. C. § 5514 (a)(1) (1988).

않는 한 이러한 반대정보들에 근거하여 어떤 개인에게 보조금 지급·제공을 차감하거나 거절하는 조치를 취할 수 없다.

또한 컴퓨터 연결을 통하여 해당 정부기관이 필요한 정도를 넘어서는 엄청난 개인정보를 획득할 위험성이 있다는 비판에 대하여 먼저, 해당 정부기관은 첫째, 연방보조금을 받기 위한 자격을 확정하거나 확인하기 위한 목적과, 둘째, 이러한 프로그램 하에서 지급된 금액이나 변제하지 못한 채무에 관한 정보를 수집하기 위한 목적을 위해서만 모든 컴퓨터연결이 행해진다는 것을 보장해야만 한다.

이에 대하여「컴퓨터연결 및 프라이버시보호법」은 나름대로의 보호대책들을 규정하고 있다. 그 내용은 ① 컴퓨터 프로그램을 수행하기 위한 목적과 법적 권한, 그리고 컴퓨터 연결을 통하여 사용될 개개 정보들을 포함하여 연결될 기록들에 관한 구체적인 서면동의가 있어야만 컴퓨터연결이 행해질 수 있고,[150] ② 컴퓨터연결을 통한 확인절차가 끝난 후에는 컴퓨터연결을 통하여 획득된 결과들을 해당 기관들은 삭제해야만 한다는 것이다.[151]

다) 검토

「컴퓨터연결 및 프라이버시보호법」은 컴퓨터 연결프로그램이 실행되면서 컴퓨터를 연결하거나 이에 참여하는 기관들에게 컴퓨터연결을 감독하고 이를 승인하기 위하여 해당기관의 상급관청들로 구성된 정보완전성위원회(Data Integrity Boards)를 설치할 것을 요구한다.[152] 이러한 요구에 따라 설치된 모든 위원회는 관련제정법이나 지침의 준수여부를 확실히 감독해야만 하고 비용·편익분석을 행하고, 연결행위들에 관한 연례보고서를 제출해야만 한다.[153] 그런데 1982년 5월 12일 만들어진 컴퓨터연결에 관한 관리예산처(OMB)[154]의 지침은 프라이버시법의 이행에 관한 1975년 지침처럼 컴퓨터연결과 프라이버시보호법의 시행을 위하여 만들어진 것이

150) 5 U. S. C. § 552 a(o)(1)(a), (C) (1988).
151) 변재옥, "정보사회에 있어서 프라이버시의 권리", 박사학위논문, 서울대학교 대학원, 1979, 33면.
152) 이에 관한 자세한 설명은 이인호, "개인정보감독기구 및 권리구제방안에 관한 연구", 2004, 한국전산원, 179면 이하 참조.
153) 5 U. S. C. § 552a, section 2, 3.
154) OMB: Office of Management and Budget): 미국에서 연방프라이버시법의 이행에 관한 감독을 맡고 있는 행정관리예산처

다. 이 지침은 프라이버시법상 일상적인 사용규정에 의거하여 한 기관으로부터 다른 기관으로 컴퓨터연결을 통하여 개인정보의 전달을 정당화하는 것을 목표로 한다. 그런데 1979년 컴퓨터 프로그램에 관한 관리예산처의 지침은 이러한 연결프로그램이 개인의 프라이버시를 침해할 수 있는 위험성이 내재해 있음을 인정하였다.

문제는 프라이버시법과 관리예산처의 지침에 규정된 '일상적 사용'이란 규정을 통하여 컴퓨터연결프로그램이 정당화된다는 것이다. 결국 컴퓨터 프로그램과 이에 관한 통제실무가 부적절하다는 것은 이러한 컴퓨터연결에 내재해 있는 이해관계들을 토론하고 형량할 수 있는 확립된 기구나 광장이 없다는 데에 있다. 물론 이러한 컴퓨터연결법은 미국에서 현실적으로 수집되는 개인정보의 양을 감소시키고 수집되는 정보의 정확성을 확실히 높이는 좋은 결과가 없었던 것은 아니다. 그러나 개인정보를 보호하기 위해서는 행정부가 검색하여 연결할 수 있는 데이터베이스의 범위를 통제해야만 하는데 현재 관리예산처 내부에서 연결이 아니라 기관간 연결만을 그 대상으로 할 뿐이라는 데에 문제가 있다. 게다가 관리예산처의 지침은 권고적일뿐이며, 제정법 자체에 따르도록 구속할 수 없을 뿐만 아니라 관리예산처 자체가 충돌하는 이익들을 형량할 수 있는 기관이 아니라는데 문제가 있다고 생각한다.

(8) 시사점

미국은 프라이버시를 헌법적인 권리로 인정하고 있지만, 유럽국가들과는 달리 포괄적이고, 기본적인 개인정보 관련 법 체계를 기지고 있지는 않다.

미국의 프라이버시보호를 위한 규제방식은 자율규제적 접근방식을 채택하고 있다. 민간 부문에서 특별히 규제할 필요성이 인정되는 경우에만 법률을 제정할 뿐, 원칙적으로 업계가 자율적으로 개인정보보호를 위한 제도를 마련하도록 유도하고 있다. 자율규제적 접근방식은 개인정보를 인권으로 보아 국가가 적극 관여하여 보호해야 한다고 보는 유럽과는 다르다.

미국의 개인정보보호법제의 가장 큰 특색은 개인정보보호를 위한 지나친 정부관여는 정보기술의 발전과 기업체들의 자유로운 경제활동을 저해할 가능성이 크다고 판단하고 개인정보보호문제를 민간자율에 맡기고 자

율규제가 실패한 경우에만 정부가 개입해야 하는 것이다. 민간부문에 관해서는 자유로운 정보유통의 확보를 전제로 한 후에 개별분야별로 프라이버시보호를 목적으로 하는 법률을 제정하는 분야별 영역에 따라 보호법제가 정비되어 있다.

따라서 미국은 일반법이 아닌 개별법을 제정하고 있는데 개별법의 장점은 보호가 특히 필요한 개인정보를 취급하는 영역에 한하여 규제할 수 있다는 점이다. 그러나 개별 영역별로 법률을 제정하기 위하여 관련업계와 이익단체의 영향을 받기 쉽다고 하는 단점도 있다. 더욱이 분야별 영역에 따른 입법방식에 의한 개별법은 규제의 대상인 업계 단체로부터 영향뿐만 아니라 적극적인 로비 등으로 인해 정치적 상황에도 크게 좌우되기도 한다.[155] 결국 미국의 개인정보보호법제는 상황에 적절한 보호조치를 취할 수 있다는 장점도 있지만, 일반적인 기본원칙이 확립되지 않은 상태에서 발생하는 부작용은 우리나라의 개인정보보호법제에 대해서도 시사하는 바가 크다고 하겠다.

2) 독일의 개인정보보호법제

(1) 개인정보보호법제의 개관

독일 기본법상 프라이버시에 해당하는 명시적인 조항은 없다. 그러나 기본법에서 프라이버시 영역(Privatsphäre)의 보호에 관한 개별적 규정들은 존재한다. 예컨대, 독일기본법은 인간의 존엄성(제1조)[156]과 인격의 자유로운 발현(제2조)[157]을 프라이버시권에 대한 근거조항으로 들 수 있다. 또 서신・우편・통신의 비밀 보호(제10조)[158]와 주거의 불가침 보장(제13

155) 박문석, 앞의 논문, 257면; Joel R. Reidenberg, 2000.5.18. 미하원 Subcommittee on Court and Intellectual Property Committee에서의 진술서, p.3.

156) 독일기본법 제1조 ① 인간의 존엄은 불가침이다. 이를 존중하고 보호하는 것은 모든 국가권력의 의무이다. ② 독일 국민은 불가침·불가양의 인권을 세계의 모든 인간 공동체, 평화 그리고 정의의 기초로서 인정한다. ③ 기본권은 직접효력을 갖는 권리로서 입법권, 집행권, 사법권을 구속한다.

157) 독일기본법 제2조 ① 누구든지 타인의 권리를 침해하지 아니하고 헌법질서나 도덕률에 위반하지 않는 한, 자신의 인격을 자유로이 발현할 권리를 가진다. ② 누구든지 생명권과 신체를 훼손당하지 아니할 권리를 가진다. 신체의 자유는 불가침이다. 이 권리들은 법률에 근거해서만 침해될 수 있다.

158) 독일기본법 제10조 ① 서신, 우편, 전기통신의 프라이버시는 침해되어서는 안 된다. ② 이러한 프라이버시의 제한은 오직 법률에 의해서만 가능하다. 프라이버시의 제한이 독일연방국가의 자유로운 민주적 기본질서 및 실존과 안보를 보호하기 위한 것인 경우에는 그러한 프라이

조)[159]은 물론, 경우에 따라서는 신앙・양심・고백의 자유의 보장(제4조 제1 내지 2항)[160], 혼인・가족・아동(제6조), 의사표현의 자유(제5조), 집회의 자유(제8조), 결사의 자유(제9조) 등도 사적 영역의 특수한 보장과 연관을 가지는 것으로 이해가 된다.[161] 하지만, 독일기본법이 제정된 후 기본법에 열거된 구체적 기본권들을 통한 사적 영역의 보호는 흠결이 있고 충분하지 못해서, 사적인 영역에 속하는 인간의 형태와 상황들이 이러한 기본권으로부터 포괄적으로 보호되지 못하였다.

따라서 학설과 판례는 기본법 제2조 제1항에서 보장되는 일반적 행동자유 외에도 연방헌법재판소는 기존의 자유권들을 통하여 파악되지 않는 '협소한 인격적 활동영역'을 보호하기 위해 일반적 인격권(기본법 제1조 제1항과 결합한 제2조 제1항)을 발전시켰다.

이러한 헌법상의 근거에 바탕을 두고 국민의 개인정보를 보호하기 위한 기본법으로는「연방정보보호법(BDSG)」과「주정보보호법(LDSG)」이 있다. 그러나 이 법률들은 특수한 영역의 정보보호규정들이 개입하지 않을 때만 적용된다. 예컨대, 정보통신분야에 문제가 발생하면「정보통신서비스 정보보호법」이 특별법으로서 우선 적용된다. 독일의 정보보호관련 법률은 <표 4>와 같다.

버시의 제한에 대하여 당해 주체에게 고지할 필요가 없음을 법률로 규정할 수 있으며, 법원으로의 소제기는 의회에서 임명된 기구 또는 그 보조기구에 의한 사건 심사로 대체할 수 있음을 법률로 규정할 수 있다; 이창범・윤주연, 앞의 책, 138면 참조.

159) 독일기본법 제13조 ①주거는 불가침이다. ②수색은 법관에 의해서만 명해진다. 지체의 우려가 있는 경우에만 법률에 규정된 다른 기관에 의해서도 명하여지며 법률에 규정된 방식으로만 행해질 수 있다. ③그 밖에도 침해와 제한은 공동의 위험이나 개인의 위험을 방지하기 위해서만 법률에 근거하여 공공의 안전과 질서에 대한 급박한 위험을 방지하기 위해서 특히 주택난을 덜기 위해서 전염병의 위험을 극복하기 위해서 또는 위험에 처한 소년을 보호하기 위해서도 행해질 수 있다.

160) 독일기본법 제4조 (신앙, 양심과 고백의 자유, 병역거부) ①신앙과 양심의 자유 그리고 종교적·세계관적 고백의 자유는 불가침이다. ②종교행사를 방해받지 않을 자유는 보장된다. ③누구도 양심에 반하여 집총병역을 강요당하지 아니한다. 상세한 내용은 연방법률로 정한다.

161) Dietwalt Rohlf, Der grundrechtliche Schutz der Privatsphäre, (1980), S. 136ff; Klaus Vogelgesang, Grundrecht auf Informationelle Seldstbestimmung?, (1987), S. 89ff.

<표 4> 독일 국내법상의 정보보호관련 현행법률

정보통신법	정보통신법(TKG) : Telekommunikationsgesetz
연방데이터보호법	연방데이터보호법(BDSG) : Bundesdatenschutzgesetz
통신서비스데이트보호법	통신서비스데이트보호법(TDDSG) Teledienstedatenschutzgesetz
통신서비스이용법	통신서비스이용법(TDNG) : Teledienstnutzungsgesetz
연방정보기술안전청설치법	연방정보기술안전청설치법(BSIG) : BSI-Errichtungsgesetz
방송시설및정보통신최종시설에관한법률	방송시설및정보통신최종시설에관한법률(FTEG) :Funkanlagen-Telekommunikationsendeinrichtungsgesetz
형법전	형법전StGB : Strafgesetzbuch (제11조, 제86조, 제86a조, 제111조, 제130-131조, 제138조, 제184-185조, 제202a조, 제203조, 제206조, 제263조, 263a조, 제269조, 제303a조, 제303b조, 제317조)
진입통제서비스보호법	진입통제서비스보호법(ZKDSG) : Zugangskontrolldiensteschutzgesetz
사이버범죄협정	사이버범죄협정(CoC) : Convention on Cybercrime
형사소송법	형사소송법(StPO) : Strafprozeßordnung(제94조, 제100a-100d조, 제100g-100i조, 제102조, 제103조)
영업조직법	영업조직법 : Betriebsverfassungsgesetz(제87조)

*이창범, 미국, 독일, 일본의 정보보호법 체계에 관한 연구, 한국정보보호진흥원, 2006, 109-110면 참조.

(2) 개인정보보호법재의 주요내용

독일「연방정보보호법」의 주된 내용은 정보주체의 권리와 정보처리자의 각종 의무, 제3국으로의 정보이전, 비디오 감시, 익명성과 가명성, 스마트카드, 민감한 정보의 수집 등이다.

이 특징으로는 다음 것을 들 수 있다. 첫째, 공공기관이 개인정보를 수집・처리・이용하거나 또는 사인이 영리적・업무상의 목적으로 개인정보를 수집・처리・이용하는 경우에 적용된다.[162] 둘째, 연방정부에 의하여 수집된 개인정보는 당사자의 동의가 있는 경우 또는 연방정보보호법이나 기타 법규에서 허용하는 경우에만 정보를 처리 및 이용할 수 있다.[163] 셋째, 정보와 관련한 공공기관의 책임은 중대한 인격권 침해의 경우에 위험책임을 규정하고 있다.[164]

162) §1 Abs 2 BDSG
163) §4 Abs 1 BDSG
164) §7 Abs. 1, 2 BDSG; Güter Schlegelmilch, Der Haftpflicht Prozeß, 22 Aufl., C.H.Beck,

「연방보호법」은 연방차원의 개인정보보호법으로서 원칙적으로 독일 전역에서 이루어지는 모든 개인정보의 수집·처리·이용에 대하여 적용된다. 그리고 법의 보호법익이 일반적 인격권임을 분명하게 규정하여 정보남용으로부터 개인을 보호하는 것에만 한정되지 않는다는 것을 밝힘으로써, 그 보호목적을 확대하고 구체화하였다. 또한 법률의 적용범위를 정보의 조사로부터 처리(저장, 변경, 유통, 삭제, 이용)를 거쳐 익명화될 때까지로 규정하고 있어 모든 개인관련정보의 자동화된 정보처리뿐만 아니라 수기문서도 그 정보의 범위에 포함시키고 있다. 또한 특정되거나 특정 가능한 자연인의 인적·물적 관계에 관한 일체의 정보도 포함한다.

이 법 제2장에서는 정보주체의 권리를 규정하고, 정보주체의 접근권(제19조, 제34조), 통지받을 권리(제19조a), 정정·삭제·통제요구권(제20조, 제35조), 이의를 제기할 권리(제20조 제5항)에 대해 규정하고 있다. 특히 제6조에서 이러한 정보주체의 권리는 계약 등 다른 법률행위에 의해 배제되거나 제한될 수 없는 불가침의 권리임을 명백히 밝히고 있다는 점이 특징이다.

또한 이 법은 개인정보처리자가 준수해야할 사항에 대해서도 규정하고 있는데, 개인정보처리자는 연방정보보호청에 개인정보처리와 관련된 소정의 사항을 고지하고 등록할 의무를 가진다. 하지만 이러한 등록의무는 해당 개인정보처리자가 내부적으로 개인정보관리책임자(data protection officer)를 임명하였을 경우에는 면제된다.[165]

또한 개인정보자기결정권을 보호하기 위하여 개인관련정보의 처리·이용 등에 대한 목적구속의 원칙이 엄격하게 규정되어 있다. 공적 영역은

1997. S. 505~506.

165) 내부 개인정보관리책임자(Data Protection Officer)란 연방이나 주의 각 행정칠 혹은 연방정보보호법이나 주법의 적용대상이 되는 민간기업체에서 내부적으로 개인정보가 올바르고 공정하게 처리되고 있는지를 관리하고 조사·심사하는 자를 의미한다. 이러한 내부정보관리책임자는 필요한 경우 자동화된 개인정보의 처리가 정보주체의 권리와 자유에 특별한 위험을 가져올 것으로 의심될 때에는 사전검사(Prior checking)를 할 수 있으며, 그 결과 개인정보처리에 문제가 있다고 판단될 때는 관계 감독청에 신고할 수 있다. 개인정보관리책임자는 이로 인해 고용관계에 있어서 불이익을 받지 않도록 보호받고 있다. 사실상 정보보호법 제4f조에 의하면, 자동화된 개인정보파일을 처리하는 모든 공공·민간기관 또는 비자동화된 개인정보파일을 처리하는 곳이라도 개인정보처리를 위해 최소 20명 이상의 인원이 고용되는 단체에서는 내부 개인정보관리책임자를 임명하여야 하기 때문에 상당수의 정보처리자가 이러한 등록의무에서 면제된다고 볼 수 있을 것이다. 다만, 이 경우에도 제한이 있는데 정보처리자가 영리목적으로 정보를 전송하기 위해 또는 익명화된 정보전송을 위해 개인정보를 저장하고 있는 경우에는 등록의무 면제사유에 해당되지 않는다. 연방정보보호법 제4d조 제4항.

물론이고 개인정보의 처리와 이용에서도 목적구속의 원칙이 특별히 강조되어 있다.

또한 자동화된 호출절차(automatisierte Abrufverfahren)로부터 개인정보를 보호하는 규정과 전체적인 온라인연결을 통해 자동적으로 개인정보가 전달되는 것을 허용하지 않고, 정보를 받는 기관이 저장한 기관에게 정보를 사실상 호출한 경우에 비로소 전달되도록 하였다. 그리고 공공기관에 적용되는 특별한 책임구성요건에 대하여 개인정보보호에 관한 다른 규정에 반하여 허용되지 않거나 정당하지 않은 방법으로 관련자의 개인관련정보를 처리한다면 해당 기관의 관련자에게도 손해배상책임을 부과하고 있다.[166]

(3) 개인정보보호기구

독일은 연방차원의 개인정보보호법인「연방정보보호법」이외에도 州차원에서 각각 개인정보보호법이 마련되어 있고, 이를 바탕으로 개인정보보호기구들이 설치되어 활동 중이다.

연방에서는 연방정보보호청(BfD: Bundesbeauftragter für den Datenschutz)이 주로 연방공공기관을 중심으로 규율하고 있다. 연방정보보호청은 1977년「연방정보보호법」에 따라 설립된 법정기구로,「연방정보보호법」과「전자통신법」을 관장하고 있다.

현재 독일 16개 州의 개인정보보호기구는 州공공기관의 정보처리에 대해 규율하고 있다. 또한 일부 영역을 제외한 대부분의 민간부문에서는 민간 감독기구를 설치하여 사적 영역의 개인정보처리에 대해 관리·감독 하고 있다. 연방정보보호청의 행정조직상으로는 연방 내무부 소속으로 예산이나 인력자원과 같은 행정적 사안에 대해서는 연방 내무부 장관으로부터 지원을 받으나, 직무수행에 있어서는 법률에 따라 독자적으로 활동할 수 있도록 보장받고 있다. 독일 연방정보보호청의 주요기능은 다음 <표 5>와 같다.

166) 한국전산원, 개인정보보호법제 정비를 위한 기본법 제정방안 연구, 한국전산원, 2004, 77면.

<표 5> 독일 연방정보보호청의 주요기능

구분	주요 기능
정보처리 등록	• 개인정보처리자로부터 소정의 사항을 신고 받아 등록
법규준수 조사·감독	• 연방정부 등의 정보보호법 준수실태 모니터링 • 의회·연방정부의 요청시 정보보호시스템에 대하여 조사 • 위반행위에 대해 시정·권고
피해구제	• 연방정부 등을 상대로 한 각종 개인정보침해신고접수 • 자료제출요구 및 현장조사 등을 통한 사실조사 • 침해행위자에 대하여 시정조치, 원상회복 등 권고 • 정보주체의 접근·정정·삭제요청 등을 대신하여 행사
정보제공	• 개인정보보호 모니터링 결과에 대한 정보제공 • 정보주체, 정보처리자 등의 권리·의무에 대한 지침제공
법률·정책자문	• 정부에 대하여 정책자문 • 매2년마다 연차보고서 작성 및 연방의회 보고 • 의회·정부 요구시 의견서, 조사서, 보고서 작성 및 제출 • 법률자문 및 권고
교육·홍보	• 개인정보보호를 위한 교육실시 • 언론보도자료 배포 및 각종 위원회 발간물 작성
국내외 협력	• 州개인정보보호기구 및 민간영역의 감독기구와 협력 • 국제협력 강화

*이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 146면.

연방정보보호청의 구성원은 연방정부의 제청에 따라 연방의회에서 과반수의 동의를 얻어 선출되며, 선출된 자는 연방 대통령이 임명한다. 연방정보보호청의 장은 선출 당시 35세 이상이어야 하고 임기는 5년으로 1회에 한하여 재임할 수 있다. 연방정보보호청은 기관장을 중심으로 약 70명의 직원이 활동하고 있으며, 총 8개[167] 부서로 나누어져 있고, 개인정보의 수

167) 제1부는 업무총괄 및 국제협력을 맡고 있으며, 제2부에서 제8부는 각 영역별로 개인정보보호 업무를 담당하는 부서로 구분되어 있다. 제2부는 법제・금융・노동행정・국방・민원서비스・외국인 대상업무에 대한 정보보호 감독업무를 행하고 있으며, 제3부는 사회복지분야의 개인정보보호 문제 및 정보보호 협력업무를 행한다. 제4부에서는 경제・의료서비스・교통・우편・통계관련 개인정보보호업무를 담당하며, 제5부는 경찰・방송・업무담당, 제6부는 기술안전정보보호 및 정보기술과 정보안전을 담당한다. 제7부는 일반 내무행정과 관련된 개인정보보호 및 형법 관련업무, 신고제 담당업무 등을 행하며, 제8부는 통신・전화 및 의료와 관련된 정보보호업무를 담당한다. 이 외 ZA(Zentrale Aufgaben)는 사무국의 인사행정과 예산수립 및 집행업무를 담당하며, 홍보부(Pressearbeit)는 미디어와 집중적인 접촉과 기자의 질문에 답변하는 업무를 담당한다. 또한 연방정보보호청에도 역시 조직 내부의 개인정보보호업무를 담당하는 내부 정보보호관리책임자가 임명되어 있다. 이창범・윤주현, 각국의 개인정보피해구

집·처리·사용과 관련하여 연방정보보호법이 적용되는 범위 내에서 활동하지만, 주의 개인정보보호기구와 각 주에서 설립한 민간 정보보호감독기구의 업무범위를 제외한 범위에서 활동한다.

연방정보보호청의 주요기능은 연방정보보호법의 일반적인 목적에 따라 개인정보의 처리로 인한 개인의 권리침해에 대하여 당해 개인을 보호하는 것이다. 따라서 개인정보를 수집·이용·처리하는 연방정부 및 공공기관에 대하여 규제하고 관리·감독하는 임무와 연방정부 및 공공기관을 상대로 제기된 불만이나 민원신고를 접수하여 처리하고 관할 영역에 해당되는 기관들의 개인정보처리현황을 조사·감독하는 기능을 주로하고 있다.

3) 영국의 개인정보보호법제

성문헌법이 없는 영국은 당연히 프라이버시권 또는 개인정보자기결정권에 대한 명시적·묵시적인 헌법상의 근거를 가지고 있지 않다. 그러나 영국은 1215년 마그나카르타(Magna Carta)에서 시작하여 인권선언의 의미를 가지는 권리청원(Petition of rights)과 권리장전(Bill of rights)의 제정을 거치면서, 시민들의 사적 자유와 인권을 존중하는 법제도 도입에 선구적인 역할을 해왔다. 이러한 인권존중의 법적 전통은 당연히 프라이버시 및 개인정보의 법적 보호로 이어져「1984년 정보보호법(The Data Protection Act 1984)」을 제정·시행하게 되었다.[168] 이 법은 개인정보보호법제에 해당되는 것으로 개인들에게 다른 사람들이 자신에 관한 어떤 정보를 가지고 있는지의 알 권리를 부여하고, 또한 개인정보를 적절히 취급하도록 한다.[169] 그리고 개인들에게 타인이 보유하고 있는 자신에 관한 정보에 대해 접근할 권리를 부여하고 있는데, 이에 관해서는 예외가 존재한다. 또한 개인정보처리과정에서 개인정보처리취급자들에게 개인정보보호의 8원칙을 준수할 책임과 적절한 보안조치를 취할 의무를 부과하고 있다.

이 법은 또한 개인정보를 보유하고 있는 자는 정보커미셔너에게 이를 등록하도록 하고 있으며, 등록할 때에는 그 정보처리의 목적과 정보의 유형·등급 및 그 출처 또는 수신자에 관한 사항을 포함하도록 하고 있다.

제제도 비교연구, 개인정보분쟁조정위원회, 2003, 144면 참조.

168) 이창범·윤주연, 위의 책, 109면; 한국전산원, 앞의 주 163, 97면 등.

169) http://www.opsi.govuk/acts/acts1998/ukpga 19980029 en 1 2009.12.3.방문.

(1) 정보보호 법제현황

영국은「1984년 정보보호법」을 제정함으로써 개인정보를 위한 첫 번째의 기초를 마련하였다고 볼 수 있다. 하지만 이 법은 일반적인 개인정보보호에 중점을 두기보다는 개인정보를 처리하는 공공기관이나 사업자 등을 등록하여 정보처리자등록부를 유지·관리하는 데 더 큰 비중을 두고 있다. 이 후 1995년「EU 지침」이 제정되면서, 영국도 이 지침의 내용에 맞추어 국내법을 전면 수정해야만 했다. 이 때 제정된 법률이「1998년 정보보호법(The Data Protection Act 1998)」이다. 그러나 이 법 역시 개인정보보호의 기본법으로서 적용범위가 광대할 뿐만 아니라 개인정보보호 기본원칙을 비롯한 개인정보와 관련된 사항을 포괄적으로 규정하고 있었다. 그리고 기본법의 특성상 각 개별 영역의 특수한 개인정보 처리상황을 모두 규율하고 있지는 않고, 특정영역에 관하여는 다른 특별법이나 하위법령에 위임하고 있다.

개인정보보호를 포함하고 있는 하위법령은 전자통신 분야에서「1999년 전자통신(정보보호 및 프라이버시)규칙(The Telecommunications(Data Protection and Privacy) Regulations)」,「2000년 조사권에 관한 법률규칙(The Regulations of Investigatory Powers Act 2000)」,「2000년 전기통신규칙(합법적인 사업관행) (통신차단)(The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations)」이 있다.

이 중「1999년 전자통신규칙」은 종합정보통신망(ISDN), 공공디지털모바일네트워크(public digital mobile network), 주문형 비디오(VOD), 쌍방향 TV 등 새로운 전자통신 분야에서의 개인정보보호를 위해 제정된 것으로, 원하지 않는 팩스 또는 전화와 같은 스팸통신에 대하여 규제하고 있다.[170] 또한「2000년 조사권에 관한 법률규칙」은 EU 전자통신 분야에서의 정보보호지침 제5조의 내용을 시행하는 별도의 입법으로 공공·민간 네트워크를 통한 전자통신의 비밀을 보호하기 위해 제정된 것이다.[171] 이

170) 이 법은 2003년 12월 11일부로「2003 프라이버시와 전자상거래 규칙(EU Directive)(The Privacy and Electronic Communications (EC Directive) Regulations 2003」으로 대체되었다. 새롭게 제정된 규칙은 전자상거래의 발달상황의 규율을 위해 1999년 규칙보다 기술과 프라이버시에 관한 사항을 많이 포함하고 있다.http://www.dca.gov.uk/ccpd/dpsubleg.html 2009.12.3.방문.

171) Gerald Spindler/Fritjof Börner(Edit),"E-Commerce Law in Europe and the USA",

밖에 정보주체가 신용정보회사 등 평가기관에서 보유하고 있는 각종 개인정보에 대하여 접근권을 행사할 수 있도록 규정한「1974년 소비자신용법(The Consumer Credit Act 1974)」, 자신의 건강 정보 또는 치료기록에 대한 접근을 요청할 수 있도록 한「1988년 의료기록 접근에 관한 법률(The Access to Medical Reports Act 1988)」,「1990년 건강기록 접근에 관한 법률(The Access to Health Records Act 1990)」등의 법률이 있다. 또한「1998년 정보보호법」의 하위법령으로 국가안보, 형사, 세금, 의료, 교육, 사회사업, 언론 등 특정 영역을 규율하는 규칙을 제정하여 시행하고 있다.[172]

<표 6> 영국의 개인정보관련 법제현황

구 분	법 률
개인정보	• 「1998년 정보보호법(The Data Protection Act 1998)」
정보공개	• 「2000년 정보자유법(The Freedom of Information)」
전자통신 분야의 정보보호	• 「1999년 전자통신(정보보호 및 프라이버시)규칙(The Telecommunications(Data Protection and Privacy) Regulations 1999(1999/2093)」 • 「2000년 조사권에 관한 법률규칙(RIPA 2000 : The Regulations of Investigatory Powers Act 2000)」 • 「2000년 전자통신규칙(합법적인 사업관행)(통신차단)(The Telecommunications(Lawful Business Practice)(Interception of Communications) Regulations 2000(2000/2699))」
신용정보	• 「1974년 소비자신용법(The Consumer Credit Act 1974)」
형사기록	• 「1997 경찰법(The Police Act 1977)」
의료정보	• 「1988년 의료기록 접근에 관한 법률(The Access to Medical Reports Act 1988)」 • 「1990년 건강기록 접근에 관한 법률(The Access to Health Records Act 1990)」
공적비밀법	• 「공적비밀법(Official Secrets Act 1989)」
공문서법	• 「공문서법(Public Records Act 1958 and 1967)」
프라이버시와 전기통신규칙	• 「2003년 프라이버시와 전기통신(EU 지침)규칙 (Privacy and Electronic Communication (EC Directive) Regulations 2003)」
인권법	• 「인권법(Human Rights Act 1998)」

Springer, (2002), p. 298.

172) 이창범・윤주연, 앞의 책, 111면 참조.

컴퓨터 오용법	• 「컴퓨터오용법(Computer Misuse Act 1990)」
저작권(컴퓨터 프로그램)규칙	• 「저작권(컴퓨터프로그램)규칙(Copyright(Computer Program) Regulations 1988)」
민사증거법 및 경찰·형사증거법	• 「민사증거법 및 경찰·형사증거법(Civil Evidence Act and Police and Criminal Evidence Act 1968)」
무선전신법	• 「무선전신법(Wireless Telegraphy Act 1949)」
통신법	• 「통신법(Communication Act 2003)」
전자상거래지침	• 「전자상거래지침(Directive on Electronic Commerce 2000)」
전자서명규칙	• 「Electronic Signatures Regulations 2002)」
수사권한법	• 「수사권한법(Regulations of Investigatory Power Act 2000)」
전기통신(합법적인 업무행위)(통신감청)규칙	• 「전기통신(합법적인업무행위)(통신감청)규칙 (Telecommunications(Lawful Business Practice) (Interception of Communication Regulations 2000)」
테러방지법	• 「테러방지법(Terrorism Act 2006)」

*이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 111면.

(2) 정보보호 법제의 주요내용

앞서 살펴본 바와 같이 영국에서 개인정보보호를 주된 목적으로 하는 법률은「1998년 데이터보호법」이다. 이 법의 대상영역은 공공부문 및 민간부문 모두이고, 대상이 되는 영역은 이 법이 대상으로 정한 자동처리된 데이터뿐만 아니라,「EU 지침」제3조가 요구하는 비자동적인 수단에 의한 개인 데이터도 대상에 포함되기 때문에 자동처리를 실행하는 장치를 이용하지 않고, 관련되는 파일링시스템의 일부로서 기록되는 데이터도 적용대상으로 하고 있다.[173]

이 법의 특색은「EU 지침」의 거의 모든 요구사항을 상세하게 규정하고 있다는 것이다.[174]

이 법 제1조에서는 공공부문과 민간부문을 불문하고 자동처리된 데이터, 자동처리를 목적으로 기록된 데이터 및 저장시스템의 전부 혹은 일부

173) Fred H. Cate, Privacy in the Information Age, D. C. : Brookings Institution Press, (1997), p.196.
174) 백윤철, 앞의 주 100), 668면.

를 구성하는 것을 목적으로 기록된 데이터를 적용대상으로 하고 있다. 그리고 이 법의 가장 큰 특징은 개인정보의 수집·처리 등을 규율하기 위한 정보보호 8원칙을 세부적으로 규정하고 있는 것을 들 수 있다.

이 법 제4조에서는 개인정보보호의 적용대상에 대하여 다음과 같은 8원칙을 제시하고 있다.

① 동의원칙: 데이터 주체의 동의가 있는 경우 또는 데이터 주체가 당사자로 계약의 이행 혹은 법률상의 의무이행을 위해 필요한 경우에만 처리가 허용된다. 또한 개인 데이터의 처리에 있어 데이터 주체에 대하여 데이터 관리자, 처리목적 등의 정보가 제공되고 있는 경우 적정하게 취득되어진 것으로 취급한다.

② 목적제한의 원칙: 개인 데이터는 명시된 적법한 목적에 한해 취득되어야 하고, 당해 목적에 반하는 방법에 의해 처리되어서는 아니된다.

③ 상응성의 원칙: 개인 데이터는 목적과 관련하여 적정하게 상응하지 않으면 안된다.

④ 정확성의 원칙: 개인 데이터는 정확하고 또한 필요한 한도에서 최신의 것이 아니면 안된다.

⑤ 보존 필요성의 원칙 : 개인 데이터는 처리목적에 필요한 기간 내에 있어서만 보존할 수 있다.

⑥ 데이터 주체의 권리의 원칙: 개인 데이터는 법이 정하는 데이터 주체의 권리에 종속하여 처리되지 않으면 안된다.

⑦ 안전보장조치의 원칙: 개인 데이터의 안전보장을 도모하기 위하여 적절한 기술적, 조직적 조치가 강구되지 않으면 안된다.

⑧ 데이터 이전제한의 원칙: EU 영역 외의 국가 등에 대해서는 개인 데이터의 처리에 관해 데이터 주체의 권리 및 자유를 위한 적절한 보호가 보장되지 않으면 당해 국가 등에 개인 데이터를 이전하지 못한다.

(3) 개인정보보호법의 적용 시스템

「1998년 데이터보호법」은 위와 같은 실체적 내용 외에 개인정보보호를 위한 행정적인 조치에 관해서도 규정을 두고 있다.

첫째, 이 법 제17조 및 제18조는 데이터 운영자에 대하여 개인 데이터를 처리하는 경우에 데이터 관리자의 성명, 개인 데이터의 내용 및 데이

터 주체, 처리목적 등을 데이터보호위원회에 신고하도록 하는 등록제도를 두었다.

둘째, 그리고 데이터보호위원회를 독립된 기관으로 설치하여 데이터보호법의 실시를 관리·감독하는 임무를 부여하였다. 이 위원회는 ① 등록부의 보전 및 이용의 기회를 제공하는 것, ② 법률에 관한 정보 및 법률의 역할을 보급하는 것, ③ 데이터 보호의 제원칙의 준수를 촉진하는 것, ④ 데이터보호의 원칙에 따른 데이터 이용자의 지침으로 된 실무 강령의 책정을 추진하는 것, ⑤ 데이터보호 위반 내지 데이터보호법 위반에 관한 불만을 처리하는 것, ⑥ 위반자의 소추 또는 경고 등의 업무를 수행한다.

셋째, 데이터보호위원회는 데이터보호법이 준수되도록 하기 위해 이 법 각 조항의 집행뿐만 아니라 데이터보호위원회의 조언에 기하여 데이터 관리자에 의한 자주적인 조치가 필요한 경우 그 임무를 수행할 수 있다.

넷째, 데이터보호위원회의 사무국은 데이터보호위원회에 설치하고 약 100명의 직원을 임용하고 있으며, 데이터보호위원회의 결정에 대한 불복을 심사하는 기관으로서 데이터보호심판소도 설치하고 있다.[175]

다섯째, 영국은 개인정보를 보호하기 위하여 1984년부터 데이터보호등록관(Data Protection Registrar)을 설치하여 자국 내에서 이루어지는 모든 개인정보처리행위를 사전 등록함으로써 개인정보를 보호해왔으며, 그 후 데이터 보호 커미셔너(Data Protection Commissioner)로 명칭을 바꾸었다. 그리고 2000년에는 정보 커미셔너(Information Commissioner)로 변천되어 오늘날에 이르고 있다.

정보커미셔너는 여왕의 특허장에 의하여 임명되며, 5년간의 임기를 보장하며 연임이 가능하다. 공공부문과 민간부문의 개인정보처리를 관할 대상으로 삼고 있으며, 온라인과 오프라인을 구분하지 않고, 일반 사업자에 의한 개인정보처리나 정부부처 등 공공기관에 의한 개인정보처리가 올바르게 이루어지고 있는지를 감시하고 규율하는 역할을 하고 있다.[176] 정보커미셔너의 주요기능으로는 관보(public register)에서 정보처리와 관련된 내용을 고지 받아 기록하고 유지·관리하는 기능과 각종 개인정보침해사건이나 사업자 또는 공공기관 등의 개인정보처리행위에 대한 불만사항을 접수하여 당사자 간의 분쟁을 해결하고, 피해자를 구제해 주는 기능을 담

175) 백윤철·이창범·장교식, 개인정보보호법, 한국학술정보, 2008, 279-283면.
176) 이창범·윤주연, 앞의 책, 115면.

당한다. 이 외에도 개인정보에 관한 각종 지침이나 규칙 제정, 법률 및 기술자문, 사업자 또는 소비자를 대상으로 한 정보제공, 교육·홍보 및 개인정보보호를 위한 조사연구, 유관기관 협력 등의 기능을 수행하고 있다.[177]

<표 7> 영국 정보커미셔너의 조직도

정보커미셔너 & 비서실					
부 커미셔너 Deputy Commissioner	부 커미셔너 Deputy Commissioner	법률자문가 (Legal Advisor)	인사회계국 (Personnel & Finance Director)	전략정책 보조 커미셔너 (Assistant Commissioner Strategic Policy)	마케팅 홍보국 (Marketing & Communication Director)

※이창범·윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 116면.

<표 8> 영국 정보커미셔너의 주요기능

주요기능	세부 내용
등록업무	• 고지 접수를 통한 개인정보처리, 등록업무 처리
피해구제	• 각종 불만사항이나 개인정보침해사건 접수 • 당사자 자료제출요구, 의견청취, 현장조사 등을 통한 사실조사 • 사실조사를 바탕으로 한 법규위반 여부 심사 • 민원심사과정에서 화해권고 등 개인정보 분쟁조정 • 법률위반사항에 대해 시정조치명령 또는 이행고지, 정보고지 부과 • 불이행시 정보법원에 소송지원 또는 형사기소
정보공개	• 정부, 공공기관 등에 대한 정보공개명령권 행사
조사·감독	• 프라이버시 침해여부에 대한 직권 실태조사 및 모니터링 • 정보보호원 및 법규 준수여부 감독 • 개인정보침해행위 및 법률위반사항에 대하여 이행명령(고지) 부과 • 이행명령 불이행시 및 법규위반 확인시 검찰 등 해당기관 고발
실행규약제정	• 각종 개인정보보호 실행규약(Code of practice)의 제정 및 고시
정보제공	• 개인, 사업자, 정부, 공공기관에 대하여 각각 정보제공 및 자문 • 정보처리자 요청시 법률상담 및 평가정보 제공
정책 및 입법자문	• 개인정보 관련 법안 심의 및 의견제시 • 정부의 각종 정책에 대하여 의견제시 및 자문
개인정보 보호연구	• 개인정보 관련기술 동향 조사 및 연구
교육·홍보	• 각종 단체에 대한 개인정보보호교육 실시 • 개인정보보호 공공캠페인 실시 • 언론 등에 대한 프라이버시커미셔너 활동 등 홍보
유관기관 협력	• 국내 개인정보 유관기관 및 시민단체와의 협력 • EU 등 해외 개인정보보호기구와 국제협력

*이창범·윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 117면.

177) 한국전산원, 앞의 주 163), 71면.

4) 일본의 개인정보보호법제

(1) 일본의 개인정보보호의 개관

일본헌법에는 개인정보보호에 관한 명시적 조항은 없지만, 제21조와 제35조에서 간접적으로 인정하고 있다. 일본헌법 제21조는 집회・결사 및 언론・출판과 기타 표현의 자유를 보장한다고 규정하고 있으며, 제35조에도 정당한 사유 또는 조사와 압류를 위해 특별히 지정된 장소를 제외하고 모든 국민이 가지는 주거, 문서 및 사유재산의 자유를 보장하며, 각각의 조사와 압류는 필요한 별개의 정당한 사유에 의거하여 소관 법관에 의해 행할 수 있다고 명시하고 있다.[178]

그러나 개인정보보호에 관한 기본법은 제정되어 있지 않았다. 그러던 중 1970년대의 자치단체사무의 컴퓨터 도입과 관련하여 소위 전산처리조례[179]를 효시로 하는 프라이버시를 의식한 조례들[180]이 제정되기 시작함에 따라 조례를 중심으로 한 프라이버시 보호법제가 등장하였다.

한편, 일본에서는 1950년대부터 개인의 사생활과 사적 사항에 대하여 프라이버시권의 이름으로 연구가 행해져왔으나, 일반국민에게까지 알려지게 된 것은 만찬 후(宴のあと) 사건[181] 이후이다.[182]

1970년 중반에 들어서는 프라이버시에 관한 외국의 입법동향, 행정과 프라이버시의 보호, 개인정보보호에 관한 입법요강 등을 집중적으로 논의하게 되었는데, 이것은 프라이버시보호에 있어서 당시의 국제수준을 명확하게 하고, 개인정보보호와 관련한 다양한 논의와 입법적 기준을 제시하였으며, 이후의 프라이버시에 대한 논의에 큰 영향을 미쳤다. 당시 프라이버시보호의 제도화가 주장되었으나, 현대적인 프라이버시권의 개념으로는 이해하지 못하고, 프라이버시 보호는 표현의 자유를 제약하는 것이라고 인식되기도 하였다.

1970년대 중반부터 시작된 개인정보보호를 제도화하려는 움직임은 1980년대에 접어들면서 더욱 가속화되었다. 특히 1970년대에 제정된 각국의

178) http://www.ntt.co.jp/japan/constitution/englich-Costirution.html 2009.12.3.방문.
179) 1975년 國立市의 '電子計算器組織の運營に關する條例'가 유명하다.
180) 福島縣春日市의 '個人情報保護條例'(1984), 川崎市의 '個人情報保護條例'(1985) 등.
181) 判例時報 第385號(1964年) 12頁; 이 사건에 대하여 동경지방재판소는 프라이버시권을 "사생활이 함부로 공개되지 않도록 하는 법적 보장 내지 권리"라고 이해하였다.
182) 이자성, "일본의 개인정보보호제도에 관한 고찰 -개인정보보호조례를 중심으로-", 한국행정학회 2007년도 추계학술대회 발표논문집(下), 한국행정학회, 2007, 769면.

개인정보보호에 관한 법률들은 개인정보보호에 대한 보호의 정도나 수준에 차이가 있어서 국제간의 자유로운 데이터의 유통에 장애가 생기고, 그것은 경제활동에도 영향을 미치게 되었다. 이에 경제협력개발기구(OECD)는 1980년 9월「프라이버시보호와 개인 데이터의 국제적 유통을 규율하는 지침에 관한 이사회 권고」를 채택하였다. OECD의 회원국인 일본에서는 OECD 이사회 권고 8원칙을 기본전제로 하면서 당시 일본의 실정도 고려하여 국가 수준에서 입법화할 필요성을 가졌으며, 지방자치단체도 영향을 받았다.[183]

이처럼 프라이버시 권리를 보호하기 위하여 개인정보보호제도를 도모할 필요성이 예전부터 지적되어 왔으나, 정부는 여전히 적극적인 자세를 보이지 않았다. 그러나「주민기본대장법」개정을 계기로 국민들 사이에 개인정보보호를 요구하는 목소리가 높아지고 정부는 개인정보보호법제의 존재방식에 관하여 검토할 것을 결단하였다. 개인정보보호기본법제의 검토의 직접적인 계기가 된 것은 1999년의「주민기본대장법」개정이었다. 이 개정은 모든 주민에게 주민표코드번호를 부여하고 주소, 성명, 성별, 생년월일이라는 일정한 정보(본인 확인 정보)를 주민기본대장을 관리하는 시(市)・정(町)・촌(村)의 틀을 넘어 광역적으로 이용할 수 있게 하였다. 이는 주민과 행정 모두에게 일정한 편리를 도모하지만, 그 편리함의 이면에는 개인정보가 하나의 식별번호를 연결점으로 하여 관리됨으로써 개인에 관한 정보가 각각의 정보의 수집목적을 넘어 망라적・포괄적으로 이용되는 것이 아닐까하는 강한 의구심을 일으키게 되었다. 이것이 국민총배번호제 그 자체는 아닌지 또는 그 자체로서는 국민총배번호라고는 말할 수 없어도 실질적으로 이를 향한 길을 열어놓은 것은 아닌지 하는 것이다. 또한 이러한 정보가 민간사업자에 의해 이용될 경우 민간사업자 사이에서도 포괄적인 개인정보 데이터베이스가 작성되는 것은 아닌가 하는 염려도 있었다. 그 때문에 이 법의 개정을 계기로 현행 개인정보보호법제의 검토를 요구하는 소리가 강하게 나온 것이다.

그 결과 국회에서는「주민기본대장법의 개정에 관한 법률안」이 제출되고, 청문회를 거쳐 2003년 5월 23일, 5개의 개인정보보호관련법률을 제정

183) 堀部政男(編), 情報公開制度·個人情報保護制度の回顧と前望, 情報公開·個人情報保護, ジェリスト增刊, 1994. 5., 9-11頁; 김배원, "일본의 개인정보보호법제의 최근 동향 -개인정보보호에 관한 법률안을 중심으로-", 공법학연구 제3권 제2호, 한국비교공법학회, 2002, 89면.

하여 개인정보보호법제를 정비하였다. 이러한 법들은「개인정보보호에 관한 법률」,「행정기관이 보유하는 개인정보의 보호에 관한 법률」,「독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률」,「정보공개·개인정보보호심사회 설치법」,「행정기관이 보유하는 개인정보의 보호에 관한 법률 등의 시행에 따른 관계법률의 정비에 관한 법률」이다. 이 법들은 2005년 4월부터 전면적으로 시행되고 있다.[184] 이 외에도 정보보호에 관한 관련 법률로서「전기통신사업법」,「특정전기통신서비스제공자의 손해배상 책임의 제한 및 발신자 정보의 개시에 관한 법률」,「특정 전자메일 송신의 적정화 등에 관한 법률」등이 있다.

(2) 개인정보보호법의 주요내용

전술한 바와 같이 일본의「개인정보보호에 관한 법률」은 2003년 5월 23일에 국회에서 의결되어 5월 30일에 공포되었다. 이 법률은 6장 59조 및 부칙으로 구성되어 있다. 이 중 제1장에서 제3장까지는 개인정보보호의 기본법 부분이고, 제4장부터 제6장까지는 민간부분을 대상으로 하여 구체적인 권리의무가 규정된 일반법 부분이지만 법문상으로는 양자를 구분하고 있지는 않다.[185] 전자의 기본법 부분은 모든 경우에 적용되는 기본이념(제3조)을 중심으로 하고 있고, 후자의 일반법 부분은 개인정보 데이터베이스를 사업용으로 이용하고 있는 민간사업자를 개인정보취급사업자로 하여 구체적 의무를 부과하는 의무규정(제4장 제1절)을 중심으로 하고 있다.

이 법에서 프라이버시라는 개념은 등장하지 않고, 이를 대신하여 개인정보, 개인 데이터, 보유개인 데이터라는 3개의 개념이 보호의 대상으로 사용되고 있다. 개인정보의 개념에 대해서는 공적 부분의 책무나 시책 외에 기본이념을 대상으로 하고 있다. 이에 반해 민간부분을 대상으로 한 구체적 의무인 개인정보취급자의 의무에 대하여는 개인정보 전반에 적용되는 의무(제15조 내지 제18조), 개인 데이터에만 적용되는 의무(제19조 내지 제23조), 더욱이 이 중에서도 보유개인 데이터에 한정하여 적용되는 의무(제24조 내지 27조)로 분류하여 규정하고 있다.

184) 백윤철, 앞의 주 100), 672면.
185) 백윤철, 앞의 논문, 673면.

또한 개인정보보호의 객체로서 위의 3가지 개념이 등장한다. 그 중 가장 넓은 개념이 개인정보이고, 이것을 한정한 개념이 개인 데이터이며, 그것을 더욱 한정한 개념이 보유 개인 데이터이다.[186]

가) 개인정보

「개인정보보호에 관한 법률」 제2조 제1항에서는 개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함된 성명, 생년월일 그 밖의 기술 등에 의하여 특정의 개인을 식별하는 것이 가능한 것(다른 정보를 용이하게 조합하는 것에 의해 특정의 개인을 식별하는 것이 가능한 것을 포함한다)을 말한다고 규정하고 있다. 이 정의에 따르면 개인정보는 생존하는 개인식별정보를 가리킨다.

「개인정보보호에 관한 법률」은 생존하는 개인에 관한 정보에 한정하고 있으므로 사자에 관한 정보는 포함되지 않는다.[187] 또한 개인에 관한 정보에 한정하고 있기에 법인에 관한 정보도 포함되지 않는다. 법인에 관한 정보 중에서도 재산법적 측면에서 보호를 요구하는 것이 존재하지만, 여기서 말하는 개인정보와는 보호해야 할 이유가 다르다. 개인에 해당하는 한 일본국적일 필요는 없고, 외국인의 개인정보도 보호대상이 된다.[188]

개인식별정보라는 개념은「OECD 지침」제1조(b) 및「EU지침」제2조(a)에서 말하는 개인 데이터(personal data)의 개념과 동일하다.[189]

나) 개인 데이터

「개인정보보호에 관한 법률」에서 말하는 개인 데이터란 개인정보 데이터베이스 등을 구성하는 개인정보를 말한다(제2조 제4항). 따라서 개인정보에 해당하는 것이라 하여도 개인정보 데이터베이스 등을 구성하는 것이 아니면 개인 데이터가 아니다. 즉, 개인 데이터는 개인정보일 것을 필요조건으로 하지만, 개인정보보다는 협의의 개념이다. 이 법률의 보호대상은 일반적으로 개인정보이지만, 개인정보취급사업자의 의무 중 일부(제19조 내지 제23조)는 예외적으로 보호대상이 개인정보가 아닌 개인 데이터

186) 岡村久道・新保史生, 電子ネットワーク個人情報保護, 経済産業調査會, 2002, 82頁.
187) 藤原靜雄, 逐條個人情報保護法, 弘文堂, 2003, 26頁.
188) 岡村久道・新保史生, 前揭書, 82頁.
189) 백윤철·이창범·장교식, 앞의 책, 312면.

가 된다는 규정형식을 취하고 있다.

다) 보유개인 데이터

「개인정보보호에 관한 법률」에서 말하는 보유개인 데이터란 개인 데이터 중 개인정보취급사업자가 개시, 내용의 정정・추가 또는 삭제, 이용정지, 소각 및 제3자에게 제공정지를 하는 것이 가능한 권한을 갖는 것을 말한다(제2조 제5항). 개인정보취급사업자의 의무규정 중 본인에 대한 공표, 개시, 정정, 이용정지 등에 관한 제규정(제24조 내지 제27조)은 보유개인 데이터를 보호대상으로 하고 있다.

보유개인 데이터는 개인정보의 일종이지만, 개인정보에 관한 이 법률 제15조에서 제18조까지의 규정에 대하여도 적용된다. 더욱이 개인 데이터의 일종이기도 하기에 개인 데이터에 관한 제19조에서 제23조까지의 규정도 적용되므로, 결국 보유개인 데이터에 대하여는 제15조로부터 제27조까지의 규정 모두에 적용된다.[190]

(3) 개인정보보호의 기본 방침

「개인정보보호에 관한 법률」제3조는 모든 국민은 개인으로서 존중된다고 규정한 헌법 제13조의 취지를 이어 받아, 개인정보는 개인의 인격존중의 이념하에 그 적정한 취급이 도모되어야 한다고 규정하고 있다. 이 기본원칙은 개인정보를 취급하는 자가 개인정보보호를 자주적으로 행하여야 할 지침이라는 측면과 정부 등이 강구해야 할 개인정보의 보호에 대한 종합적인 제도를 전개해야 하는 시책이라는 2가지 측면을 갖는다.[191] 또한 공공부문과 민간부문을 가리지 아니하며, 개인정보를 취급해야 할 자는 개인정보의 보호를 위하여 스스로 노력해야 할 의무를 진다는 것을 암시한다. 그러나 이것은 구체적인 법적 의무는 아니며, 일종의 노력의무를 선언한 추상적 규정이며, 이를 준수하지 않는 경우에도 법적인 강제력이 부여되는 것은 아니다.

이어 이 법 제2장에서는 국가 및 지방공공단체의 책무 등에 관하여 제4조 내지 제6조에 규정하고 있다. 제4조는 '국가는 이 법률의 취지에 따라

190) 岡村久道・新保史生, 前揭書, 105頁.
191) 藤原靜雄, 逐條個人情報保護法, 弘文堂, 2003, 36-37頁.

개인정보의 적정한 취급을 확보하기 위하여 필요한 시책을 책정하고 이를 실시할 책무를 갖는다'고 규정하고, 제5조는 지방공공단체의 책무에 관한 규정으로 '지방공공단체는 이 법률의 취지에 따라 그 지방공공단체의 구역의 특성에 따라 개인정보의 적정한 취급을 확보하기 위하여 필요한 시책을 책정하고 이를 실시할 의무를 갖는다'고 규정하고 있다. 그리고 제3장에는 제4조의 책무규정에 이어 정부의 개인정보보호에 관한 기본방침의 수립의무를 정하고 있다(제7조). 그리고 제4장 제1절에서는 개인정보취급사업자의 의무를 정하고 있고, OECD 8원칙을 수용하고 있다.

이러한 의무규정의 적용대상인 정보는 개인정보, 개인 데이터, 보유개인 데이터의 3종류로 분류되는데, 이 분류에 따라 개인정보취급사업자의 의무규정의 적용범위가 다르다.

나. 국제기구의 개인정보보호 규범

1) 경제개발협력기구(OECD) 가이드라인

(1) 개설

정보 시스템의 발달과 인터넷 통신의 등장은 개인정보의 보호에 국제적인 통일규범의 필요성을 가져왔고 경제협력개발기구(OECD)가 가장 활발하게 대처하고 있다.[192] 이는 정보기술의 발달이 OECD 선진국들을 중심으로 이루어지기 때문이다.[193] 국제기관에 의한 개인정보보호의 대응방법으로 지침적인 역할을 하고 있는 OECD는 1980년 9월 23일「프라이버시 보호와 개인 데이터의 국제유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Information)에 대한 이사회 권고」(이하에서「OECD 가이드라인」이라고 함)를 채택하여 개인정보의 보호와 유통에 관한 국제적 기준을 제시하였다.「OECD 가이드라인」과 같은 국제적으로 개인정보보호를 위한 가이드라인이 요구되는 이유는 컴퓨터에 의해 대량의 개인정보가 처리됨에 따라 이들의 자유로운 유통을 확보하면서도 적절한 보호가 필요하고, 또한 이를 위해 각국이 법제도를 통일해야 할 필요가 있기 때문이다.

---

192) 현대호, 행정정보공동이용에 관한 법적 과제 한국법제연구원, 2007, 29면.
193) 한국전산원, 앞의 주 174), 64면.

「OECD 가이드라인」이전, 각국은 컴퓨터를 이용한 정보처리에 대응하여 개인정보의 보호를 목적으로 하는 법률 정비하여 왔다. 예컨대, 미국에서는「1970년 공정신용보호법」을 비롯하여「1974년 프라이버시법」,「1978년 금융프라이버시법」등이 제정되었다. 또한 1973년의 스웨덴의「데이터법」을 비롯하여 1977년부터 1979년까지 독일, 프랑스, 오스트리아, 덴마크, 노르웨이, 룩셈부르크가 개인정보의 보호를 목적으로 하는 다수의 법률을 제정하였다.

그러나 각국의 법률은 국내사정을 반영하였기 때문에 개인정보보호와 규제에 관한 방식이 각각 달랐다. 반면에 경제활동의 국제화에 따라 개인정보의 유통도 세계적인 규모로 커져 갔기 때문에 그 유통에 있어서 각국 상호간의 법제도의 조정이 필요하게 되었으며, 개인정보보호대책을 준비하고 있지 않던 나라에 있어서는 개인정보의 보호를 목적으로 하는 법률의 제정을 촉구할 필요성이 제기되었던 것이다.

이와 같이, 각국이 개인정보의 보호에 관하여 다른 법률이나 가이드라인을 가지고 있었기 때문에 자유로운 데이터의 교환이 이루어지지 않는 등 상거래에 장애가 발생하게 되었다. 그리하여 개인정보의 보호와 자유로운 상거래가 균형을 이루도록 각국이 만족할 만한 개인정보보호의 수준을 OECD의 권고로서 정리하였고, 각국은 이 권고에 따라 자국의 제도를 정비한다는 합의를 하였는데, 이것이「OECD 가이드라인」이다.

이「OECD 가이드라인」은 개인정보의 보호를 위하여 8개의 원칙을 제시하였다.[194] 그리고 개인정보를 보호하고, 정보의 자유로운 흐름을 촉진하며, 각 국가의 프라이버시보호법에 의하여 정보의 자유로운 흐름이 부당하게 억제하는 것을 예방하고, 여러 국가들의 관련 법률규정들을 조화시킬 목적을 가지고 있다.[195] 이후 영국은「1984년 데이터보호법」으로, 미국은 1995년 정보기반 특별 전담기구(Information Infrastructure Task Force)[196]를 통하여「OECD 가이드라인」의 프라이버시 보호원칙을 재확인하였다.[197]

그러나「OECD 가이드라인」은 법적 구속력이 없는 권고형식으로 되어

194) 백윤철, 앞의 논문, 2009, 666면; 백윤철·이창범·장교식, 앞의 책, 235면.
195) Raymond Wacks, supra note 104), p.207.
196) http://itlaw.wikia.com/wiki/Information_Infrastructure_Task_Force 2009.12.3.방문.
197) 강경근, "개인정보침해 국내외 판례조사 및 분석", 개인정보연구 00-1, 한국정보보호센터, 2000, 105-106면.

있으며, 제5조에는 연방국가들의 특수성을 인정하는 규정을 두고 있다. 또한 제2조에는 처리형태 및 그 성질 또는 이용의 전후관계로 보아 개인의 프라이버시와 자유에 대하여 위험성이 있는 공적 또는 사적 부문의 개인데이터에 적용된다고 규정하고 있다. 그리고「OECD 가이드라인」제2장 및 제3장에 기재된 가이드라인의 제원칙은 국가주권, 국가안전보장 및 공공질서에 관계되는 경우 적용이 면제된다(제4조).[198]

(2) 국내적용상의 기본원칙 -프라이버시보호를 위한 8원칙

① 수집제한의 원칙(Collection Limitation Principle)

개인 데이터의 수집에는 제한을 두어야 하고, 어떠한 개인 데이터라도 합법적이고 공정한 절차를 거쳐야 한다. 그 수집이 정당한 경우에는 정보주체에 통보하거나 동의를 구한 다음에 수집하는 것이 당연하다고 규정하고 있다. 즉 수집은 하되 적법하고 공정한 수단에 의해 수집해야 하며, 본인의 동의를 얻은 후에 수집을 해야 한다는 원칙이다(제7조).

② 정보정확성의 원칙(Data Quality Principle)

개인정보는 그 이용목적에 부합되는 것이어야 하며 이용목적에 필요한 범위 안에서 정확하고 완전하게 최신의 것이어야 한다(제8조). 즉 정보는 정확하고 완전해야 하며, 최신의 것으로 보관해야 한다. 개인정보를 이용하는 기업에서는 수집된 개인정보를 기초로 그 사람을 판단한다. 중간의 무리한 수집이나 보관, 다른 개인정보와 혼재된 개인정보를 제공하면 본인에게 이익이 되는 경우도 있지만 오히려 폐를 가져올 가능성도 있다.

③ 목적명확성의 원칙(Purpose Specification Principle)

개인 데이터의 수집목적은 늦어도 수집 시까지는 명확하게 제시되어야 하며, 그 이용은 수집목적의 실현 또는 수집목적과 양립되어야 하고 목적이 변경될 때마다 명확하게 제시하여야 한다(9조). 말하자면 수집목적을 명확하게 하여 수집해야 하고 수집목적에 한하여 사용해야 한다. 기업이 개인정보를 수집하는 것은 어떠한 목적이 있으며, 우편발송이나 회원가입

198) 권건보, "자기정보통제권에 관한 연구 -공공부문에서의 개인정보보호를 중심으로-", 박사학위논문, 서울대학교 대학원, 2004, 157-159면.

절차를 위하여 필요한 경우나 애프터서비스 이후의 영업활동을 목적으로 하는 경우도 있을 수 있다. 어느 경우에도 고객으로부터 정보를 수집할 때는 목적을 명확히 밝혀야 하며, 일정한 목적을 가지고 수집한 개인정보는 그 목적을 위해서만 사용되어야 하고, 다른 용도로 사용하는 것은 금지된다.

④ 이용제한의 원칙(Use Limitation Principle)

개인 데이터는 제9조에 의해 명확하게 제시된 목적 이외의 목적을 위하여 개시, 이용, 기타 사용에 제공되어서는 안된다. 다만, 데이터 주체의 동의가 있는 경우와 법률의 규정에 의한 경우에는 그러하지 아니하다(제10조). 즉, 개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확하게 제시된 목적 이외의 용도로 제공되거나 이용되어서는 안 된다. 이것이 수집된 개인정보의 이용에 관한 원칙이다. 목적명확성의 원칙과 내용이 일부 중복되지만 이용제한의 원칙에서도 목적이외의 사용을 금지하고 있다. 다만, 이 원칙에는 본래의 원칙이 아니더라도 본인의 동의를 얻으면 사용해도 좋다고 규정되어 있는 경우와 개인정보의 공개를 의무적으로 규정한 법률의 규정에 의한 경우에는 예외로 하고 있다.

⑤ 안전보호의 원칙(Security Safeguards Principle)

개인 데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 취함으로써 보호하여야 한다(11조). 안전보호의 원칙은 기업이 수집·보존하고 있는 개인정보가 분실, 불법적인 접근, 파괴, 정보수정 및 공개와 같은 위험에 대비하여 합리적인 안전보호장치를 마련해야 하는 것이다.

⑥ 개인참가의 원칙(Individual Participation Principle)

개인 데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인 데이터의 존재, 성질 및 그 주요 이용목적과 함께 데이터 관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다(제12조).

⑦ 공개의 원칙(Openness Principle)

개인은 데이터 관리자가 자기에 관한 데이터를 갖고 있는지 여부에 대하여 데이터 관리자 또는 기타의 자로부터 확인을 받을 권리, 개인에 관한 데이터를 상당기간 내에 과다하지 않는 비용으로, 합리적인 방법과 알기 쉬운 형태로 본인에게 통지하도록 하는 권리, 그리고 이상의 요구가 거부당한 경우에는 그 이유를 밝히도록 하고, 이와 같은 거부에 대하여 이의를 제기하는 권리, 자기에 관한 데이터에 대하여 이의를 제기하고 그 이의가 인정되지 않을 경우에는 그 데이터를 소각, 수정, 완전화, 보완하게 하는 권리를 가진다(제13조). 개인정보에 관한 개발, 운용 및 정책에 있어 일반적인 공개의 원칙이 적용되어야 한다. 개인정보의 존재, 성격, 주요 사용목적 및 정보관리자의 신원, 통상의 주소를 확인하는데 공개방법은 쉽게 이용될 수 있어야 한다.

⑧ 책임의 원칙(Accountability Principle)

데이터 관리자는 위의 제원칙을 실시하기 위한 조치에 따른 책임이 있다(제14조). 개인정보를 관리하는 자는 이에 대하여 책임을 져야 한다. 개인정보관리자는 위에서 제시한 원칙들이 지켜지도록 필요한 제반조치를 해야 한다. 이 원칙에는 기업 등 개인정보관리자가 이들 원칙을 지키기 위해 구체적인 업무나 조치를 취할 책임이 있다고 한다.

(3) 국제적 적용상의 기본원칙 -자유로운 유통과 합법적 제한

회원국은 개인 데이터의 국내에서의 처리 및 그 재유출이 다른 회원국에 미칠 영향에 대하여 배려하여야 한다(제15조). 그리고 단순한 통과도 포함된 개인 데이터의 국제유통이 저해되지 않고 안전하도록 하기 위하여 모든 합리적이고 적정한 수단을 강구하여야 한다(제16조).

회원국은 자국과 다른 회원국간의 개인 데이터 국제적 유통을 제한하지 않아야 한다. 다만 회원국이 아직 가이드라인을 실질적으로 준수하고 있지 않을 경우 또는 관계 데이터의 재유출이 그 나라의 프라이버시 보호조치를 우회하는 경우에는 유통을 제한할 수 있다. 회원국은 자국의 프라이버시법제가 그 성격으로 인하여 특별한 규정을 하고 있는 특정한 범주에 속하는 개인 데이터에 관하여 또는 다른 회원국이 그러한 종류의 개인 데이터에 대하여 자국의 그것과 동일한 정도의 보호를 하고 있지 않을 경우

에는 그 유통을 제한할 수 있다(17조).

그리고 회원국은 개인의 프라이버시와 자유의 보호라는 명목으로 이들의 보호에 필요한 정도를 넘어 개인 데이터의 국제유통에 장애를 만들 수 있는 법률 또는 정책의 설정 및 관행의 실시를 억제하여야 한다(제18조).

(4) 국내실시

제2장 및 제3장에 규정되어 있는 제원칙을 국내에서 실시함에 있어 회원국은 개인 데이터에 관한 프라이버시와 자유의 보호를 위한 법적·행정적 또는 기타 절차나 제도를 확립하여야 한다. 회원국은 특히 적당한 국내법을 제정하고, 행동규율 기타 형식의 자주적 규제를 장려하고 지원하며, 개인에게 그 권리를 행사하는데 필요한 합리적인 수단을 제공한다. 그리고 제2장 및 제3장의 제원칙을 실시하는 조치에 응하지 않을 경우에는 적당한 제재 및 구제수단을 강구하며, 데이터 주체에 대한 부당한 차별이 없도록 하여야 한다(제19조).

(5) 국제협력

회원국은「OECD 가이드라인」제원칙의 준수사항에 대하여 요구가 있으면 다른 회원국에 통보하여야 한다. 회원국은 또 개인 데이터의 국제교류 및 개인의 프라이버시와 자유의 보호에 대한 절차가 간명하여야 하고 가이드라인을 준수하고 있는 다른 회원국의 그것과 양립하도록 하여야 한다(제20조). 회원국의 가이드라인에 관한 정보교환과 절차적 조사사항에 대한 상호원조를 용이하게 하기 위한 정치를 확립하여야 한다(제21조). 회원국은 개인 데이터의 국제적 교류에 적용할 수 있는 법률을 제정하기 위하여 국내적·국제적으로 제원칙이 발전되도록 작업하여야 한다(제22조).

2) 유럽연합(EU) 지침

유럽연합 회원국들이 개인정보보호에 관심을 갖기 시작한 것은 60년대에서 70년대 초까지로 거슬러 올라간다. 그러나 유럽연합국이 회원국의 개인정보보호정책에 대해서 최초로 공식적인 관심을 표명한 것은 1981년 1월 28일 유럽연합 이사회가 채택한「개인정보의 자동처리로부터 개인보호에 관한 협약」[199]이라고 할 수 있다.

이 개인정보보호협약은 70년대 들어 유럽 국가들 사이에서 컴퓨터 등 자동정보처리장치의 보급 및 이용이 확대되고, 이에 따라 정부 및 기업에 대한 개인정보의 처리의 양과 기회가 증가한데 따른 프라이버시 침해 위협으로부터 개인의 자유와 권리를 보호하기 위하여 제정된 것이다.[200] 이 협약에 바탕을 두고 유럽연합회는 1990년 9월에 국내법을 조정함으로써 개인 데이터의 자유로운 유통을 확보하는 것을 목적으로 하는 지침의 기초안을 제의하였고, 5년 후에「개인 데이터 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 1995년 10월 24일의 유럽의회 및 이사회의 95/46/EU지침」(이하「EU 지침」이라고 함)이 채택되었다.[201] 「EU 지침」의 주요내용은 <표 9>와 같다.

<표 9> 「EU 지침」의 개인정보보호 내용

구 분	내 용
적용범위	• 물적 범위 : 자동처리되는 개인정보 및 구조화된 파일링시스템에 포함되는 개인정보 • 인적범위 : 자연인의 개인정보
적용제외 영역	• 국가안보, 공공의 안전 및 방위를 위한 개인정보의 처리 • 형사법 영역에서의 개인정보의 처리 • 서신왕래와 같은 지극히 개인적이고 사적인 목적의 개인정보처리 • 언론보도, 문학, 예술적 표현을 위한 개인정보 처리
정보처리자 의무	• 공정하고 적법한 개인정보의 처리 • 정보처리목적의 명시 • 정보처리목적과의 적절성과 관련성, 비례성 유지 • 개인정보의 정확성과 최신성 확보 • 기술적, 조직적 보안조치 확보 • 감독기구의 정보처리에 대하여 고지
정보주체 권리	• 정보처리의 전반적인 사항에 대하여 통지받을 권리
제3국으로의 정보이전 금지	• 적절한 보호수준을 갖추지 않은 제3국으로의 개인정보이전 금지
독립기구 설치	• 회원국 내 독립적인 개인정보보호기구의 설치

*이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 106면 참조.

199) Council of Europe's Convention (108) for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg, 28.1.1981).
200) 백윤철·장교식·이창범, 앞의 주 172), 243면.
201) 이창범・윤주연, 앞의 책, 67면.

「EU 지침」은 자동처리 및 수동처리된 개인 데이터의 처리에 적용된다. 여기에서 개인 데이터란 자연인을 직접 또는 간접적으로 식별가능한 모든 개인 데이터를 말한다. 자동으로 처리되지 않고 수동으로 처리된 개인 데이터가 파일링시스템의 일부를 구성하는 경우에는 수동처리된 개인 데이터에도 적용된다. 파일링시스템 이란 일정한 기준에 따라 접속하는 것이 가능한 개인 데이터의 집합을 구성하는 것이다. 그리고 처리란 수집, 기록, 축척, 번안, 검색, 참조, 이용, 분포, 삭제 또는 파기 등의 작업이 실행되는 것을 말한다.

자동 또는 수동처리된 이들 데이터는 어떤 조직과 단체가 보유해서 이용하는 것이지만,「EU 지침」의 적용대상이 되는 조직은 전자 또는 인쇄매체에서 개인 데이터를 보유하는 모든 조직 및 유럽연합과 유럽경제지역(EEA) 내의 모든 나라 사이에서 데이터의 이전을 행하는 기업이다.

「EU 지침」의 적용을 받는 지역은 유럽연합에 가맹하고 있는 15개국[202]은 물론, 유럽경제지역[203]에 대해서도 적용된다. 그러나 중앙 및 동유럽 각국에는 적용되지 아니한다.[204] 따라서「EU 지침」의 적용을 받지 않는 나라는 유럽연합에 가맹하지 않는 한 이 지침에서 말하는 제3국이 된다.

「EU 지침」의 특색은 공공부문과 민간부문의 구별을 하지 않고 적용되고 있는 것이다. 또한「EU 지침」은 EU 내부에서만 적용되기 때문에 한국에 직접 영향은 없고, 유럽위원회가 교섭을 신청하였을 경우에 정부로서는 대응하는 것이 불가능하다.[205] 이러한 이유에서 일본은 민간부문을 포함하여 개인정보보호를 위한 법률의 정비에 대한 검토가 이루어졌다.

그 외에 EU는 특히 전기통신분야에 있어서 개인정보보호를 위해서는「전기통신분야에 있어서의 개인 데이터 처리 및 프라이버시보호에 관한 1997년 12월 15일의 유럽의회 및 이사회의 97/66/EC지침」[206]을 제정하

202) 벨기에, 프랑스, 독일, 이탈리아, 룩셈부르크, 네덜란드, 영국, 아일랜드, 덴마크, 그리스, 포르투갈, 스페인, 오스트리아, 핀란드, 스웨덴을 들 수 있다.
203) 아이슬란드, 리히텐슈타인, 노르웨이 등이다.
204) 헝가리, 폴란드, 체코, 슬로바키아, 불가리아, 루마니아, 에스토니아, 라토비아, 리투아니아, 슬로베니아를 말한다.
205) 堀部政男(編), 前揭書, 363頁.
206) Directive 97/661 EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the

였다.[207]

다. EU의 개인정보보호 추진체계

유럽연합의 개인정보보호정책은 회원국마다 설치되어 있는 개인정보보호감독기구를 중심으로 추진된다. 유럽연합 회원국의 개인정보보호감독기구는 <표 10>과 같다.

개인정보보호감독기구는「EU 지침」이 시행되기 전부터 1981년 개인정보보호협약에 서명한 가맹국에게는 설치가 의무화되어 있었다. 따라서 개인정보보호감독기구는 유럽의 개인정보보호정책에 있어서 역사가 길며, 국내 개인정보보호정책은 물론 유럽연합의 개인정보보호정책에 있어서도 중추적 역할을 수행해오고 있다. 회원국뿐만 아니라 2003년 12월부터는 유럽공동체조약 제286조[208]와 유럽공동체 개인정보규정에 의하여 유럽집행위원회 내에도 유럽연합 내부 조직 및 기관들에 의한 개인정보처리를 모니터링하기 위해 유럽 데이터 보호 관리자(EDPS: The European Data Protection Supervisor)라고 하는 개인정보보호 감독관 직책이 신설되었다.[209]

각국의 개인정보보호감독기구는 업무적으로 완전히 독립되어 있어야 한다.「EU 지침」은 물론「1981년 개인정보보호협약 Additional Protocol」에서도 개인정보보호감독기구의 완전한 독립(complete independence)이 강조되고 있다. 따라서 유럽연합 회원국들의 개인정보보호법에는 대부분 개인정보보호감독기구의 독립성이 명시되어 있다. 또한 개인정보보호감독기구는 나라에 따라 조금씩 차이는 있지만 일반적으로 조사권, 정보수집권(자료제출요구권), 청문권, 개입권, 권고권, 시정명령권, 소제기권, 소송대리권, 청원수리권, 진정처리 등의 권한과 기능을 가지며 분야별 지침 제정 등 일정한 범위에서 입법권도 가진다(지침 제28조).

개인정보보호감독기구는「EU 지침」이 자국 내에서 충분히 효력을 발

---

telecommunications sector, 397L0066, Official Journal L024, 30/01/1998 p.00011~0008.

207) 백윤철, 앞의 주 100), 667면.

208) Article 286 of the EC Treaty는 유럽공동체 내부 조직 및 기관에 의한 개인정보처리를 감시할 독립된 감독기구(independent supervisory body)의 설치를 규정하고 있다.

209) 백윤철·장교식·이창범, 앞의 책, 245-246면.

휘하도록 이행할 책임을 지며 개인정보보호정책에 대한 포괄적인 권한을 가지고 책임도 진다. 개인정보보호법 또는 정보보호법의 집행에 대한 책임뿐만 아니라, 개별법에 포함되어 있는 개인정보보호관련 규정의 집행에 대해서도 일반적으로 개인정보보호감독기구가 책임을 지는 경우가 많다. 또한 개인정보보호감독기구는 다른 정부부처나 의회가 개인정보보호와 관련이 있는 법률을 제·개정하려고 하는 경우에는 의견을 제시할 수 있으며, 필요한 경우에는 관련 법령에 대한 제·개정을 권고할 수도 있다.

<표 10> 유럽연합 회원국의 개인정보보호기구

국 가	기 구 명	비 고
프랑스	정보자유위원회 (Commission Nationale de l'Informatique et des Libertès)	독립위원회
영국	정보보호 커미셔너 (Information Commissioner)	국왕소속
스페인	개인정보보호원 (Agencia de Protección de Datos)	독립법인
오스트리아	정보보호위원회(Österreichische Datenschutzkommission)	연방수상소속
	정보보호 자문위원회	"
네덜란드	정보보호위원회(Dutch Data Protection Authority)	법무부가 사무국 운영지원
필란드	정보보호옴브즈만(Office of Data Protection Ombudsman)	법무부가 사무국 운영지원
	정보보호위원회	"
독일	연방정보보호청(Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)	내무부가 사무국 운영지원
아이슬란드	정보보호위원회(Icelandic Data Protection Agency)	법무부 소속
스웨덴	정보조사원(Datainspektionen)	재정부 소속
덴마크	정보보호원(Datatilsynet)	법무부 소속
그리스	정보보호원(Hellenic Data Protection Authority)	법무부/대통령
노르웨이	정보조사원((Datatilsynet The Data Inspectorate)	국왕/노동내무부
	프라이버시 항소위원회	국왕/노동내무부

*백윤철·이창범·장교식, 개인정보보호법, 한국학술정보, 2008, 247면.

유럽집행위원회는 개인정보보호를 위한 회원국 간 협력과 공동연구를 매우 중요시 하고 있다. 이에 따라「EU 지침」제29조는 유럽집행위원회

내에 개인정보보호 실무위원회(Data Protection Working Party)를 설치하도록 하고 있다. 실무위원회는 회원국의 개인정보보호감독기구를 대표하는 자들로 구성되며,「EU 지침」의 통일적 적용, 회원국 및 제3국의 개인정보보호수준 평가, 집행위원회에 대한 개인정보보호정책 자문, 유럽연합이 채택한 각종 개인정보보호 이행지침에 대한 의견제출, 개인정보보호에 관한 정책발의 등의 기능을 수행한다(지침 제30조)[210]

<표 11> 유럽연합의 개인정보보호법제

구 분	내 용
지침 (Directives)	전자통신 분야에서 개인정보처리 및 프라이버시보호에 관한 지침(2002)
	전자통신 서비스 또는 공중 통신 네트워크의 제공과 관련하여 생성·처리되는 데이터의 보유 및 2002년 지침의 개정에 관한 지침(2006)
	전기통신 분야에서 개인정보처리 및 프라이버시보호에 관한 지침(1997)
	개인정보처리에 관한 개인보호 및 개인정보의 자유로운 이전에 관한 지침(1995)
협약(Convention)	개인정보의 자동처리에 관한 개인보호 협약(1981)
결정(Decision)	미국 세관에 전송된 항공여행자의 이름에 포함된 개인정보의 적절한 보호에 관한 결정(2004)
	개인정보의 제3국 이전을 위한 표준계약 조항의 도입에 관한 2001년 결정의 수정에 관한 결정(2004)
권고 (Recommendation)	고용 목적으로 사용되는 개인정보보호에 관한 권고(1989)
	의료정보의 보호에 관한 권고(1997)

*백윤철·이창범·장교식, 개인정보보호법, 한국학술정보, 2008, 250면 참조.

210) 백윤철·장교식·이창범, 앞의 책, 245-246면.

<표 12> 유럽연합 회원국의 개인정보보호 법제

국 가	법 률
영국	개인정보보호법(Data Protection Act, 1998)
프랑스	정보처리파일및자유에관한법률(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
독일	연방정보보호법Bundesdatenschutzgesetz, 1974) 각주 정보보호법
스웨덴	개인정보법(Personal Data Act)
스페인	개인정보보호기본법(Organic Law on the Protection of Personal Data, 1999)
네덜란드	개인정보보호법(Personal Data Protection Act,1999)
오스트리아	연방개인정보보호법(Datenschutzgesetz, 1978)
벨기에	개인정보처리에관한프라이버시보호법(Law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data, 1992)
덴마크	개인정보처리에관한법(The Act on Processing of Personal Data, 2000)
핀란드	개인정보법((Personal Data Act, 1999)
그리스	개인정보처리에서의개인정보보호에관한법(Law on the Protection of Individuals with regard to the Processing of Personal Data, 1997)
아일랜드	정보보호법(Data Protection Act, 1988)
이탈리아	개인정보처리에서의개인및기타주체의보호에관한법(Law on the Protection of Individuals and other subjects with regard to the Processing of Personal Data, 1996)
룩셈부르크	개인정보처리에서의개인의보호에관한법(Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, 1998)
포르투갈	개인정보보호법(Act on the Protection of Personal Data, 1998)
노르웨이	개인정보법(Personal Data Act 2000)
아이슬란드	개인정보처리및보호에관한법(Act on the Protection and Processing of Personal Data, 2000) *비회원국
스위스	연방정보보호법(Federal Act on Data Protection, 1992)*비회원국

*백윤철·이창범·장교식, 개인정보보호법, 한국학술정보, 2008, 251면 참조.

<표 13> 각국의 입법체계

법률체계(입법방식)	국가명	법률명
일원적 통합주의	이태리	「정보보호법」
일원적 구분주의 (중간형태: 기본법-일반법)	일본	개인정보보호에 관한 법률 공공부문: 행정기관이 보유하는 개인정보의 보호에 관한법률(공공부문의 일반법) 민간부문: 개인정보보호에 관한 법률과 개별법
일원적 개별주의 (기본법-개별법)	영국	「정보보호법」
	독일	「연방정보보호법」
	프랑스	「정보처리파일및자유에관한법률」
	프페인	「개인정보보호기본법」
이원적 구분주의 (부문별 일반법)	캐나다	공공: 「프라이버시법」
		민간: 「개인정보보호및전자문서에관한법률」
개별주의 (기본법・일반법 없음)	미국	관련 개별법에 산재

*홍준형, 개인정보보호법제 정비를 위한 기본법 제정방안 연구, 한국전산원, 2004, 109면 참조.

라. 분석 및 시사점

1) 입법체계

개인정보보호법제의 입법체계는 <표 13>에서 제시된 바와 같이, 크게 일원주의 입법체계, 이원주의 입법체계, 개별법 입법체계로 구분할 수 있다. 일원주의 입법체계는 먼저, ① 공공부문, 민간부문, 그리고 각 개별법까지 통합시킨 일원주의적 입법체계, ② 통합기본법 체계를 유지하면서 각 영역에 적용되는 개별법에서 개인정보관련 조문을 갖고 있는 일원적 입법체계, ③ 통합법은 기본적 지위를 갖고 있으면서 추상적이고 원칙적인 규정을 두고, 각 분야별로 일반법을 제정하여 이를 구체화시키는 일원주의적 입법체계이다. 다음으로, 통합하는 기본법이 없이 공공부문에 적용되는 일반 개인정보보호법체계와 민간부문에 적용되는 개인정보보호법 체

계가 이원적 입법체계이다. 마지막으로 개별주의 입법체계는 기본법이나 통합법의 체계는 없고 각 개별법에 개인정보 관련 조항들이 산재해 있는 입법체계가 개별적 입법체계이다.

전술한 바와 같이 일본은 통합기본법(개인정보보호법)을 갖고 있으면서 각 영역에 적용되는 개별법에서 정보보호관련 조문을 갖고 있는 일원적 입법체계를 가지고 있고, EU 등 유럽은 통합법을 제정하여 기본법의 지위를 부여하여 추상적이고 기초적인 원칙과 관련된 규정을 두고 있으면서, 각 분야별로 일반법을 제정하여 이를 구체화시키는 법률을 채택하는 방식의 입법체계이다. 그리고 미국이나 우리나라는 기본법이나 일반법이 없이 개별법에 개인정보보호조항이 산재해 있는 입법체계를 유지하고 있는 나라에 속한다.

2) 미국

미국은 헌법상 프라이버시에 관한 명문은 규정되어 있지 않지만 판례를 통하여 헌법상 권리로 인정하고 있고, 유럽국가들과는 달리 포괄적이고 체계적인 개인정보 관련 입법체계를 두고 있지는 않다. 하지만 기본법이 제정되어 있지는 않아도 사회적 변화나 정보통신기술의 발달에 따라 각 영역별로 개인정보와 관련한 개별법적 접근을 취하여 대응하고 있다. 미국은 개인정보보호를 위한 방식으로는 자율규제방식을 취하고, 민간부문에서 특별히 규제할 필요성이 인정될 경우에만 법률을 제정한다. 그러나 원칙적으로는 업계가 자율적으로 개인정보보호를 위한 제도를 마련하도록 유도하고 있다. 또 사회적·기술적 변화에 신속한 대응으로 온라인 프라이버시, 전자태그(RFID)[211] 프라이버시 보호 등과 같은 새로운 이슈에 신

211) 위키백과 백과사전: RFID(Radio-Frequency IDentification) 기술이란 전파를 이용해 먼 거리에서 정보를 인식하는 기술을 말한다. 여기에는 RFID 태그(이하 태그)와, RFID 판독기(이하 판독기)가 필요하다. 태그는 안테나와 집적회로로 이루어지는데, 집적회로 안에 정보를 기록하고 안테나를 통해 판독기에게 정보를 송신한다. 이 정보는 태그가 부착된 대상을 식별하는 데 이용된다. 쉽게 말해, 바코드와 비슷한 기능을 하는 것이다. RFID가 바코드 시스템과 다른 점은 빛을 이용해 판독하는 대신 전파를 이용한다는 것이다. 따라서 바코드 판독기처럼 짧은 거리에서만 작동하지 않고 먼 거리에서도 태그를 읽을 수 있으며, 심지어 사이에 있는 물체를 통과해서 정보를 수신할 수도 있다. RFID는 사용하는 동력으로 분류할 수 있다. 오직 판독기의 동력만으로 칩의 정보를 읽고 통신하는 RFID를 수동형(Passive) RFID라 한다. 반수동형(Semi-passive) RFID란 태그에 건전지가 내장되어 있어 칩의 정보를 읽는데는 그 동력을 사용하고, 통신에는 판독기의 동력을 사용하는 것을 말한다. 마지막으로 능동형(Active) RFID는 칩의 정보를 읽고 그 정보를 통신하는 데 모두 태그의 동력을 사용한다. RFID를 동

속하게 응답할 수 있도록 유도하고 있다.

또한 세이프하버원칙을 통하여 지속적으로 유럽으로부터 데이터를 전송받을 수 있다. 세이프하버원칙은 국제조약으로서의 성격을 가지지는 않지만, 이 원칙을 따르는 경우 유럽위원회로부터 개인정보보호의 적정성을 인정받는 결과가 되기 때문에 EU 회원국가와 별도의 합의가 없어도 그 적정성을 추정 받게 된다.

또한 개인정보의 공동이용과 관련하여「컴퓨터 연결 및 프라이버시법」을 제정하여 행정정보를 공동이용함에 있어서도 개인정보를 보호하는 법률을 제정하여 운용 하고 있다. 전술한 바와 같이 이 법의 제정 배경은 컴퓨터연결 프로그램을 통하여 정부의 보조금지급 프로그램에서 사기 또는 실수나 남용을 찾아내고, 정부보조금에 대한 부정 수혜자 색출 및 예산절감 등의 목적으로 사용한다. 그런데 이러한 컴퓨터 연결 프로그램을 통한 예산절감은 프라이버시 침해라는 기회비용의 지급 없이는 발생하지 않는다고 프라이버시보호 주장자들은 생각하였고, 결국 의회는 프라이버시보호자들의 손을 들어주었다. 이에 따라서 컴퓨터 연결 프로그램의 사용에 따르는 개인정보를 보호하기 위한 법률이 제정된 것이다. 그러나 프라이버시법과 관리예산처(OMB) 지침에 규정된 '일상적 사용'이란 규정을 통하여 개인정보가 침해된다는 논란이 있었고, 통제실무가 부적절하다는 것이다.

3) 독일

독일의 개인정보보호 입법체계는 공적·사적 영역을 구분하지 않는 일원주의적 법체계하에서 보호하고 있다. 이는 개인의 사생활을 보호함에 있어서 공공부문과 민간부문이 다르지 않으며, 개인정보의 공동이용과 제공에 대한 일반적인 규제 역시 다르지 않으므로 동일한 원칙하에서 규율한다는 것이다.

독일의 개인정보보호법은 다음과 같은 특징을 지니고 있다.

력 대신 통신에 사용하는 전파의 주파수로 구분하기도 한다. 낮은 주파수를 이용하는 RFID를 LFID(Low-Frequency IDentification)이라 하는데, 120~140 킬로헤르츠(khz)의 전파를 쓴다. HFID(High-Frequency IDentification)는 13.56 메가헤르츠(Mhz)를 사용하며, 그보다 한 층 높은 주파수를 이용하는 장비인 UHFID(UltraHigh-Frequency IDentification)는 868-956 메가헤르츠 대역의 전파를 이용한다.

① 법적용의 범위가 확대되어 공공기관이 보유하고 있는 정보와 자료 가운데 자동화된 정보처리뿐만 아니라 수기(手記)로 처리된 문서들도 그 적용범위에 포함시키고 있다. ② 개인정보관리통제권을 보호하기 위하여 개인정보를 수집·보유·사용할 때 목적구속의 원칙이 엄격하다. ③ 개인에게 자신에 관한 통제의 권리가 보장되는 것은 권리가 향상되었다는 것을 의미한다. ④ 컴퓨터 연결을 통한 호출에 있어서 관련자의 이익을 고려하여 필요한 경우에만 허용하여 자동화된 호출절차로부터 개인정보를 보호한다.

개인정보공동이용과 관련하여서는 별도의 입법은 제정되지 않았고, 「연방정보보호법」제10조에 근거하여 온라인 연결을 통한 정보제공의 원인·목적·수신인·종류 등이 문서로 확인되어야 한다. 그리고 자동호출절차에 의한 제공의 실질적 허용성은 다른 법률 규정이나「연방정보보호법」규정에 따라 결정된다.

개인정보보호에 관한 공·사 부문을 구별하지 않고 통일법 체계로 개인정보를 보호한다는 것은 우리에게는 시사하는 바가 적지 않다. 이와 관련하여 우리나라에서도 개인정보보호법을 제정할 때 고려할 필요가 있다고 본다.

4) 영국

성문헌법이 없는 영국은 당연히 프라이버시권 또는 자기정보통제권에 관한 명시적·묵시적 권리에 대한 헌법상 근거는 없다. 그러나 시민혁명 과정에서 인권을 존중하는 법제도가 도입되었고, 이러한 제도는 당연히 프라이버시 및 개인정보의 법적보호로 이어졌으며, 1984년에「정보보호법」을 제정·공포하게 되었다. 이 법은 EU지침이 제정되면서 전면 수정을 거쳐, 공공부문과 민간부문의 구분 없이 개인정보 처리에 적용되는 개인정보보호 기본법의 역할을 담당하고 있다. 기본법의 특성상 일반 추상적·기본적 내용을 규정하고 있으며, 구체적인 내용은 다른 특별법이나 하위법령에 위임하고 있다. 그리고 이 법은 개인정보보호원칙을 비롯하여 정보주체의 권리와 정보처리자의 의무, 개인정보보호기구의 설립 및 운영, 정보법원의 설치, 개인정보의 국외이전에 관한 사항 등을 포괄적으로 규정하고 있으며, 적용범위에 있어서도 공·사의 구분 없이 일원주의 입법

체계를 구성하고 있다.

또 개인정보보호를 위한 감독기구를 두고 있는데, 이 기구는 독임제 구조를 가진 독립된 법정기구인 정보커미셔너이다. 정보커미셔너는 행정부의 지시나 감독을 받지 않고 독자적으로 운영되기 때문에 독립성과 자율성이 보장된다고 볼 수 있다. 정보커미셔너의 역할은 공공부문과 민간부문 모두에서 모든 정보처리를 관할 대상으로 삼고 있어 개인정보보호에 관한 한 다른 나라에서 보다 오히려 더 보장이 되는 것으로 볼 수 있다.

우리나라의 경우도 공·사 부문을 통합하는 기본법을 제정할 필요가 있으며, 또 독립된 공·사 부문을 통합하는 독립적인 감독기구의 설치가 요구된다.

5) 일본

일본 역시 정보통신기술의 발달로 다양한 개인정보침해 문제에 직면하였다. 여러 가지 개인정보 유출·침해 문제와 EU개인정보보호지침에 의하여 정보이전 제한에 따른 대응의 필요성을 인식하여 공공부문을 중심으로 개인정보보호법의 제정에 대한 논의를 시작하게 되었고, 우여곡절을 거쳐 종합적인 개인정보 기본법이 2003년 제정되어 시행되고 있다.

일본의「개인정보보호법」의 입법체계는 통합 기본법 체계로서 일원주의를 취하고 있는데, 그 특징으로는 공·사 양 부문에서 개인정보의 적정한 취급이 보장되도록 하고 있고, 민간사업자에 대한 조치뿐만 아니라 국가와 지방, 공공단체의 책임, 기본방침의 작성 기타 시책의 기본사항을 제2장, 제3장, 제4장에 걸쳐 포괄적으로 규정하고 있다. 이 법에서는 민간분야에 관해서도 법률의 대상으로 하는 점에서 유럽형과 유사하다.

하지만 개인정보의 고충처리와 관련하여서는 이 법 제31조, 34조, 42조 등에 분산하여 정보주체의 권리·이익을 보호하고 있지만, 이는 일원화된 창구의 역할을 하기에 부적합하고, 절차의 다양화로 인하여 오히려 피해를 구제받고자 하는 정보주체에게 혼선을 초래할 수 있다는 단점도 있다 이러한 점을 해결하기 위한 강력하면서도 단일화된 독립기구의 설치가 요구된다. 아무리 개인정보보호를 위한 훌륭한 법제가 잘 정비되어 있고, 정보주체의 권리를 법적으로 보장하고 있다고 하더라도 법제운용의 미숙이나 권리실현을 위한 절차가 복잡하면 사실상 권리구제의 현실성은 불가

능하게 되고 개인정보보호의 이념은 형식에 불과하게 된다.

이러한 점에서 우리나라의 개인정보보호와 관련된 규정에 있는 개인정보심의기구 등에 대한 심도 깊은 논의가 제기된다.

2. 우리나라의 개인정보보호법제

가. 「공공기관의 개인정보보호에 관한 법률」

1) 제정경위

「공공기관의 개인정보보호에 관한 법률」(이하「개인정보보호법」이라 한다)은 공공부문에서 개인정보보호에 관한 일반법적 성격을 갖은 법률로서 정보사회에 부응하여 행정전산화로 인한 개인의 사생활보호라는 목적으로 1988년부터 입법을 추진하여 1994년 법률 제4734호로 공포되고, 1995년 1월 8일부터 시행하게 되었다. 그 동안 5차례의 개정을 거쳐 현재의 법률로 시행되고 있다. 이 법률은 정부기록에 대한 자기정보관리통제권을 구체화하는 기본법으로서 중요한 의미를 가진다.

2) 주요내용

(1) 목적

「개인정보보호법」은 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다(법 제1조). 따라서 공공기관이 보유하는 각종 개인정보를 보호하여 국민의 권리와 이익을 보호하여 헌법 제17조에서 보장하고 있는 사생활의 비밀과 자유의 확장 개념인 자기정보관리통제권에 대한 공공부문에서의 일반법으로서의 중요한 의미를 가진다.

(2) 적용범위와 보호대상

「개인정보보호법」은 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보를

그 보호대상으로 하고 있다(법 제1조). 여기서 개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다(법 제2조 제2호). 즉, 공공기관에 의하여 처리되는 개인정보를 대상으로 하기 때문에 민간부문에서 처리되는 개인정보의 처리는 보호의 대상에서 제외된다. 오늘날 민간부문에서 막대한 양의 개인정보가 수집되어 관리되고 있으며, 민간이 처리하는 각종의 신용정보와 고객관리정보, 상품판매 고객정보 등은 그 사용목적에 따라서 개인의 기본권을 침해할 우려가 매우 높다.[212]

또 컴퓨터에 의하여 처리되는 개인정보를 대상으로 하고 있기 때문에 수작업으로 처리되는 정보는 이 법에 의하여 보호를 받지 못한다. 이들 수작업처리의 일반문서에 수록된 개인정보는 기록의 대량성, 검색의 신속성과 용이성, 처리의 불투명성 등의 특징을 갖는 전산처리정보에 비하여 상대적으로 개인의 사생활 침해의 가능성이 적을 수 있다. 그리고「형법」,「국가공무원법」,「주민등록법」,「의료법」,「사회복지사업법」등의 개별 법률에서 직무관련비밀 누설금지 의무 등이 규정되어 있어 어느 정도 규율이 가능한 것이 사실이다.

(3) 적용대상

「개인정보보호법」의 적용대상은 공공기관에 한정한다. 다만 이 법 제22조에서 민간에 대한 의견제시·권고는 허용되고 있다. 여기서 말하는 공공기관이란 국가행정기관·지방자치단체 기타 공공단체 중 대통령이 정하는 기관을 말한다(법 제1조 제1호). 기타 공공단체 중 대통령이 정하는 기관이란「초·중등교육법」및「고등교육법」과 그 밖의 다른 법률에 따라 설치된 각급 학교,「공공기관의 운영에 관한 법률」제4조에 따른 공공기관, 특별법에 의하여 설립된 특수법인,「지방공기업법」에 따른 지방공사 및 지방공단이 해당한다. 다만 특별법에 의하여 설립된 특수법인 중「금융실명거래 및 비밀보장에 관한 법률」제2조 제1호에 따른 금융기관은 이에 포함되지 아니한다(시행령 제2조).

212) 총무처, 앞의 주 109), 26-28면 참조.

(4) 적용제외

「개인정보보호법」은 공공기관의 컴퓨터 등에 의하여 처리되는 개인정보의 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우 적용되지 아니하며, 특히 공공기관의 컴퓨터 등에 의하여 처리되는 개인정보 중「통계법」에 의하여 수집되는 개인정보와 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공·요청되는 개인정보의 보호에 관하여는 적용하지 아니한다(법 제3조).

통계법에 의하여 수집되는 개인정보의 경우 특정 개인을 식별할 수 없는 형태로 처리되는 것이 일반적이어서 개인의 기본권을 침해할 가능성이 적고, 통계법이 개인정보를 위한 규정을 별도로 두고 있기 때문에「개인정보보호법」의 적용에서 제외된다.[213]

그리고 국가안전보장과 관련된 정보 분석 목적의 개인정보도 고도의 비밀성과 보안성이 유지될 필요가 있고 국가정보원 등 관련 법률에 비밀누설금지 등의 조항이 마련되어 있기 때문에 적용제외의 사유로 인정되었다.[214] 이를 상세히 살펴보면 <표 14>와 같다.

<표 14> 「개인정보보호법」적용 제외 대상정보

「통계법」에 의해 수집되는 개인정보	■ 적용제외 이유 - 개인정보의 통계처리로 사생활 침해 가능성 희박 - 「통계법」에 관계조항 규정 : 비밀번호의무(제8조), 통계목적 외 사용금지(제9조), 비밀누설에 대한 벌칙(제18조 제1항) 등 ■ 외국의 입법례 - 일본 : 통계목적을 위해 수집된 개인정보는 적용제외 - 미국 : 통계관련 개인정보는 파일공고 등 특정사항 적용제외
국가안전보장 관련 정보분석 목적 개인정보	■ 대상정보 - 국가정보원이 수집·작성하는 대공 및 대정부 전복 등에 관한 국내외 정보, 통신정보 등 ■ 적용제외 이유 - 국가안전보장과 관련된 정보는 그 특성상 고도의 비밀성·보안성 유지 필요 - 국가정보원 등 관계 법률에 비밀누설금지 등 관계조항 규정 ■ 외국의 입법례 : 대부분의 국가에서 적용제외
수작업 처리 일반문서에 수록된 개인정보	■ 수작업 개인정보의 보호체계 - 현행「형법」및 각 개별법에 직무관련 비밀누설금지 의무 등을 규정하고 위반시 형벌 부과 · 현행「형법」에 의한 규정 : 공무원의 직무상 비밀누설금

213) 총무처, 앞의 책, 46면.
214) 권건보, 앞의 주 102), 127-128면.

	지(제127조), 업무상 비밀누설금지(제317조) · 기타 개별법에 의한 규제 :「국가공무원법」,「주민등록법」,「의료법」,「사회복지사업법」등에서 직무상 알게 된 비밀의 누설금지 및 위반시 형벌 또는 징계 부과 ■ 적용제외 이유 - 그 특성상 외부유출 등의 가능성이 적을 뿐 아니라 현행 법률로도 규제 가능 · 각 개별법에 의한 처벌조항 적용시 공무원 의제 규정 적용 등 - 일반문서까지 적용할 경우, 행정부담 가중으로 법의 실효성 확보 곤란 · 대장작성, 열람, 정정 청구의 처리 등 법 운영에 필요한 인력, 경비 등의 가중으로 본연의 업무수행 곤란 ※ 개인정보보호 문제는 전산처리 특성인 기록의 대량성, 처리의 신속성 등으로 인해 발생 ■ 외국의 입법례 - 영국, 일본, 독일, 프랑스, 스웨덴 : 컴퓨터에 의한 전산처리정보에 한정 - 미국 : 수작업 처리 등 일반문서 포함

3) 공공기관의 의무

「개인정보보호법」은 공공기관의 장에게 자기정보관리통제권을 보장하기 위하여 필요한 의무를 규정하고 있다. 먼저 공공기관의 장이 개인정보를 수집하는 경우 그 목적을 명확히 하여야 하고, 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 한다. 그리고 수집된 정보를 목적 외의 용도로 활용하여서는 아니되며, 처리정보의 정확성 및 최신성을 보장하고, 그 보호의 안전성을 확보하여야 한다.

또한 공공기관의 장은 개인정보관리의 책임관계를 명확히 하고, 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다(법 제3조의2). 이것은 공공기관이 컴퓨터에 의해 개인정보를 처리하고 보유하는 과정에서 발생할 수 있는 개인정보의 오·남용 및 유출을 방지하기 위한 것이다.

이러한 의무는「개인정보보호법」이 컴퓨터에 의해 대량으로 처리되는 개인정보를 보호대상으로 한다는 점과 공공부문이라는 특성상 공익도 중요한 가치로 인정되기 때문에 특히 중요하다.

(1) 수집·보유의 제한

「개인정보보호법」은 일반 국민들의 개인정보를 공공기관이 대량으로 처리한다는 점에서 개인정보의 수집·보유의 근거를 법률상으로 규율하고 있다. 즉, 공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다. 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 문서 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있도록 안내하여야 한다. 다만, 개인정보파일의 보유를 위하여 행정안전부장관과 사전협의가 필요 없는 개인정보파일을 보유할 목적으로 개인정보를 수집하는 경우에는 그러하지 아니하다(법 제4조). 이 규정은 인간 내면의 자유나 양심의 자유 등 기본권의 본질적 내용을 침해할 우려가 있는 정보에 대해서는 수집단계에서부터 제한함으로써 자기정보관리통제권의 보호에 만전을 기한다는 점에서 의의가 있다.

그러나 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있다(법 제5조). 공공기관의 장이 개인정보파일을 보유하고자 하는 경우에는 중앙행정기관의 장은 개인정보파일의 명칭·보유목적, 보유기관의 명칭, 개인정보파일에 기록되는 개인정보 및 항목의 범위, 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭, 개인정보파일의 열람예정시기, 열람이 제한되는 처리정보의 범위 및 그 사유, 기타 대통령령이 정하는 사항 등을 행정자치부장관에게 제출하여야 한다(법 제6조 제1항). 이는 공공기관이 개인정보파일을 보유하기 전에 감독기관에 사전에 통보하여 감독기관이 개인정보처리의 현황 및 실태를 파악하도록 하기 위함이다.[215] 다만, 일정한 개인정보파일에 대해서는 중앙행정기관의 장을 거쳐 관련서류를 제출하여야 한다(법 제6조 제2항).

그리고 행정안전부장관 또는 관계 중앙행정기관의 장은 사전 통보를 받은 사항을 년1회 이상 관보 또는 인터넷 홈페이지 등에 공고하여야 하며(법 제7조), 보유기관의 장은 당해 기관이 보유하고 있는 개인정보파일별로 개인정보파일대장을 작성하여 일반인이 열람할 수 있게 하여야 한다

215) 김태현, "개인정보보호제도에 관한 헌법적 고찰", 박사학위논문, 경희대학교 대학원, 2003, 156면.

(법 제8조).

(2) 이용 및 제공의 제한

개인정보 보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니된다(법 제10조). 또한 보유목적에 따라 처리정보를 이용하게 하거나 제공하는 경우에도 업무수행에 필요한 최소한의 범위로 그 이용 또는 제공을 제한하여야 한다(법 제10조 제2항).

이에 대한 예외로서 일정한 사유에 해당되면 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있다(법 제10조 제3항). 그 사유로서는 ① 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, ② 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 공공기관 개인정보보호 심의위원회의 심의를 거친 경우, ③조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, ④ 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우, ⑤ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 이용하게 하거나 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, ⑥ 범죄의 수사와 공소의 제기 및 유지에 필요한 경우, ⑦ 법원의 재판업무수행을 위하여 필요한 경우 등이다.

그러나 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 정보처리 이용 및 제공이 금지된다(법 제10조 제3항 단서).

처리정보를 정보주체 외의 자에게 이용하게 하거나 제공하는 때에는 처리정보를 수령한 자에 대하여 사용목적·사용방법 기타 필요한 사항에 대하여 제한을 하거나 처리정보의 안전성확보를 위하여 필요한 조치를 강구하도록 요청하여야 하며, 이러한 요청을 받은 정보수령자는 처리정보의 안전성 확보를 위한 조치를 취하여야 한다(법 제10조 제4항). 그리고 보유기관으로부터 처리정보를 제공받은 자는 보유기관의 동의 없이 당해 처리

정보를 제3자에게 이용하게 하거나 제공하여서는 아니된다(법 제10조 제5항). 한편 보유목적 외의 목적으로 이용하게 하거나 제공하는 경우에는 그 이용 또는 제공의 법적 근거·목적 및 범위 등에 관하여 필요한 사항을 정보주체가 쉽게 확인할 수 있도록 관보 또는 인터넷 홈페이지 등에 게재하여야 한다(법 제10조 제6항).

또 목적한 사용이 종료된 경우에는 지체 없이 파기할 것을 규정하고 있다. 보유기관의 장은 개인정보파일의 보유목적 달성 등 당해 개인정보파일의 보유가 불필요하게 된 경우에는 당해 개인정보파일을 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 파기할 수 없다(법 제10조의 제2항). 개인정보파일을 파기한 경우 보유기관의 장은 개인정보파일을 파기한 사실을 관보 또는 인터넷 홈페이지 등에 공고하여야 한다(법 제10조의 제6항).

4) 처리정보의 열람청구와 정정청구

정보주체는 개인정보파일대장에 기재된 범위 안에서 문서로 본인에 관한 처리정보의 열람 또는 문서에 의한 사본의 수령을 보유기관의 장에게 청구할 수 있다(법 제12조 제1항).

청구를 받은 보유기관의 장은 청구서를 받은 날부터 10일 이내에 청구인으로 하여금 당해 처리정보를 열람할 수 있도록 하여야 한다. 이 경우 10일 이내에 열람하게 할 수 없는 정당한 사유가 있는 때에는 청구인에게 그 사유를 통지하고 열람을 연기할 수 있으며, 그 사유가 소멸한 때에는 지체 없이 열람하게 하여야 한다(법 제12조 제2항).

그러나 일정한 경우 보유기관의 장은 열람을 제한할 수 있다. 즉 열람을 청구한 청구인으로 하여금 당해 처리정보를 열람하도록 하는 것이 ① ㉠ 조세의 부과·징수 또는 환급에 관한 업무, ㉡「초·중등교육법」및「고등교육법」에 따른 각 급 학교와「평생교육법」에 따른 평생교육시설에서의 성적평가 또는 입학자의 선발에 관한 업무, ㉢ 학력·기능 및 채용에 관한 시험, 자격의 심사, 보상금·급부금의 산정 등 평가 또는 판단에 관한 업무, ㉣ 다른 법률에 의한 감사 및 조사에 관한 업무, ㉤ 대통령령이 정하는 업무로서 당해 업무의 수행에 중대한 지장을 초래하는 경우, ② 개인의 생명·신체를 해할 우려가 있거나 개인의 재산과 기타의 이익

을 부당하게 침해할 우려가 있는 경우, 그 사유를 통지하고 당해 정보처리의 열람을 제한할 수 있다(제14조 제1항).

한편 본인의 처리정보를 열람한 정보주체는 보유기관의 장에게 문서로 당해 처리정보의 정정 또는 삭제를 청구할 수 있다. 다만, 다른 법률에 당해 처리정보가 수집대상으로 명시되어 있는 경우에는 그 삭제를 청구할 수 없다(법 제14조 제1항).

정정 또는 삭제청구를 받은 보유기관의 장은 처리정보의 내용의 정정 또는 삭제에 관하여 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다(제14조 제2항).

이와 같은 개인정보 처리의 열람·정정 청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 「행정심판법」이 정하는 바에 따라 행정심판을 청구하거나「행정소송법」이 정하는 바에 따라 행정소송을 제기할 수 있다. 행정심판을 제기하는 경우 국가행정기관 및 지방자치단체 외의 공공기관의 장의 처분 또는 부작위에 대한 감독행정기관은 관계 중앙행정기관의 장으로 한다(법 제15조).

5) 지도 및 감독

행정안전부장관은 이 법의 목적을 달성하기 위하여 필요하다고 인정되는 경우에는 공공기관의 장에게 개인정보의 보호에 관하여 의견을 제시하거나 권고할 수 있다(법 제19조).

한편 관계 중앙행정기관의 장은 컴퓨터 등에 의하여 처리되는 개인정보의 보호를 위하여 필요한 때에는 국가행정기관 및 지방자치단체 외의 공공기관에 대하여 개인정보의 보호에 관하여 의견을 제시하거나 지도·점검 등을 할 수 있다(법 제21조).

그리고 공공기관외의 개인 또는 단체는 컴퓨터 등을 사용하여 개인정보를 처리함에 있어 공공기관의 예에 준하여 개인정보의 보호를 위한 조치를 강구하여야 하며, 관계중앙행정기관의 장은 개인정보의 보호를 위하여 필요한 때에는 공공기관외의 개인 또는 단체에 대하여 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다(법 제22조).

<표 15>「개인정보보호법」의 보호내용과 한계

「공공기관의 개인정보보호에 관한 법률」	
제정일	■ 1994. 1. 7(공포), 1995. 1. 8(시행), 2번의 일부개정과 3번의 타법개정을 거침. ■ 현행법률 제8871호, 2008. 2. 29, 타법개정, 2008. 2. 29(시행)
적용분야	■ 공공분야
공공기관의 범위	■ 국가행정기관・지방자치단체・학교・정부투자기관・특수법인
보호대상	■ 컴퓨터에 의하여 처리되는 생존하는 자연인의 개인정보 (단, 개인정보 DB에 수록된 개인정보만 보호) ※ 체계적인 검색시스템(DB)을 구축하지 않는다면, 아무런 제한 없이 개인정보 수집 가능함
적용제외 개인정보	■ 「통계법」에 의해 수집되는 개인정보 ■ 국가안전보장 목적으로 수집되는 개인정보
수집제한의 원칙	■ 사상・신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보는 수집 자체가 금지됨(단, 동의가 있거나 다른 법률에서 명시적으로 수집을 허용하고 있는 경우에는 수집 가능) ■ 소관업무 수행에 필요한 범위 안에서 개인정보DB 보유가능 ■ 보유절차: 공고사항(보유목적・수집방법・DB수록 항목 등)을 행정안전부장관에게 사전통보 → 연 1회 이상 관보게재(8가지의 광범위한 예외를 인정하고 있음) ■ 보유기관: 위 공고사항을 기재한 개인정보DB대장을 작성・비치 ※ 개인정보의 개별수집에 대해 이 원칙을 요구하는 것이 아님 ※ 정보주체의 인식명확성 요건이 사실상 결여되어 있음
목적구속의 원칙	■ 원칙: 사전에 공시된 개인정보DB의 보유목적이 아닌 다른 목적으로 개인정보를 이용하거나 제공하는 것을 금지 ■ 예외: 8가지의 광범위한 예외를 인정하고 있음 - 소관업무 수행을 위해 이용할 상당한 이유가 있는 경우 - 범죄의 수사와 공소의 제기 및 유지에 필요한 경우 - 기타 대통령령이 정하는 특별한 사유가 있는 경우 등 ※ 광범위한 예외 때문에 원칙이 형해화될 가능성이 있음 ※ 정보주체의 동의나 인식 없이 목적외 이용・제3자의 제공 가능
시스템 공개의	■ 원칙: 개인정보 DB 내역을 관보게재, 개인정보DB대장 작성

원칙	・비치 ■ 예외: 상당한 DB가 관보게재・DB대장수록・일반인의 열람에서 제외 통계목적・국가안전보장목적의 DB는 아예 이 법의 적용을 받지 않음 ※ 시스템공개원칙이 유명무실해질 가능성이 높음
정보정확성의 원칙	■ 보유기관의 장은 정보처리의 정확성・최신성 확보 노력 ※ 선언규정에 불과함
보안의 원칙	■ 보유기관의 장은 안전성확보에 필요한 조치를 강구하여야 함(선언규정) ■ 개인정보처리기관은 개인정보의 누설이나 부당목적 이용이 금지됨(형사처벌)
참여의 원칙	■ 정보주체는 개인정보의 DB에 기재된 범위 안에서 서면으로 열람・정정을 청구할 수 있음 ■ 일정 업무의 경우 업무수행에 중대한 지장이 있을 때 열람제한 가능
감독의 원칙	■ 행정안전부가 법상의 집행기관이나, 위법사실에 대한 감시・감독・집행의 권한과 기능을 가지지 못함. 독립된 감독기구의 부재

*이인호, 개인정보보호법제의 현대화방안에 관한 연구. 국회사무처 법제실, 2005, 32면 참조.

6) 문제점

(1) 적용 대상의 제한

전술한 바와 같이「개인정보보호법」은 공공기관의 컴퓨터에 의하여 처리되는 개인정보를 보호하기 위하여 각 행정기관이 개인정보처리 시스템 내지 개인정보 데이터베이스 즉, 개인정보파일을 개인별로 보유하고 있는 경우에 그 보유범위 및 내부적 절차를 규율하고, 개인정보파일에 개인별로 수록된 개인정보를 이용하거나 제3자에게 제공하는 것에 대해 일정한 실체적 및 절차적 제한을 가하며, 정보주체에게 열람 및 정정청구권을 인정하는 것을 주된 내용으로 하고 있다.[216]

하지만「개인정보보호법」은 공공기관이 컴퓨터에 의하여 자동처리된 개인정보만을 적용대상으로 하고 있어 수작업에 의해 처리된 문서에 대해서는 적용할 수 없는 한계를 가지고 있다. 개인정보를 효과적으로 보호하기 위해서는 전산화된 개인정보뿐만 아니라 수기로 작성된 개인정보에 대

216) 이인호, 개인정보보호법제의 현대화방안에 관한 연구. 국회사무처 법제실. 2005. 20면.

해서도 적용되어야 할 것이다.

또한 이 법률은 자연인에 관한 정보만을 보호대상으로 하고, 법인이나 단체에 관한 정보를 제외하고 있어 법률적용의 범위와 한계에 대한 문제가 따를 수 있다.

(2) 적용 범위의 제한

「개인정보보호법」은 개인정보보호에 관하여 지나치게 예외조항을 두고 있어 오히려 국민의 기본권 침해를 정당화시키는 결과를 초래할 가능성이 있다. 즉, 법 제3조 제1항은 '공공기관의 컴퓨터 등에 의하여 처리되는 개인정보의 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법이 정하는 바에 의한다'고 규정함으로써 이 법률이 공공부문에 있어서의 개인정보보호에 관한 명실상부한 기본법이면서도 스스로 예외를 인정하고 있다.

또한 '공공기관의 컴퓨터 등에 의하여 처리되는 개인정보 중「통계법」에 의하여 수집되는 개인정보와 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공·요청되는 개인정보의 보호에 관하여는 이 법을 적용하지 아니한다'라고 규정함으로써「통계법」에 의하여 수집되는 개인정보와 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공·요청되는 개인정보'에 관하여는 정보처리의 존재 자체가 정보주체의 인식이나 사회적 감시로부터 완전히 벗어날 수 있도록 광범위한 예외를 규정[217]하고 있어 자기정보관리통제권을 인정하고 있는 헌법정신에 배치된다. 뿐만 아니라 법률자체가 개인정보보호법이 아닌 개인정보이용법 또는 국가보호법 내지는 국정보호법의 형태로 존재할 가능성이 크다.

(3) 개인정보 수집에 대한 규제 미비

개인정보보호는 정보조사나 수집의 단계에서부터 이루어져야 한다. 즉, 수집된 개인정보의 오·남용으로부터 개인정보를 보호하는 것은 당연한 것이지만, 보다 효율적인 것은 그 전단계인 수집단계에서부터 보호장치를 마련하는 일이다. 따라서 자기정보관리통제권에서는 수집제한의 원칙이

217) 이인호. "한국의 개인정보보호법제의 문제점과 정비방안. 각국 개인정보보호법 제도의 비교법적 접근", 2003 제2회 개인정보보호 심포지움, 한국정보보호진흥원, 2003. 3. 15, 114-115면.

요구된다.

그런데「개인정보보호법」은 컴퓨터를 이용하여 처리된 개인정보와 이를 개인정보파일 형태로 보유하는 것을 적용대상으로 하고 있다. 공공기관이 보유하는 개인정보는 수집과정을 거치지 않고는 보유할 수 없는 것임에도 불구하고 수집과정에 대한 규정이 없이 개인정보의 입력·저장·편집·검색 및 출력 기타 이와 유사한 행위에 대해서만 규정하고 있다. 따라서 개인정보 중 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 경우가 아니면 개인정보파일 형태로 작성된 것이 아닌 경우, 공공기관은 아무런 제한도 받음이 없이 개인정보를 수집·보유할 수 있다는 결과가 된다.

또한 개인정보 수집자는 정보의 수집에 앞서 정보주체에게 개인정보 수집의 목적, 용도, 안전보호장치 등에 대하여 알리는 것이 선진국의 일반적인 입법동향임에도 불구하고 '공공기관의 장이 개인정보파일을 보유하고자 하는 경우에는 행정안전부장관과 협의하여야 한다'고 하면서도 정보주체에 대하여는 고지의무를 규정하고 있지 않다. 따라서 개인정보주체의 권익보호에 대한 배려가 미흡하다.

(4) 목적구속의 원칙으로 인한 의미 반감

「개인정보보호법」제10조 제1항에서는 '보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니 된다'고 하여 이른바 목적구속의 원칙을 규정하고 있다. 그러나 제10조 제2항에서 매우 광범위하게 예외를 인정하고 있어 이 목적구속의 원칙의 의미가 반감되고 있다.

(5) 민간부문의 개인정보 남용에 대한 규제 미흡

「개인정보보호법」은 공공기관을 제외한 민간부문에서의 개인정보 남용에 대해서는 아무런 규정을 두고 있지 않다. 개인이나 민간기업에 대해서는 제22조에서 '공공기관외의 개인 또는 단체는 컴퓨터 등을 사용하여 개인정보를 처리함에 있어 공공기관의 예에 준하여 개인정보의 보호를 위한 조치를 강구하여야 하며, 관계중앙행정기관의 장은 개인정보의 보호를

위하여 필요한 때에는 공공기관외의 개인 또는 단체에 대하여 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다'고 규정하고 있을 뿐이다. 그리고 이 규정은 위반시 벌칙조항을 두고 있지 않아 강제규정이라고 할 수 없다. 따라서 민간부문에서의 개인정보보호가 소홀해질 우려가 있다.[218]

나.「정보통신망 이용 촉진 및 정보보호에 관한 법률」

1) 주요내용

「정보통신망 이용 촉진 및 정보보호에 관한 법률」(이하「정보통신망법」이라함) 제1조에서는 이 법의 목적으로 '정보통신망의 이용을 촉진하고 정보통신 서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함'을 규정하고 있다.

여기에서 말하는 정보통신망이란「전기통신기본법」에 따른 전기통신을 하기 위한 기계·기구·선로 기타 전기통신에 필요한 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다. 그리고 '정보통신서비스'란「전기통신기본법」에 의하여 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다(제2조 제1항 제1호 내지 제2호). 또한 개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보를 말하며, 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다(제2조 제1항 제6호).

2) 적용대상 및 범위

「정보통신망 이용 촉진 및 정보보호에 관한 법률」은 정보통신 서비스

218) 김연수, 개인정보보호, (주)사이버출판사, 2001, 126면 ; 김태연, 앞의 주 112), 160면.

제공자와 그로부터 이용자의 개인정보를 제공받은 자에게 적용된다. 정보통신 서비스 제공자란「전기통신사업법」에 의한 허가를 받거나 등록 또는 신고를 하고 전기통신역무를 제공하는 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다(제2조 제1항 제3호).

한편「정보통신망 이용 촉진 및 정보보호에 관한 법률」제67조는 이 법의 일정조항을 정보통신 서비스 제공자 외의 자에 대하여 준용하도록 규정하고 있다. 즉 정보통신 서비스 제공자 외의 자로서 재화 등을 제공하는 일정한 자가 자신이 제공하는 재화 등을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에는 이 법이 규정하고 있는 개인정보의 보호에 관한 조항(법 제22조 내지 제32조 중의 중요사항)을 준용하도록 하고 있다. 따라서 오프라인상에서 개인정보를 취급하는 자에게도 이 법을 적용할 수 있는 근거규정을 마련하였다.

3) 개인정보의 수집 및 제한

정보통신 서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 개인정보의 수집·이용목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용기간 등의 모든 사항을 이용자에게 알리고 동의를 받아야 한다(법 제22조 제1항). 하지만, 정보통신 서비스 이용계약의 이행을 위하여 필요한 경우, 정보통신 서비스 제공에 따른 요금정산을 위하여 필요한 경우,「정보보호법」또는 다른 법률에 특별한 규정이 있는 경우에는 이용자의 동의를 얻지 않아도 된다(법 제22조 제2항 제1호 내지 제3호).

한편 정보통신 서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다(법 제23조 제1항). 또한 정보통신 서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신 서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니된다(법 제23조 제2항). 이는 인간 내면의 자유나 양심의 자유와 같이 기본권의 본질적인 내용을 침해할 우려가 있는 정보에 대해서는 수집 자체를 금지함으로써 자기정보관리통제권을 보호하기 위함일 것이다.

다만, 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다(법 제23조 제1항 단서).

4) 개인정보의 이용 및 제공

「정보통신망법」은 개인정보를 보호하기 위하여 개인정보의 이용 및 제공을 제한하는 규정을 두고 있다. 먼저, 정보통신 서비스 제공자는 이용자의 동의가 있거나, 정보통신 서비스의 제공에 따른 요금정산을 위하여 필요한 경우, 통계작성·학술연구 또는 시장조사를 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우, 다른 법률에 특별한 규정이 있는 경우를 제외하고는 고지의 범위 또는 정보통신서비스 약관에 명시된 범위를 넘어 개인정보를 이용하거나 제3자에게 제공하여서는 아니된다(법 제24조 제1항).

그리고 정보통신 서비스 제공자 등이 제3자에게 개인정보 수집·보관·처리·이용·제공·관리·파기 등을 할 수 있도록 위탁하는 경우에는 그 사실을 이용자에게 고지하여야 하고, 이러한 사실을 변경하는 경우에도 같다(법 제25조 제1항).

한편 정보통신 서비스 제공 등이 영업의 전부 또는 일부를 양도하거나 합병·상속 등으로 그 권리·의무를 이전하는 경우 이용자에게 일정한 사항을 인터넷 홈페이지에 게재하고 통지하여야 한다(법 제26조 제1항). 이들 규정들은 정보통신 서비스 제공자 등으로 하여금 타인의 개인정보에 대한 오·남용을 방지함으로써 정보주체의 권리와 이익이 부당하게 침해되는 것을 방지하기 위함이다.

5) 이용자의 권리

「정보통신망법」은 정보통신 서비스 제공자가 제공하는 정보통신 서비스의 이용자의 권리를 명시적으로 규정하고 있다. 먼저 이용자는 정보통신 서비스 제공자 등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다(법 제30조 제1항). 이용자가 동의를 철회하면 정보통신 서비스 제공자 등은 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다(법 제30조 제3항).

그리고 이용자는 정보통신 서비스 제공자 등에 대하여 정보통신 서비스 제공자 등이 가지고 있는 이용자의 개인정보, 정보통신 서비스 제공자 등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황, 정보통신 서비스 제공자 등에게 개인정보 수집·이용·제공 등의 동의를 한 현황에 대한 열람이나 제공을 요구할 수 있고(법 제30조 2항), 오류가 있는 경우에는 그 정정을 요구할 수 있다. 열람 또는 제공을 요구받은 정보통신 서비스 제공자 등은 지체 없이 필요한 조치를 하여야 한다(법 제30조 제4항).

정보통신 서비스 제공자 등은 오류의 정정을 요구받으면 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알리는 등 필요한 조치를 하여야 하고, 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공하여서는 아니된다(법 제30조 5항).

6) 개인정보의 누설금지

이용자의 개인정보를 취급하고 있거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니되며, 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니된다(법 제28조의2 제1항 내지 제2항).

7) 검토

(1) 입법체계상의 모순

「정보통신망법」의 목적은 정보통신망의 이용을 촉진하면서도 한편으로는 개인정보보호를 목적으로 하고 있어, 동일법 내에서 서로 상반된 가치를 추구하는 규정을 두고 있다. 그리고 정보통신망의 이용촉진 및 정보통신 서비스를 이용하는 자의 개인정보를 보호하는 것으로 명시하고 있음에도 불구하고 이 법 제58조에서 정보통신망과 무관한 오프라인 민간 사업자에 대해서도 규율하는 것은 입법체계상 모순을 내포하고 있다.

이러한 입법체계상의 모순을 해결하고 개인정보보호의 실효성을 확보하기 위해서는 이 법의 '정보통신망 이용촉진' 부분과 '정보보호' 부분을 분리하고 '정보보호'는 '개인정보보호'로 고쳐서 이 두 부분을 별도 법률로 규정해야 할 필요가 있다.

(2) 적용범위의 제한

「정보통신망 이용 촉진 및 정보보호에 관한 법률」제24조 제3항에서 정보통신 서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자를 '정보통신 서비스 제공자 등'이라고 규정함으로써 이 법의 적용대상으로 하고 있고, 또한 제58조에서는 정보통신 서비스 제공자 외의 자로서 재화 또는 용역을 제공하는 자 중 대통령령이 정하는 자가 자신이 제공하는 재화 또는 용역을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에만 준용하도록 하고 있다.

여기서 '대통령령이 정하는 자'라 함은 여행업 또는 호텔업을 행하는 자, 항공운송사업을 행하는 자, 학원 또는 교습소를 설립·운영하는 자, 그 밖에 재화 또는 용역을 제공하면서 회원제 또는 그와 유사한 형태로 개인정보를 수집하는 사업자로서 관계중앙행정기관의 장과 협의하여 정보통신부령으로 정하는 자를 말한다(시행령 제28조).

따라서 정보통신 서비스를 제공하는 비영리법인이나 단체 또는 개인이 영리 목적 없이 개인정보를 수집·이용하는 경우와 정보통신 서비스 사업자가 아닌 자로서 시행령 제28조에 열거되지 아니한 기업들이 개인정보를 수집하고 이를 이용하여 마케팅활동을 하는 경우에는 적용되지 않는다.[219]

또한 정보주체의 범위를 정보통신서비스의 이용자로 한정함으로써 이용자 외의 제3자에 대한 개인정보침해에 대한 규제에 한계가 있다.[220] 즉, 이 법은 개인정보보호를 위해 설정하고 있는 기본 구도가 개인정보처리자와 정보주체간의 관계가 아니라 서비스 제공자와 그 서비스를 이용하는 이용자 사이에서 발생하는 개인정보의 수집·이용·제3자 제공을 규율하는 관계임에 따라 적용범위가 제한되어 있어 온라인 및 오프라인에서 개인정보보호를 위한 일반법으로 기능을 다하기에는 한계가 있다.

---

219) 이형구, 개인정보 수집자 및 이용자의 책임에 대한 입법론, 개인정보보호 주요 쟁점, 한국정보보호진흥원, 2001, 87-89면.

220) 이인호, 앞의 주 212), 166-167면.

다.「전자정부법」

「전자정부법」은 행정업무의 전자적 처리를 위한 기본원칙·절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것을 목적으로 하고 있다.

이 법에서는 행정정보공동이용의 원칙과 개인정보보호의 원칙을 규율하고 있다. 먼저 행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다(법 제11조)고 규정하여 행정정보공동이용의 원칙과 행정정보의 중복 수집을 금지하고 있다.

그리고 행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다(법 제12조)고 하여 자기정보관리통제권을 법률로 규정하고 있다.

또 민원인으로부터 전자문서를 수신한 행정기관의 장은 그 수신사실을 인터넷 등에 게시하여 전자문서를 송신한 자가 확인할 수 있도록 하여야 하며, 인터넷 등에 수신사실을 게시하는 때에는 접수번호·수신일자·접수등록번호·제목·수신기관 및 담당공무원의 연락처 등을 명시하되, 전자문서를 송신한 자의 개인정보가 침해되지 아니하도록 하여야 한다(시행령 제6조 제2항 내지 제3항)고 명시, 개인정보의 침해를 방지하고 있다.

행정기관은 행정정보를 서로 공동이용하기 위하여 정보통신망으로 다른 행정정보의 보유기관에 송신하고자하는 경우에는 특별한 사유가 있는 경우를 제외하고는 개인정보의 보호를 위하여 국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 대통령이 정하는 방법으로 송신하여야 한다(법 제21조 제 3 항).

한편 행정안전부장관이 설치하는 행정정보공동이용서비스센터는「공공기관의 개인정보보호에 관한 법률」에 의한 개인정보파일에 관한 공고 내용의 데이터베이스화와 그 안내서비스 제공의 업무를 행한다(시행령 제29조 제2항 제2호).

제4절 전자정부하에서 개인정보보호

1. 개인정보의 수집 및 관리

가. 개인정보 수집

1) 개인정보의 수집 근거

개인정보보호를 위해서는 먼저 수집제한의 원칙들이 지켜져야 한다. 즉, 개인정보의 수집은 제한되어야 하고, 그러한 자료는 합법적이고 정당한 수단에 의하여 정보주체의 인지나 동의에 의하여 수집되어야 한다.

우리나라의「전자정부법」은 행정정보공동이용을 위한 기본법에 해당함에도 불구하고 개인정보의 수집에 대한 명확한 규정을 제시하지 않고 있다.

수집의 제한과 관련해서는「공공기관의 개인정보보호에 관한 법률」에 의하면 공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 예외가 있다. 그리고 공공기관의 장은 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 문서(「전자정부법」제2조 제5호에 따른 전자문서) 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있도록 안내하여야 한다(법 제4조 제1항 내지 제2항).

여기서 '현저하게 침해할 우려'가 있는 개인정보를 수집하여서는 아니된다고 하는데 그 현저한 범위가 어디까지이며, 그 기준과 범위는 어디까지인가. 매우 추상적인 문구라고 하지 않을 수 없다. 또한 정보의 공동이용시에 정보주체의 인지나 동의에 의한 수집의 원칙은 침해될 위험이 매우 크다. 즉, 행정정보공동이용에서는 개인정보를 개인으로부터 직접수집하기보다는 다른 파일이나 다른 조직이 구축하여 놓은 개인정보를 활용하는 것이 특징이므로 인지나 동의를 얻기가 어려울 뿐만 아니라 인지나 동의가 있다고 하더라도 형식화될 위험성이 상존하게 된다.

2) 수집목적의 구체화

행정정보공동이용을 위해 개인정보를 수집할 경우, 수집 당시에 그 목적이 구체화되어 있어야 하고 목적의 범위 내에서 사용되어야 한다.

그러나「공공기관의 개인정보보호에 관한 법률」에서는 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있다(법 제5조)고 포괄적으로 규정하고 있어서 수집목적의 구체화가 제도적으로 확립되지 못하고 있다. 개인정보의 이용 실태에서도 개인정보의 수집근거가 법적인 근거를 가지고 있지 않다는 것은 또 다른 측면에서 보면 개인정보를 수집하는 기본적인 목적이 명확하지 않은 것으로 추론될 수 있다.

개인정보공동이용은 대부분 특정 기관이 자기의 사업 목적을 위하여 수집·관리하고 있는 개인정보를 연계하여 사용하게 된다. 이러한 개인정보공동이용은 수집당시에 그 목적이 구체화되어야 한다는 원칙을 위배하는 것이고, 목적 외 다른 기관이 사용하는 경우가 많아지게 된다. 특히 신원조사제도는 그 정보의 수집목적이 매우 추상적이고 자의적으로 설정되어 있어서 개인의 기본권을 침해할 소지가 매우 높다[221]고 할 수 있다.

나. 개인정보 관리

1) 개인정보 자료의 질의 문제

개인정보공동이용에 있어서 개인정보가 부정확하고 질이 낮을 경우 의사결정과정에서 생각하지도 못하는 오류가 발생할 수 있다. 정보의 공동이용은 정보의 완전성, 정확성, 적절성 등과 같은 정보의 질이 더욱 중요시 된다.

데이터 질을 유지하는 방법으로 파일의 오류수정을 하는 경우 집중화된 시스템이 분산 시스템보다는 더 용이하다고 하지만, 미래의 정보관리체계는 분산 데이터베이스 시스템이 보다 일반화될 전망이다. 이러한 분산 시스템에서는 데이터의 정확성의 문제는 더욱 커지게 될 것이다. 이것이 불완전하고 부정확한 데이터의 질을 초래하는 중요한 요인이 될 수 있다.

2) 자료의 안전성 확보

221) 이에 관해서는 박홍윤, 앞의 주 88), 80-83면 참조.

공공기관에서 관리하는 개인자료는 자료의 상실이나 부당한 접근, 파괴, 이용, 수정이나 공개와 같은 위험에 대하여 적절한 안전장치에 의하여 보호되어야 한다. 그러나 개인정보를 공동이용하는 경우 공동이용 시스템이 가지는 네트워크화, 분산시스템의 운영, 사용자 중심의 시스템 운영, 온라인에 의한 데이터의 처리 등에 의하여 자료의 안전성 문제는 지속적으로 발생한다.

가장 문제가 되는 것은 정보유출로 인한 개인정보의 침해 문제다. 개인정보의 이용률의 증가에 따라 유출의 가능성도 그 만큼 증가되는 것이다. 공동이용할 수 있는 데이터베이스 시스템의 확대와 네트워크화는 이용자 수의 증대와 시스템의 복잡성에 의하여 안전성의 문제를 더욱 가중시킨다. 이에 의하여 불법·부당한 시스템과 자료에 접근이 증대한다.

또한 공동이용의 특징인 데이터의 공유성은 데이터의 처리비용의 감소라는 이점은 있으나 가외성을 줄여 데이터의 질에 대한 위험성을 증대시키는 결과를 가져오게 된다. 일반적으로 가외성은 오류의 발생을 방지함으로써 체제의 신뢰성과 적응성을 높여주는 필요한 장치이다. 이러한 가외성이 없는 시스템은 오류의 발생률이 가장 높은 체계로 이행된다. 가외성은 문제의 불확실성이 높은 상태에서 더욱 필요한 데, 운영환경에 있어서 불확실성이 증대되는 공동이용은 이러한 시스템과 데이터의 가외성을 줄이는 정보관리라고 할 수 있다.

개인정보의 데이터베이스화와 공동이용에 의하여 온라인에 의한 자료의 전송이 일상화되고, 컴퓨터를 통한 신원조회 및 적격심사가 일상화됨으로써 전술한 바와 같이 안성성에 대한 침해사례도 급증하고 있다. 대부분의 매스컴 등에서 관심을 가지고 보도되고 있는 사례들도 주로 안전성과 관련된 개인정보의 유출이 주를 이루고 있다.[222]

2. 개인정보의 이용 및 통제

가. 개인정보 이용

행정정보공동이용의 본래 목적은 이용의 제한이 아니라 이용의 활성화

222) 이에 관한 자세한 설명은 박홍윤, 앞의 책, 84-94면 참조.

를 위한 것이므로 개인정보의 보호를 위한 이용제한의 원칙과는 근본적으로 갈등의 선상에 놓인다. 공동이용시스템이 구축되면 개인정보의 이용률이 확대되고 이용이 확대되면 남용의 문제도 발생하게 된다.

이렇게 공동이용이 확대됨으로써 공동이용시스템 본래의 존재목적 이외로 활용되기도 한다. 또 개인정보를 공동이용하는 과정에서 그 정보들을 표준화시킬 수밖에 없고, 그럴수록 개인의 특성은 무시되고 사회적인 스키마(skimmer)에 의지하는 결정을 하게 된다. 특히 프로파일링에 의해 창출되는 정보는 사실정보가 아닌 판단정보의 특성을 지니기 때문에 주관적인 해석의 가능성이 높다.

개인정보의 공동이용은 전후사정을 무시한, 또는 부분적·불완전한 정보의 사용으로 특정개인에 대한 잘못된 판단을 초래하여 정치·경제·사회적 활동에 치명상을 입히는 경우, 틀린 정보 또는 특정시점에 국한된 정보를 이용하여 특정인을 잘못 인식하도록 만들어서 명예를 실추시키고 신용을 잃게 만드는 경우가 많이 발생할 수 있다.

나. 개인정보 통제

행정정보공동이용을 위해서는 개인자료의 개발, 활용, 정책들을 일반에게 공개해야 한다. 이를 위해서는 개인자료의 존재와 성격 그리고 주요한 이용 목적 및 데이터의 통제자를 명확히 하고 권한과 책임의 소재를 분명히 해야 한다.

일반적으로 관료제는 특히 통제업무와 관련하여 법률에 의하여 또는 법률의 특별 규정이나 예외규정에 의하여 거의 방해를 받지 않는다. 행정정보공동이용에 있어서 정보체계관리에 대한 공개의 문제는 조직 내 정보관리체계의 공개문제와 거의 비슷한 형태의 문제가 나타난다고 할 수 있다.

기존의 개인정보보호를 위한 법률체계들은 개인에게 자신의 정보를 보호하도록 많은 책임을 부여한다. 그러나 조직의 개인정보의 전산화와 통합관리는 개인의 책임과 개인의 조직을 감시하는 능력간에 격차를 증대시킨다. 이러한 불균형은 개인의 자기정보에 대한 관리통제권의 행사를 더욱 어렵게 한다. 개인통제의 전제인 알 권리와 관련하여 개인정보의 조직간 이동의 확대목적 이외 이용 가능성의 확대는 조직에서의 개인정보처리와 이용에 대한 개인의 인지를 더욱 어렵게 한다.[223]

3. 요약 및 분석

앞서 검토한 바와 같이 행정정보공동이용은 전자정부를 구현하는데 필수요건임에 틀림없다. 행정정보공동이용은 정보통신망에 의한 컴퓨터시스템과 네트워크를 활용한 공동이용 방식으로 신속성·정확성 확보, 지리적·시간적 한계의 극복, 종이문서 사용 절약으로 국민은 시간적·경제적 비용 등의 절감으로 높은 만족감을 향유할 수 있게 된다.

또한 행정기관은 전자정부 사업에 필요한 다양한 행정정보 자료를 신속하고 정확히 입수하고 활용할 수 있으므로 조직의 능률성 및 부처간 협조를 통한 부처이기주의를 극복하고, 복잡하게 얽혀있는 다른 부처의 상호조정과 신속한 협조가 이러한 문제들을 쉽게 해결할 수 있어 현대 사회에서는 꼭 필요한 것이라 할 수 있다.

하지만 아무리 필요하고 좋은 제도라고 해도 그것이 정작 국민의 인권을 침해하거나 또 정보주체의 자기정보관리통제권의 실현을 저해한다면 제고해 보아야 할 것이다. 행정정보공동이용을 위해서는 먼저 선행되어야 할 과제가 행정정보의 공개이다. 그리고 행정정보공동이용에 필요한 자료의 수집 및 관리·이용·통제·안전성 확보를 위한 방안이 강구되어야 한다. 그러나 지금까지 검토한 바로는 아예 법률의 근거가 없는 것에서부터 있다고 하여도 매우 추상적이거나 미흡한 경우가 대부분이었다.

「전자정부법」은 제11조에 행정정보공동이용을 위한 원칙을 규정하고 있으며, 제12조에서는 개인정보보호를 위한 규정을 두고 있다. 하지만 구체적으로 정보의 안전성 또는 개인정보보호를 위한 규정은 없다. 개인정보보호를 위해서는 각 개별법의 규정을 준용 또는 응용하고 있다. 그렇다면 현행「전자정부법」을 일반법의 성격으로 분류하고 그에 따르는 기본적이고 일반적인 사항이 제정되어야 마땅하다. 현행「전자정부법」은 앞의 11조 내지는 12조의 성격처럼 추상적인 문구를 두고 있는가 하면 또 제21조 내지 제22조 등에서는 전자행정을 위한 절차에 대하여 규정하고 있다.

「행정절차법」제8조 제1항도 행정청은 다른 행정청에 행정응원을 요청할 수 있다고 하고 있지만 행정정보공동이용에 대한 내용은 없다. 이렇게

223) 박홍윤, 앞의 책, 102-105면.

전자행정을 위한 입법체계가 혼란함으로 인하여 전자행정을 실행하는 공무원도 그 기준점을 어디에 두어야 할지 혼란이 가중될 뿐이다. 전자정부를 운용하기 위해서는 첫째,「전자정부법」을 개정하여 기본법의 입법체계를 세우고, 둘째, 전자행정을 위하여 행정정보공동이용을 위한 특별법을 제정하여 전자행정에 관한 전반적인 사항을 구체적으로 규정하여야 한다. 셋째, 전자행정을 위한 구체적인 절차 및 운용사항에 관하여는 시행령을 따르도록 해야 한다. 그리고 또 개별 법률에 규정되어 있는 개인정보보호 규정은 개인정보보호를 위한 구체적 사항을 적시하여 국민의 기본권인 자기정보관리통제권의 실현을 위한 내용을 보완 내지는 정정하여 규정해야 한다.

따라서 행정정보공동이용을 위한 구제적인 법률이 제정되어야 할 필요가 있다고 생각한다.

정부는 지난 2006년 11월 14일「행정정보고동이용법(안)」을 제17대 국회에 제안하였고, 2007년 2월 21일 소관 상임위원회인 행정자치위원회에 상정되었으나 2008년 5월 29일 결국 임기만료로 폐기되고 말았다. 이 법안이 통과되지 못한 가장 큰 이유는 행정정보공동이용의 핵심쟁점이 그 범위와 한계에 관한 것이었다고 한다. 행정정보공동이용에 있어서 그 절차도 중요하지만 정보의 공동이용을 위한 범위와 한계가 먼저 설정되어야 하는 것이 당연하다. 따라서 그 범위와 한계를 다시 설정하여 법률을 제정하여야 할 것이다.

제4장 전자정부와 자기정보관리통제권

제1절 자기정보관리통제권의 보장범위와 한계

1. 자기정보관리통제권의 등장배경

농업사회를 지나 산업혁명을 가져왔던 기계기술의 발전이 인간의 근육노동을 대상으로 한 것이었다면, 정보혁명의 기술은 인간사회의 커뮤니케이션 기술을 대상으로 하여 만들어진 것으로 볼 수 있다.[224]

정보통신기술이 나날이 발전되어 가면서 다양한 정보가 컴퓨터에 저장·축적될 수 있는 양이나 그것을 인출하기 위한 속도도 비약적으로 향상되어 모든 국민의 데이터를 관리하는 것도 기술적으로 가능하게 되었다. 이러한 시대적 배경을 기초로 원래 혼자 있을 권리라는 소극적인 권리였던 프라이버시 권리는 자기정보 내지 개인정보에 관한 정보의 흐름을 통제하는 권리라는 적극적인 위치를 갖게 되었다. 이러한 상황에서 많은 사람들은 자신에 관한 정보가 자유로이 인출되어 악용될 수 있다고 걱정하게 되었다. 그래서 개인정보의 누설·악용을 방지하기 위하여 프라이버시권은 보다 넓은 의미로 확대될 것이 요구되었다. 이 확대된 권리는 자신과 관계된 정보의 흐름을 통제하는 권리(individual right to control the circulation of information relating to oneself)로 정의되고,[225] 이것이 바로 자기정보관리통제권, 개인정보자기지배권, 개인정보관리권, 개인정보자기통제권, 개인정보자기결정권 등으로 불리게 되었다.

이러한 현대의 정보통신기술의 발달, 특히 컴퓨터를 통한 개인정보의 데이터베이스화가 진행되면서 개인정보의 처리와 이용이 시공에 구애됨이 없이 간편하고 신속하게 이루어질 수 있게 되었고, 정보처리의 자동화와 정보파일의 결합을 통하여 여러 기관과의 정보교환이 용이해짐에 따라 한 기관이 보유하고 있는 개인정보를 다른 기관이 동시에 활용하는 것이 가능하게 되었다. 따라서 개인의 인적 사항이나 생활상의 각종 정보가 정보

224) 고영삼, 전자감시사회와 프라이버시, 한울 아카데미, 1998, 39면.
225) 백윤철, "헌법상 자기결정권과 개인정보자기결정권", 헌법학연구 제9권 제3호, 한국헌법학회, 2003, 228면.

주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격하게 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다.[226] 나아가 컴퓨터에 의한 관리는 합리성·효율성이 있는 반면, 정보의 누설이나 다른 목적에 쉽게 이용될 수 있다는 문제가 있음으로, 적절한 관리와 보호가 필요하다.[227] 더구나 현대사회는 정보통신기술의 발달로 인하여 앞다투어 전자정부를 구축하고 개인정보를 기관상호간 공동이용함으로써 많은 문제들이 발생함은 물론이고, 그 중에서도 특히 자기정보관리통제권에 관한 문제는 상당한 논란을 불러일으키고 있다.[228]

이러한 사회적 배경에서 개인이 각자의 정보를 보호하기 위한 권리를 헌법상 기본권으로 승인하는 것은 현대 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로 개인의 결정의 자유를 보호하고 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단할 수 있는 법적·제도적 장치를 강구하게 되었고, 이것이 바로 자기정보관리통제권을 헌법상의 기본권으로 인정하는 이유가 된 것이다.[229]

그런데 이러한 자기정보관리통제권의 헌법적 근거와 관련하여 다양한 학설이 주장되고 있고, 헌법재판소 역시 견해를 변경하는 등 혼란을 보이고 있다. 자기정보관리통제권의 헌법적 근거에 관한 문제는 곧 개인정보자기결정권의 성격과 연관되므로 중요한 논의의 대상이 될 수 있다.

가. 용어의 정립

자기정보관리통제권을 고찰함에 있어서 용어의 정립이 먼저 선행되어야 한다. 정보보호와 관련하여 개인정보에 관한 자기결정권이라는 용어는 독일이나 일본처럼 사생활의 보호에 관한 헌법적 근거를 인간의 존엄 또는 행복추구권에서 찾는 나라에서 주로 사용되고 있다.[230]

---

226) 헌법재판소, 2005. 5. 26. 99헌마513 등, 판례집 17-1, 682면.
227) 백윤철, 앞의 주 222), 221면.
228) 헌법재판소, 2005. 5. 26. 99헌마513 등, 판례집 17-1, 682면.
229) 이상명, “개인정보자기결정권의 헌법적 근거에 관한 고찰”, 공법연구 제36집 제3호, 한국공법학회, 2008, 225면.
230) 권건보, 앞의 책, 92면.

그리고 개인정보보호 내지 자기정보통제라는 용어는 개인정보관리자나 개인정보처리자 등의 입장 내지 개인정보를 둘러싼 법질서를 설계하고 적용・집행하는 측의 관점을 반영한 것이라 할 수 있다.[231]

현재 국내에서 개인정보의 보호와 관련하여 사용하는 용어는 자기정보관리통제권,[232] 자기정보에 대한 통제권,[233] 자기에게 관련된 정보의 전파를 컨트롤할 수 있는 권리,[234] 정보자결권,[235] 개인정보자기결정권,[236] 자기정보통제권,[237] 개인정보통제권,[238] 개인정보자기통제권,[239] 정보상자기결정권,[240] 개인정보결정권[241] 등 다양하게 사용되고 있다. 이러한 용어들은 대체로 컴퓨터통신망에서 자신에 관한 개인정보의 운용을 스스로 관리・통제할 수 있는 정보 프라이버시권을 의미한다.

자기정보관리통제권은 자신에 관한 정보에 있어서 자율적으로 통제 내지 관리할 수 있는 권리를 의미하는 것으로 볼 수 있다. 구체적으로 보면 정보주체가 정보시스템 안에 보관되어 있는 자기의 개인정보에 접근하여 그 정보를 열람하고, 정보처리기관에 대하여 자신에 대한 정보의 정정, 차단, 삭제, 공개 등을 요구함으로써 자신에 관한 정보의 관리・통제력을 행사할 수 있는 권리라고 할 수 있다.

한편 정보자기결정권이란 자신에 관한 정보에 있어서 스스로 결정할 수 있는 권리를 의미한다. 즉 개인정보의 주체가 자신의 식별 데이터를 외부에의 개시 여부와 공개범위를 결정할 수 있는 정태적인 권리로서,[242] 개

231) 위의 책, 87면.
232) 권영성, 헌법학원론, 법문사, 2009, 454면.
233) 성낙인, 헌법학, 법문사, 2009, 582면.
234) 김철수, 헌법학신론, 박영사, 2005, 420면.
235) 허영, 한국헌법론, 박영사, 2005, 383면; 정태호, “개인정보자결권의 헌법적 근거 및 구조에 대한 고찰 -동시에 교육행정정보시스템(NEIS)의 위헌여부의 판단에의 그 응용 -”, 헌법논총 제14집, 헌법재판소, 2003, 202-203면.
236) 강경근, 헌법, 법문사, 2004, 701면; 김일환, 주민등록번호의 위헌성여부에 관한 고찰, 87면 이하; 김승환, “정보자기결정권”, 헌법학연구 제9권 제3호, 한국헌법학회, 2003, 149면 등.
237) 강경근, 앞의 책, 701면; 김일환, 논문, 87면; 김승환, 앞의 논문, 149면 등.
238) 김용섭, “정보공개와 개인정보보호의 충돌과 조화”, 공법연구 제29집 제3호, 한국공법학회, 2001, 5, 181면; 김종철, 헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론, 23면 등.
239) 성낙인 외, 개인정보보호를 위한 정책방안 연구, 정보통신부, 1999, 23면.
240) 박윤흔, 최신행정법강의(상), 박영사, 2002, 540면 이하; 홍정선, 행정법원론(상), 박영사, 2001, 28면 등.
241) 백윤철, 앞의 주 222), 209면.
242) 정영화, 앞의 주 239), 13면.

인이나 단체가 자신에 관한 정보를 타인에게 알릴 것인지 말 것인지, 알린다면 언제, 어떻게, 어느 정도 전달할 것인가에 관하여 스스로 결정할 수 있는 권리이다. 이러한 개념은 자신에 관한 사항이 자신의 의사와 무관하게 타인에 의하여 결정될 경우 정보주체의 인격적 가치가 형해화될 위험[243]이 있다. 이러한 점에서 전자정부 구축에 따른 개인정보공동이용에 있어서도 정보주체의 사실과 다른 정보로 인하여 개인의 명예, 재산, 신용 등에 돌이킬 수 없는 문제를 야기할 수 있다는 문제의식에서 출발한 것이라 할 수 있다. 결국 개인정보가 전자행정을 위해 구축되었다하더라도 정보주체는 자기정보관리통제권을 보장하기 위하여 개인이 자신에 관한 정보를 스스로 관리 또는 통제할 수 있어야 한다.

나. 양자 구별의 실익에 관한 논의

학계에서 혼용되고 있는 정보자기결정권과 자기정보관리통제권을 구별할 실익이 있는가?

전술한 바와 같이 정보자기결정권은 헌법상 인격권에 근거한 권리로서, 개인정보의 주체가 자신의 식별 데이터를 외부에의 게시 여부와 공개범위를 결정할 정태적인 권리라고 한다면, 자기정보관리통제권은 정보주체의 개인정보를 외부에 적법하게 제공·이용·보유하는 제3자에게 자신의 데이터를 열람·정정·이용중지 및 삭제 등을 청구함으로써 자신의 개인정보를 관리 및 통제할 수 있는 적극적 권리이다.[244] 그런데 정보자기결정권이 개인정보의 비밀을 반드시 요하지 않는다는 점에서 사생활의 비밀을 요소로 하는 정보 프라이버시권과 구별해야 한다는 견해가 있는데, 정보자기결정권은 비밀성 이외에도 공유성을 본질적인 특징으로 하는 점에서 사생활의 비밀을 요소로 하는 프라이버시권과 구별이 된다[245]고 한다.

그리고 자기정보관리통제권은 소극적인 자유권으로서의 성격뿐만 아니라 적극적인 청구권으로서의 성격을 아울러 가지고 있지만, 정보자기결정권은 소극적 자유권과 부분적 정보접근에 머물고 있는 권리이다. 이는 일

243) 권건보, 앞의 책, 89면.
244) 정영화, 앞의 주 239), 14면.
245) 정준현, “민간 온라인 개인정보보호법제에 대한 검토”, 공법연구 제29집 제3호, 한국공법학회, 2001, 153면.

반적 인격권은 단지 공개된 영역에서 자신의 본래 모습이 훼손되거나 잘못되지 않도록 할 접근권을 갖는데 불과하며, 적극적으로 다른 사람의 정보처리과정을 통제할 수 있는 권리는 아니다. 나아가 정보자기결정권은 '홀로 있을 권리'와 '개인정보통제권'의 중간에 있는 어떤 것을 의미한다. 따라서 정보자기결정권에는 개인정보통제권, 개인정보공개청구권, 개인정보열람청구권, 정정 및 삭제청구권 등이 포함된다[246]고 할 수 있다.

한편, 자기정보관리통제권이 정보프라이버시의 관점에서 주창된 것이라 할지라도 그것은 비밀의 이익을 보호하기 위한 것으로 단정하는 것은 곤란하다. 하지만 타인의 간섭배제나 비밀의 유지라는 프라이버시의 소극적 측면에서 벗어나 자신에 관한 정보의 흐름을 통제할 수 있는 가능성에 주목하여 프라이버시를 이해하려는 시도가 정보 프라이버시로 나타났던 점을 상기할 필요가 있다.[247]

또한 개인이 공개 여부를 선택하는 자신의 정보는 자신의 인격이나 정체성에 영향을 미친다고 할 수 있으며, 강제적인 공개의 위협은 독립적인 행동에 관여할 자신의 자유에 상당한 제약을 가하게 된다. 이러한 점에 비추어 보면 자기정보관리통제권과 정보자기결정권은 상당 부분 중첩된다고 할 수 있다.[248] 권영성 교수도 자기정보관리통제권에 대하여 넓은 의미에서 자기정보관리통제권이라 함은 자신에 관한 정보를 보호받기 위하여 자신에 관한 정보를 자율적으로 결정하고 관리할 수 있는 권리라고 하며, 이에 대하여 좁은 의미의 자기정보관리통제권이란 자신에 관한 정보의 열람·정정·사용·중지·삭제 등을 청구[249]할 수 있는 권리를 말한다.

결국 이러한 논리에서 본다면 정보자기결정권이나 자기정보관리통제권은 엄격히 구별해야 할 실익은 없다고 할 것이다. 따라서 이하에서는 자기정보관리통제권이란 용어를 주로 사용하기로 한다.

---

246) 김용섭, 앞의 주 235), 181-182면.
247) 권건보, 앞의 책, 90면 이하 참조.
248) Fred H. Cate, supra note 170), pp.19-20.
249) 권영성, 앞의 주 229), 452-453면.

2. 자기정보관리통제권의 의의 및 법적 성격

가. 자기정보관리통제권의 의의

자기정보관리통제권 역시 전술한 개인정보의 보호에서 논한 바와 같이 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 관리·통제하고 결정할 수 있는 권리이다.[250] 헌법재판소도 "자기정보관리통제권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말하는바, 개인의 고유성, 동일성을 나타내는 지문은 그 정보주체를 타인으로부터 식별가능하게 하는 개인정보"라고 하였다. 즉, 자기정보관리통제권은 개인이 자신에 관한 정보의 흐름을 파악하여 관리·통제할 수 있는 권리'로 간단히 정의할 수 있다. 이는 자신에 관한 정보의 생성, 유통, 소멸 등에 주도적으로 관여할 법적 지위를 보장하는 것이라고 할 수 있다.[251] 또한 넓은 의미에서의 자기정보관리통제권은 자신에 관한 정보를 보호받기 위하여 자신에 관한 정보를 자율적으로 결정하고 관리할 수 있는 권리를 말한다. 이러한 의미에서 자기정보관리통제권은 자신에 관한 정보를 함부로 침해당하지 아니할 권리와 협의에서 자신에 관한 정보의 열람·정정·사용·중지·삭제 등을 요구할 수 있는 권리이다.[252]

또한 자기정보관리통제권은 소극적 측면뿐만 아니라 적극적 측면도 아울러 가진다. 개인정보의 수집·축적·보관·제공 등을 거부하는 것 또는 본인의 의사에 반하거나 잘못된 개인정보의 보유나 처리에 대하여 정정이나 폐기 또는 손해배상을 청구하는 것은 자기정보관리통제권의 소극적 측면이라 할 수 있다. 반면에 자신에 관한 정보의 보유상황을 확인하기 위하여 자료의 열람이나 조사를 청구하거나 혹은 원하는 대상에게 그 정보를 스스로 공개하거나 제공하는 것은 자기정보관리통제권의 적극적 측면이라 할 수 있다.[253]

---

250) 성낙인, 앞의 책, 582면.
251) 권건보, 앞의 책, 94면.
252) 권영성, 앞의 책, 452면.
253) 권건보, 앞의 책, 94면.

자기정보관리통제권은 컴퓨터통신망을 인프라로 하는 사이버 공간에서 개인정보를 보호하는 사생활의 자유권이라고 할 수 있다. 또한 전자정보 이동의 대량성, 고속처리, 신속한 전파성, 정보의 집중과 결합, 검색의 용이성, 원격처리 등 전산처리과정의 몰개인성이 높아지면 높아질수록 개인정보의 침해가능성은 높아지고 있는데, 자기정보관리통제권은 이러한 침해를 배제하거나 사후에 구제할 수 있는 기본권이다.[254]

궁극적으로 자기정보관리통제권은 개인의 의사소통능력을 보장함을 목적으로 한다. 의사소통은 모든 사회에 있어서 필수적인 것이며, 상호간의 의사소통은 민주사회에 있어서 더욱 필수적인 것이다. 따라서 상호간의 의사소통을 확실히 하여야 하는데 특히, 공동체에 한정되는 경제적·사회적·문화적·정치적 활동영역에서 개인은 특별한 의사소통을 가져야 한다. 이러한 자기결정권은 그 시민들의 행동과 협력 능력에 바탕을 두고 있는 자유민주적 공동체의 기본적인 기능조건이다.[255] 따라서 국가가 개인에 관한 어떤 정보를 조사·처리해도 되는지를 결정·통제할 수 있는 권리를 개인에게 부여하는 것이 반드시 필요하다.

그러나 자기정보관리통제권이 단지 사적인 개인의 복리를 촉진하는 것을 보장하여야 하는 것은 아니다. 오히려 그것은 "그 시민의 행위 가능성과 협력 가능성에 기초하는 자유민주적 공동체의 기초적 기능조건도 된다. 그러나 여기에서 말하는 공동체는 법인이나 단체를 포함하는 것은 아니다. 설령 단체 고유의 인격적 가치가 존재한다고 하더라도 그것은 그 구성원의 자기정보관리통제권을 통하여 간접적으로 보호될 수 있다. 따라서 단체는 원칙적으로 자기정보관리통제권의 주체가 될 수 없다"[256]고 할 수 있다.

또한 국가가 국민의 기대에 부응하여 복리증진이라는 국가적 과제를 합리적이고 효과적으로 수행하기 위해서는 국가에 의한 개인정보의 수집·처리의 필요성이 증대되므로 여기에는 정보기술의 뒷받침이 필연적이라고 할 수 있지만, 한편으로 현대의 정보통신기술의 발달은 그 그림자도 짙게 드리우고 있다. 즉, 오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로

254) 강경근, 앞의 주 233), 701면.
255) 권건보, 앞의 책, 95면.
256) 강경근, 앞의 책, 701면; 권건보, 앞의 책, 96-97면 등.

집적되고 이용되고 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 개인에 대한 국가의 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다. 이와 같이 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단할 수 있는 제도적 장치가 필요[257]하다고 생각한다. 여기서 자기정보에 대한 관리·통제권이라는 권리가 인식되어야 할 필요가 있게 된다.

나. 자기정보관리통제권의 법적 성격

자기정보관리통제권권의 법적 성격에 관하여, 이를 인격권적 성격으로 보는 것이 다수설의 입장이다.[258] 인격권적 성격은 대체로 헌법 제10조에서 도출해내고 있다. 그런대 제17조의 사생활의 비밀과 자유가 공권력 또는 제3자에 대한 소극적·방어적 성격이라면, 자기정보관리통제권은 청구권적 성격이 강한 능동적·적극적 권리이다. 또한 자기정보관리통제권은 일신전속 권리이다. 그리고 자기정보관리통제권 중에서 자기정보열람청구권은 알 권리로서의 성격도 가지고 있기 때문에 정보공개청구권과 중복되는 측면도 있다.[259]

현대사회의 특성과 현실을 감안하면 자기정보관리통제권은 재산권적 성격[260]도 아울러 가진다고 볼 수 있을 것이다. 어차피 자기정보관리통제권

257) 성낙인, 앞의 책, 582면; 권건보, 앞의 책, 94면 이하 등.

258) 권영성, 앞의 책, 454면; 성낙인, 앞의 책, 577면; 정준현, 앞의 주 110), 720면; 백윤철, 앞의 주 222), 230면; 권형준, "자기정보통제권에 관한 고찰", 헌법학연구 제10권 제2호, 한국헌법학회, 2004, 100면; 정영화, 앞의 주 103), 15면; 권헌영, "개인정보권의 헌법적 수용 - 헌법재판소의 결정 분석을 중심으로-", 토지공법연구 제35집, 2007, 326면 등.

259) 권영성, 앞의 책, 454면.

260) "현대의 개인정보는 다양한 속성을 가지고 있고, 그 이용환경이나 태양에 따라 프라이버시권의 대상이 될 수도 있고, 아닐 수도 있다. 누군가 내 이름을 안다고 하여 그것이 개인정보권을 침해하는 것이라고 할 수는 없다. 친구로부터 다른 친구에 대한 정보를 얻는 경우에도 동의가 없으면 불법이 되어야 하는지도 권리로서의 개인정보에 대한 검토대상이다. 또한 재산적 가치를 고려한다면 이를 인격권만으로 볼 수도 없을 것이다. 대체로 현행 헌법을 해석하면서 그 근거를 찾는 데에 있어서는 개인정보권을 헌법에 명시되지 아니한 기본권으로 이해하는 견해를 일관되게 유지하는 것이 좋을 수도 있다. 특히, 개인정보의 재산권적 성격을 인정할 필요가 있는 입장에서는 이러한 견해가 보다 유연하게 개인정보권을 객관화 하는데 도움이 될 수 있을 것으로 생각한다"고 한다. 권헌영, 앞의 주 255), 328면.
재산권적 성격에 대해서 위의 견해에 동의할 수 있다. 오늘날 개인정보는 공공부문에서는 단

자체가 프라이버시권의 확장 개념이고, 프라이버시권은 불법행위에 기한 재산적 손해배상에 기초하여 이루어진 권리이기 때문에 재산권적 성격도 가진다고 할 수 있다.[261] 예컨대, 금융기관에서 유통 또는 활용되는 신용정보는 비록 개인정보라 하더라도 고급 금융정보로서 재산적 가치를 가진다. 만약 금융기관에서 보유하고 있는 개인정보가 유출이 된다면, 개인으로는 재산적으로 큰 타격을 입을 수 있고, 그 구제 또한 용이하지가 않다.

한편, 자기정보의 열람청구는 정정청구 등과 달리 피해의 구제로서의 의미보다는 예방청구의 성격이 강하다. 여기서 말하는 예방적 청구는 침해의 가능성이 현저한 경우뿐만이 아니라, 개인정보가 적법하게 처리되고 있는지 확인하려는 경우에도 허용된다.

다. 자기정보관리통제권의 법적 근거

1) 헌법적 근거

자기정보관리통제권에 관한 법적 근거는 일반적으로 헌법에서 찾는 경우가 대부분인데, 이것은 국가에 따라 다소의 차이가 있다. 미국에서는 자기정보관리통제권을 프라이버시의 문제로 보고 논의하고 있고, 독일에서는 일반적 인격권의 문제로 보고 있으며, 일본에서는 행복추구권을 보장하고 있는 일본헌법 제13조에서 그 근거를 찾고 있다. 우리나라의 경우 자기정보관리통제권에 관하여 헌법상 명문규정이 없다. 학설과 판례는 내용상 약간의 차이를 보이고 있으나 자기정보관리통제권의 헌법적 근거를 헌법 제10조의 인간의 존엄과 가치 및 행복추구권에서 찾는 견해, 헌법 제17조 사생활의 비밀과 자유에서 찾는 견해, 이 둘을 종합적으로 해석하여 실정법적 근거를 찾는 견해 등이 있다.

(1) 외국의 경우

가) 미국

미국에서는 1960년대 말부터 컴퓨터의 대량보급에 힘입어 정보사회가

순한 인격권의 침해로 볼 수도 있겠지만, 민간부문에서는 특히, 기업체 등에서는 개인정보의 보유 내지 활용은 상당한 상업적 가치를 낳고 있으며, 그로 인한 개인정보침해 건수가 날로 증가하고 있다.

261) 권건보, 앞의 책, 97면.

진전되면서 개인정보에 대한 침해가능성이 증대되자, 개인정보보호의 필요성이 부각되었다. 이에 관한 프라이버시를 정보 프라이버시(information privacy) 또는 데이터 프라이버시(data privacy)라 하는데, 이는 개인정보의 수집·이용·제공 등에 대한 개인의 통제를 의미하는 것이다.[262]

미국 연방대법원이 정보 프라이버시권을 최초로 인정한 것은 투약 목록을 행정기관에 보관하도록 규정한 뉴욕주법의 위헌성을 심사한 1977년 월런(Whalen)판결[263]이었다. 이 판결에서 연방대법원은 헌법상 프라이버시권은 사적인 일을 분별없이 공개할 수 없다는 개인의 법익을 보호하는 정보통제권으로서의 권리성과 사적인 일에 대한 간섭을 받지 않는다고 하는 개인의 법익을 보호하는 자율권으로서의 권리성을 가진다고 명시하고, 이 두 가지의 측면을 가진 권리가 프라이버시의 권리라고 하였다.[264] 즉, 그 하나는 개인적인 사안의 공개를 회피하는 개인적인 이익이고, 다른 하나는 독립하여 어떤 종류의 중요한 결정을 행하는 이익이라고 지적하였다. 그리고 연방대법원은 수정헌법 제14조의 적법절차와 자유보장 등에 근거하여 정부로부터 개인정보의 공개가 강요당하지 않을 헌법상 권리를 인정하였다.

1980년 워렌(S. D. Warren)과 브렌다이스(L. D. Brandeis)가 발표한 논문에 의하여 주창된 프라이버시권은 1928년의 옴스테드(Olmstead)판결[265]에서 부당한 수색·압수로부터의 자유를 보장하고 있는 수정헌법 제4조와 관련하여 헌법문제로서 최초로 다루어졌다. 이 판결에서 브렌다이스 대법관은 비록 소수의견이기는 하지만 프라이버시권이 헌법상의 권리로서 '홀로 남겨져 있을 권리, 즉 권리 중에서 가장 포괄적이고 문명인에 의하여 매우 가치 있다고 평가되는 권리'라고 하였다. 마침내 1965년에 이르러 연방대법원은 그리스월드(Griswold) 판결[266]에서 명시적으로 프라이버시권을 헌법상 보호되는 기본권의 하나로 인정하였으며, 이후 이 두 판결을 축으로 하는 1980년대의 일련의 판결[267]에 의하여 실체적 적법절차를 보

262) 황인호, "개인정보보호제도에서의 규제에 관한 연구", 박사학위논문, 건국대학교 대학원, 2001, 38-39면.
263) Whalen v. Roe. 429 U. S. 589 (1977).
264) Fred H. Cate, supra note 170), p.62.
265) Olmstead v. United States, 277 U. S. 438 (1928).
266) Griswold v. Connecticut, 381 U. S. 479 (1965).
267) Loving v. Virginia, 338 U. S. 1 (1967); Eisenstadt v. Baird, 405 U. S. 438 (1972); Moore v. East Cleveland, 431 U. S. 494 (1977); Zablocki v. Redhail, 434 U. S. 374

장하고 있는 수정헌법 제14조의 생명·자유의 개념에는 사생활의 비밀과 자유에 관한 권리가 포함되어 있다고 천명하기에 이르렀다.

오늘날 정보사회의 진전으로 공권력이나 일반기업에 의한 개인정보의 남용우려가 증대된 소위 데이터 뱅크(data bank) 사회가 출현하자 종래의 사사(私事)의 공개나 사생활의 침해로부터 보호라는 소극적 관념으로 구성된 전통적 프라이버시권의 개념을 새로운 상황에 대응하게 재구성하여 적극적 성격을 지닌 자기정보에 대한 통제권으로 파악하려고 하는 견해가 유력해지고 있다. 웨스틴(Alan Westin) 교수는 이미 1967년에 "프라이버시권은 자기에 관한 정보를 언제, 어떻게, 어느 정도까지 타인에게 전달할 것인가를 스스로 결정하는 개인, 집단 혹은 조직의 권리"라고 주장하였고,[268] 많은 학자들은 정보사회의 특성을 고려하여 프라이버시권의 개념을 넓게 파악하여 개인의 자기정보관리통제권을 이에 포함시키고 있다.[269] 다만, 연방대법원은 닉슨(Nixon)사건[270]에서 개인정보문제를 다루면서 개인의 프라이버시권에 대한 요구는 추상적으로 검토될 수 있는 것이 아니라 구체적인 법규정과 관련하여 검토되어야 한다고 판시하였다.[271] 그러나 헌법적 차원에서 개인의 자기정보관리통제권을 인정하고 있는 판례는 아직 보이지 않고 있다.

나) 독일

독일기본법에서는 명문으로 프라이버시권을 인정하고 있지는 않지만, 학설과 판례는 "모든 사람은 타인의 권리를 침해하지 않고 헌법적 질서 또는 도덕률에 위반하지 않는 한 자기의 인격을 자유로이 발현시킬 권리를 가진다"고 규정하고 있는 독일기본법 제2조 제1항을 중심으로 하여 "인간의 존엄성은 불가침이다"라고 선언하고 있는 기본법 제1조 제1항을

(1978); Parham v. JR, 442 U. S. 584 (1979); Thomburgh v. Amencan College of Obstetricians and Gynecologists, 476 U. S. 747 (1986) 등.

268) Alan F. Westin, Privacy and Freedom, New York: Atheneum, (1967), p.7.

269) Charles Fried, Privacy, 77 Yale L. J. 475 (1968), pp.482-483; Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossier, Ann Arber: The University of Michigan Press, (1971), p.226; Thomas Huff, Thinking Clearly About Privacy, 55 Washington Law Review, 777(1980), p. 782; W. M. Beaney, The Right to Privacy and American Law, Law and Contemporary Problems, Duke University, (1966), p. 254.

270) Nixon v. Administrator of General Services, 433 U. S. 458 (1977).

271) 김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 공법연구 제29집 제3호, 한국공법학회, 2001, 93면.

결부시켜 자기정보관리통제권의 헌법적 근거를 찾고 있다.[272]

독일기본법 제정 초기에는 제2조 제1항의 권리성을 부인하는 입장도 없지 않았으나,[273] 다수설은 권리성을 인정해 오고 있고,[274] 연방헌법재판소도 이를 인정하였다. 1954년 연방헌법재판소는 기본법 제2조 제1항에 근거를 두고 투자조성(Investitionshilfe) 판결[275]을 내렸고, 1957년 Elefes 판결[276]에서는 기본법 제2조 제1항이 일반적 행동의 자유를 보장하고 있다는 획기적인 판결을 내렸다. 연방헌법재판소는 그 이후 일관되게 이 입장을 견지하면서 일반적 행동의 자유에 의하여 보호되는 행위로서 포괄적인 자유 이외에 외국여행의 자유, 집회의 자유, 경제활동의 자유 등과 같은 특정의 독립된 자유를 도출하는 입장을 취하고 있다.

그리고 1964년 일기(Tagebuch) 판결[277]에서 피고인이 자기의 일기와 편지의 내용에 의거한 유죄판결이 기본법 제1조 제1항과 제2조 제1항에 위반된다고 주장하면서 헌법소송을 제기하였고, 연방헌법재판소는 "일기와 편지의 이용이 당사자의 내밀영역(Intimsphare)과 인격의 자유로운 발현권의 보호와의 관계에서 허용될 것인가 아닌가에 대하여 다시금 해명되지 않으면 안 된다"고 판시하였다. 이 판결 이후 연방헌법재판소는 기본법 제2조 제1항과 제1조 제1항에 의거하여 일반적 행동의 자유와는 약간 다른 권리인 일반적 인격권 및 이로부터 파생하는 정보에 관한 자기결정권, 자기의 출생에 관하여 알 권리 등을 도출해 오고 있는데, 여기서 일반적 인격권은 프라이버시권 관념과 유사하여 널리 개인의 사적 사안에 대한 간섭을 배제하고 그 존중을 구하는 권리를 말한다.

---

272) 이상명, 앞의 주 226), 235면.

273) D. Haas, Freie Entfaltung der Personlichkeit, DÖV, 1954, S. 70ff; F. Klein in v Mangoldt/Klein, Das Bonner Grundgesetz, 2. Aufl., (1955), S. 160ff.

274) 기본법 제2조 제1항의 권리성을 인정하는 입장은 다시 어떠한 행위를 보장대상으로 하고 있는가에 관하여 학설이 두 가지로 나뉘고 있다. 하나는 기본법 제2조 제1항의 기본권을 개인의 일반적 행동의 자유라고 하여 모든 생활영역에서의 행동의 자유의 포괄적 보장이라고 파악하는 다수설의 입장이고(G. Hurig, Die Menschenauffassung des Grundgesetzes, JR 1952, S. 259ff; Hamann, Die Freiheit der Personlichkeitsentfaltung im wirtschaftlichen Bereich, BB (1955), S. 105ff, H. Krüger, Neues zur Freiheit der Personlichkeitsentfaltung und deren Schranken, NJW (1955), S. 201ff), 다른 하나는 인격적인 것의 핵심영역이라는 고차적인 레벨을 보장하고 있다는 인격핵심설(H. Peters, Freis Entfaltung der Personlichkeit, in Festschrift für Laun, (1953), S. 673ff)이다.

275) BVerfGE 4, 7.

276) BVerfGE 6, 32.

277) BVerfGE 18, 146.

한편 1971년 슈타인 뮐러(Wilhelm Steinmüller)가 처음으로 '정보자기결정권'이란 용어를 사용하였는데, 이는 '개인에 관한 어떠한 개인정보를 그리고 어떠한 상황에서 누구에게 전달할 것인가에 관한 개인의 자기결정권'으로 이해하였다.[278]

또한 1983년의 인구통계조사판결[279]에서는 "기본법 제1조 제1항의 인간의 존엄은 기본법의 가치질서에 있어서 최고의 가치이고, 기본법 제2조 제1항 및 제1조 제1항은 공권력의 개입으로부터 면제된 사적인 생활형성의 불가침영역을 시민에게 보장하고 있다"고 판시하여 자기정보관리통제권의 헌법적 근거를 기본법 제2조 제1항 및 제1조 제1항에서 구하고 있다.

다) 일본

일본헌법도 프라이버시권에 관한 명문의 규정을 두고 있지 않아 헌법상의 근거가 무엇인가가 문제가 되지만, 일반적으로 "모든 국민은 개인으로 존중된다. 생명, 자유 및 행복추구에 대한 국민의 권리에 대하여는 공공의 복지에 반하지 않는 한 입법 그 밖의 국정에 있어서 최대의 존중을 필요로 한다"고 규정하고 있는 일본헌법 제13조를 근거로 프라이버시권을 인정하고 있다. 학설상으로는 오늘날의 정보사회에 있어서 종래 소극적인 자유권으로서의 프라이버시권을 적극적인 '자기에 관한 정보를 컨트롤 할 수 있는 권리(정보 프라이버시권)'로 파악하여야 한다는 주장이 유력하다.

일본에서 프라이버시권을 둘러싼 최초의 사건은 1964년 동경지방법원의 만찬 후(宴のあと) 사건[280]이다. 이 사건에서 법원은 프라이버시권이라 함은 사생활이 함부로 공개되지 않을 법적 보장 내지 권리라고 정의하였다. 그리고 이 사법상의 권리(인격권)는 개인의 존엄을 유지하여 행복의 추구를 보장함에 있어서 필요불가결한 것이며, 그것이 헌법에 기초한 권리라고 인정하였다. 이러한 취지는 그 후의 명예권과 프라이버시권에 관한 재

278) Wilhelm Steinmüller, Grundfragen des Datenschutzes: Gutachten im Auftrag des Bundesministeriums des Innern, Deutscher Bundestag -6.Wahlperiode- Drucksache 6/3826 Anlage 1, Juli (1971).

279) BVerfGE 27.1

280) 東京地判 昭和 39.9.28. 民集 15卷7號 237頁. 이 사건은 전임 외상(外相)인 원고 有田八郎이 三島紀夫의 소설 《만찬 후(宴のあと)》가 자신을 모델로 하고 있어 자신의 프라이버시가 침해되었다며, 1961년 三島由紀夫와 출판사 新朝社를 피고로 동경지방법원에 위자료와 사죄광고를 청구한 민사소송사건이다.

판에서도 계속 나타나고 있다.

이와 같이 사법상의 권리로서 인정된 인격권의 하나로서의 프라이버시권은 최고재판소의 판결[281]에 의하여 헌법상의 권리로서 확립되었고, 오늘날 일본의 판례 및 통설은 일본헌법 제13조를 근거로 하여 헌법적 권리로서 프라이버시권을 인정하고 있다.[282]

자기정보관리통제권에 대하여 사토 고지(佐藤幸治) 교수가 자신에 관한 정보를 통제할 권리라고 처음으로 주장하였는데, 이는 단순히 타인이 자신에 관한 정보를 가지는 상태를 말하는 것이 아니라, 타인이 자신에 관한 정보를 가질 수 있고, 어떠한 정보를 가지면 안 되는지에 대하여 통제할 수 있는 권리를 의미한다[283]고 하며, 이는 정보사회에서 프라이버시의 보장을 주된 목적으로 한 권리 개념으로 현재 통설로 인정되고 있다.[284]

과거에는 일본에서 프라이버시권이 개인의 사적 영역에 제3자가 무단으로 개입하여서는 아니된다는 자유권적 소극적인 권리로 이해되어 왔지만, 오늘날 일본에서 정보사회가 진전함에 따라 프라이버시권은 적극적으로 자기에 관한 정보를 컨트롤하는 권리(정보 프라이버시권)로 파악하여 자유권적 측면뿐만이 아니라 프라이버시권의 보호를 공권력에 대하여 적극적으로 청구하는 측면을 강조하는 입장이 유력하게 제기되고 있다.[285] 이는 개인정보가 행정기관에 의하여 집중적으로 관리되고 있는 현대사회에 있어서 개인이 자기에 관한 정보를 스스로 컨트롤 하고 자기의 정보에 대하여 열람, 정정 또는 말소를 청구하는 것이 필요하다고 생각하게 된 것에 기초를 두고 있는 것이다.[286]

라) 분석 및 요약

미국의 경우 헌법상 개인정보에 관한 명문의 규정이 없기 때문에 그 법적 근거는 판례를 통하여 인정해 오고 있다. 오늘날과 같이 개인정보를

---

281) 京都府學連事件, 最大判 昭和 44. 12 24, 刑集 23卷12號 1625面; 前科照會事件, 昭和 56. 4. 14, 民集 35卷3號, 620頁.

282) 芦部信喜, 廣義のプライバシー權(2)-包括的基本權(1), 法學教室 127號, 1991 57面; 芦部信喜, 廣義のプライバシー權(2)-包括的基本權(4), 法學教室 131號, 1991, 76-77頁; 佐藤幸治, 日本國憲法と「自己決定權」-その根據と性質をめぐつて, 法學教室 98號, 1988, 6頁.

283) 佐藤幸治, 前揭書, 6頁.

284) 岡村久道新保史生, 電子ネットワーク個人情報保護, 經濟産業調査會, 2002, 72頁.

285) 芦部信喜, 前揭書, 118頁; 佐藤幸治, 前揭書, 316頁.

286) 권형준, 앞의 주 255), 91-96면; 이상명, 앞의 주 226), 234-238면.

헌법상 근거로 인정하기까지는 많은 시간이 흐르는 동안 점차로 확립된 것이다.

오늘날 정보사회의 진전으로 공권력이나 일반기업에 의한 개인정보의 남용우려가 증대되는 소위 데이터 뱅크(data bank) 사회가 출현하자 종래의 私事의 공개나 사생활의 침해로부터 보호라는 소극적 관념으로 구성된 전통적 프라이버시권의 개념을 새로운 상황에 대응하게 재구성하여 적극적 성격을 지닌 자기정보에 대한 통제권으로 파악하려는 견해가 유력해지고 있다.

독일기본법 제정 초기에는 제2조 제1항의 권리성을 부인하는 입장도 없지 않았으나, 다수설은 권리성을 인정해 오고 있고, 연방헌법재판소도 이를 인정하였다.

일본헌법도 프라이버시권에 관한 명문의 규정을 두고 있지 않아 헌법상의 근거가 무엇인가가 문제가 되지만, 일반적으로 "모든 국민은 개인으로 존중된다. 생명, 자유 및 행복추구에 대한 국민의 권리에 대하여는 공공의 복지에 반하지 않는 한 입법 그 밖의 국정에 있어서 최대의 존중을 필요로 한다"고 규정하고 있는 일본헌법 제13조를 근거로 프라이버시권을 인정하고 있다.

위와 같이 미국, 독일, 일본에서 자기정보통제권의 법적 근거를 논의한 바, 이들 나라에서는 헌법상으로 개인정보 내지 자기정보통제권에 관한 명문규정은 없지만 판례를 통하여 개인정보 또는 사생활을 보장해오고 있다. 또 명문규정이 없는 관계로 대부분 그 법적 근거를 우리 헌법 제10조에 해당하는 인간의 존엄과 가치, 생명권, 행복추구권에서 그 법적 근거를 도출해내고 있다. 특히 독일의 경우 기본법 제1조 제1항의 인간의 존엄은 기본법의 가치질서에 있어서 최고의 가치라고 보아 자기정보관리통제권을 기본법의 가치질서에서 그 근거를 찾기도 한다.

(2) 우리나라의 경우

우리나라의 경우 헌법 제17조에서 그 법적 근거를 찾고 있기는 하나 오늘날 문제가 되고 있는 자기정보관리통제권에 관한 법적 근거에 대해서는 아직 명확한 근거를 제시하지 못해 학설과 판례의 견해가 나뉘어져 있다.

자기정보관리통제권에 대한 헌법적 근거에 대해서는 헌법 제17조는 소

극적 권리이므로 인간의 존엄과 가치를 규정한 헌법 제10조에서 찾는 견해[287], 헌법 제17조의 사생활의 비밀과 자유를 근거로 하는 견해,[288] 헌법 제10조와 제17조를 종합하여 이해하는 견해,[289] 제16조의 주거의 자유와 제18조 통신의 비밀보장 및 주거이전의 자유 등에서 결합적으로 찾는 견해가 있다.

이에 대하여 대법원은 헌법 제10조와 제17조에서 개인정보자기결정권을 도출하고 있으며,[290] 최근 헌법재판소는 개인정보자기결정권의 헌법상 근거에 대하여 헌법에 열거되지 아니한 독자적인 기본권으로 보고 있다.

가) 학설

㈀ 권영성 교수는 자기정보관리통제권을 사생활의 비밀과 자유의 일환으로 보아 헌법적 근거를 헌법 제17조에서 찾고 있다. 즉, 자기정보관리통제권은 헌법 제17조의 사생활의 비밀과 자유의 일환으로서 보장되고, 궁극적으로는 인간의 존엄성 존중의 내용이 되는 인격의 자유로운 발현과 법적 안전성을 그 보호법익으로 한다고 한다. 그러므로 자기정보관리통제권은 인격권의 일종이라고 보고 있다. 그러나 사생활의 비밀과 자유가 공권력 또는 제3자에 대한 소극적·방어적 성격의 권리라면, 자기정보관리통제권은 청구권적 성격이 강한 능동적·적극적 권리이며, 자기정보관리통제권은 일신전속권리이라고 한다. 그리고 자기정보관리통제권 중에서 자기정보열람청구권은 알 권리로서의 성격도 가지고 있기 때문에 정보공개청구권과 중복되는 측면이 없지 아니하다[291]고 한다.

㈁ 김철수 교수는 자기정보관리통제권의 헌법적 근거를 헌법 제10조의 인간의 존엄과 가치 및 행복추구권 규정에서 근거를 찾고 있다. 즉, 사생활의 비밀과 자유의 권리는 오늘날 적극적인 자유권에 그치는 것이 아니고, 자기에게 관련된 정보의 전파를 컨트롤할 수 있는 권리로 파악하려는 경향이 있으며, 이는 오늘날의 정보화사회에서 개인의 존엄을 보장하기

287) 정태호, “개인정보자결권의 헌법적 근거 및 구조에 대한 고찰 -동시에 교육행정정보시스템(NEIS)의 위헌여부의 판단에의 그 응용-”, 헌법논총 제14집, 헌법재판소, 2003, 401-496면; 한수웅, “헌법상의 인격권”, 헌법논총 13, 헌법재판소, 2002, 623-678면 등.
288) 정태호, 앞의 논문, 401-496면.
289) 김일환, 앞의 주 268), 102면.
290) 대법원 1998. 7. 24. 선고 96다42789 판결.
291) 권영성, 앞의 주 229), 454면.

위하여 필수적인 것으로 인정되어야 할 것이라고 하였다. 그러나 우리 헌법의 해석으로는 이러한 적극적 권리가 소극적 자유권으로 규정하고 있는 헌법 제17조의 사생활의 자유에 의해 보장된다고 보기보다는 다른 헌법규정에서 그 근거를 찾는 것이 타당할 것이며, 자기의 정보를 컨트롤 할 수 있는 적극적 권리, 즉 정보에 대한 자기결정권은 헌법 제10조에서 보장되고 있다고 볼 것이다[292]라고 주장한다.

㈐ 김종철 교수는 자기정보관리통제권을 자유로운 인격성의 보장을 위한 측면과 권력통제권이라는 정치적 권리로서의 성격을 동시에 가지는 복합적 권리로 파악하고, 그 헌법적 근거도 자유로운 인격성의 보장을 위한 측면은 인간의 존엄과 가치 및 행복추구권에 관한 조항 헌법 제10조에서 찾고, 정치적 권리로서의 개인정보통제권의 근거는 궁극적으로 우리 헌법의 기본원리로서의 국민주권의 원리와 민주주의의 원칙에서 찾고 있다.[293]

㈑ 백윤철 교수는 정보사회에 있어서 프라이버시권은 소극적 권리뿐 아니라 적극적 권리로서 개인정보에 대하여 자기가 결정할 수 있는 권리로 발전하였으므로 개인정보자기결정권에서 개인정보의 개념을 프라이버시권에 한정하는 개념으로 이해해서는 안 되며, 넓은 개념으로 이해해야 하므로 개인정보자기결정권은 헌법 제10조를 그 이념조항으로 하고, 제17조를 근거조항으로 하며, 제16조와 제18조 등에 의해서 보장된다[294]고 한다.

㈒ 정태호 교수는 개인정보자기결정권의 헌법적 근거를 헌법 제10조 제1문 전단의 인간의 존엄 및 가치와 연계된 동조 제1문 후단의 행복추구권에 그 근거가 있는 일반적 인격권에서 찾고, 헌법 제17조의 사생활의 비밀과 자유를 일반적 인격권에 근거를 두는 포괄적 개인정보자기결정권의 특별규정으로 이해한다. 따라서 사생활과 관련된 개인정보보호에 관해서는 제17조가 우선적으로 적용되며, 사생활 영역의 정보가 아닌 개인정보자기결정권의 보호를 위해서는 일반적 인격권에 기초한 일반적 개인정보

---

292) 김철수, 앞의 책, 420면.

293) 김종철, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 인터넷법률 제4호, 법무부, 2001, 43면-44면. 아울러 김종철 교수는 소극적인 자유권으로서 뿐만 아니라 적극적인 청구권으로서의 복합적인 성격을 지니는 자기정보관리통제권의 특성에 비추어 사생활의 비밀과 자유에 관한 헌법 제17조와 인간으로서의 존엄과 가치 및 행복추구권에 관한 헌법 제10조가 종합적으로 그 실정법적 근거를 이루고 있다고 주장한다.

294) 백윤철·장교식·이창범, 앞의 책, 162면.

자기결정권이 보충적으로 적용된다고 한다.[295]

㈁ 성낙인 교수는 사생활의 비밀과 자유는 가장 최근에 헌법적 가치를 갖는 기본권으로서 자리 잡게 되었다고 하면서, 자기정보관리통제권의 일차적인 근거를 헌법 제10조에서 찾고 있다. 즉 헌법 제10조의 자기결정권은 그것의 보충적 권리성과 개별적 기본권과의 관련성에 비추어 좁은 의미로 이해하여야 하고, 자신에 관한 정보의 흐름에 주도적으로 관여할 수 있느냐 하는 것은 기본적으로 사생활의 자유와 관련되는 문제이므로 결국 자기정보에 대한 통제권은 헌법 제17조로부터 찾아야 한다[296]고 주장한다.

나) 헌법재판소의 견해

㈀「주민등록법」제17조의8 등 위헌확인 사건

이 사건[297]은 구주민등록법시행령 제33조 제2항에 의한 별지 제30호 서식 중 열 손가락의 회전지문과 평면지문을 날인하도록 한 부분과 경찰청장이 주민등록증발급신청서에 날인되어 있는 지문정보를 보관·전산화하고 이를 범죄수사목적에 이용하는 행위의 위헌 여부를 심판한 것이다. 결국 이 사건 심판청구는 개인정보의 하나인 지문정보의 수집·보관·전산

295) 정태호, 앞의 주 284), 208-209면. 반면, 개인정보가 개인의 사생활의 비밀과 자유의 본질적인 구성부분을 이루고 있고, 상호 불가분의 관계를 맺고 있으므로, 개인정보자기결정권의 헌법적 근거를 헌법 제17조의 사생활의 비밀과 자유에서 찾되, 그것은 '사생활의 비밀'과 '사생활의 자유'라는 문언과는 별개의 독자적 의의를 가지는 것으로 이해해야 한다고 주장한다. 김승환, 앞의 논문, 167면.

296) 성낙인, 앞의 책, 584-585면.

297) 헌법재판소 2005. 5. 26, 결정, 99헌마513 등, 판례집 17-1, 683면; 구 주민등록법은 현행 주민등록법(2007. 5. 11. 법률 제8422호) 제24조에 해당한다; "개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다"라고 판시하고 있다. 하지만 헌법재판소는 개인정보자기결정권의 근거를 헌법상 어느 몇몇의 특정한 조항에서 구하는 것을 포기하는 듯한 태도를 보여주고 있다. 이는 일면 진솔하면서도 간명한 설명방식일 수 있다. 하지만 헌법에 명시되지 아니한 독자적 기본권임을 내세워 헌법적 근거를 이념적 기초에 소급하는 것은 지나친 감이 없지 않다. 적어도 국민주권원리와 민주주의원리 등에까지 헌법적 근거를 확대시키는 것은 문제가 있는 것으로 보인다. 권건보, 앞의 주 102, 108면 참조.

화・이용이라는 일련의 과정에서 적용되고 행해진 규범 및 행위가 헌법에 위반되는지 여부를 그 대상으로 하는 것이다.

이 사건에서 헌법재판소는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다고 하였다.

그리고 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함하며, 또한 그러한 개인정보를 대상으로 한 조사・수집・보관・처리・이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다고 보았다.

개인정보자기결정권의 헌법상 근거에 대해서는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이라고 하여 헌법 제37조 제1항에 규정되어 있는 '헌법에 열거되지 아니한 권리'로 이해하였다.

㈏ 개인정보수집 등 위헌확인 사건

소위 교육정보시스템(NEIS) 위헌판결[298]에서 헌법재판소는 개인정보자

298) 헌법재판소 2005. 7. 21. 결정, 2003헌마282·425(병합), 판례집 17-2, 91면; 이 결정에서는 개인정보자기결정권에 대한 일반적 설명은 위의 지문날인제도에 관한 헌법소원에서 판시한 내용을 그대로 인용하면서도, 그 헌법적 근거에 대해서는 일반적 인격권(헌법 제10조 제1문)과 사생활의 비밀과 자유(헌법 제17조)에 한정지으려는 태도를 보여주고 있다. 이것이 얼마나 의미있는 차이인지는 좀 더 두고 보아야 할 것이다. 권건보, 앞의 책, 109면.

기결정권의 근거에 대한 견해를 변경하였다.

이 사건은 교육정보시스템(NEIS : National Education Information System)이라는 컴퓨터 네트워크 시스템이 전국적으로 구축되었고 2003학년도 1학기부터 개통하여 운영되었는데, 이 시스템은 교육 부문의 전자정부 구현 추진사업으로서, 종전에 학생 및 교원 관련 정보에 대하여 각 학교별로 데이터베이스(database)를 구축·운영하여 오던 것에 대신하여 각 시·도교육청에 데이터베이스를 구축하고 전국의 1만여개 초·중등학교와 16개 시·도교육청 및 구교육인적자원부를 인터넷망으로 연결하여 교무, 학사뿐만 아니라 인사, 예산, 회계 등 교육 관련 전체업무를 상호 전자적으로 연계하여 업무를 처리하고자 한 종합교육정보시스템을 통하여 초·중등학교 졸업생의 성명, 주민등록번호, 직업, 최종학력, 졸업연월일, 가족상황에 관한 정보, 학생생활, 성적, 건강 및 의료 등에 관한 정보를 수집하고 이에 대한 정보파일을 보유하고 있는 것이 행복추구권, 사생활의 비밀과 자유 등의 기본권 침해 여부에 관한 헌법소원심판이다.

이 사건에서 헌법재판소는 개인정보자기결정권의 개념과 개인정보자기결정권의 보호대상이 되는 개인정보에 대하여 전술한「주민등록법」제17조의8 등 위헌사건과 같이 판시하였으나, 개인정보자기결정권은 인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장된다고 하였다.

㈐ 소득세법 제165조 제1항 등 위헌확인등 사건

이 사건[299]은 연말정산 간소화를 위하여 의료기관에게 환자들의 의료비 내역에 관한 정보를 국세청에 제출하는 의무를 부과하고 있는 소득세법 제165조 제1항 등이 환자의 개인정보자기결정권, 양심의 자유 등을 침해하가 하는 것이 문제되었다.

이 사건에서 헌법재판소는 개인정보자기결정권의 개념과 개인정보자기결정권의 보호대상이 되는 개인정보의 법적근거에 대해 NEIS 사건과 같은 견해를 취하였다.

299) 2008. 10. 30. 2006헌마1401·1409(병합) 전원재판부.

㈃ 의료급여법시행령 별표 제1호 가목 등 위헌확인 사건

이 사건[300]에서는 의료급여기관으로 하여금 의료급여 수급권자를 진료함에 있어 진료 전에는 국민건강보험공단에서 구축한 의료급여 관리시스템을 통하여 의료급여 수급권자의 자격정보를 확인하여야 하고 진료 후에는 이들의 투약일수, 입원일수 등 자세한 정보를 국민건강보험공단에 알려주어야 할 의무를 부담하게 하는「선택의료급여기관 적용 대상자 및 이용 절차 등에 관한 규정」제3조의 개인정보자기결정권 침해여부가 문제되었다.

이 사건에서 헌법재판소는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리로서, 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장된다고 하였다.

그리고 개인정보의 공개와 이용에 관하여 정보주체 스스로가 결정할 권리인 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다고 하였다.

다) 법원의 견해

㈀ 대법원의 견해

대법원은 사생활의 비밀과 자유 및 초상권 등을 헌법 제10조에 의한 인격권으로 파악하고 있다. 대법원은 헌법 제10조와 제17조는 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하는 데에 그 취지가 있는 것으로 해석된다[301]고 하였다.

또한 사람은 누구나 자신의 얼굴 기타 사회통념상 특정인임을 식별할

300) 헌법재판소 2009. 9. 24. 2007헌마1092결정.
301) 대법원 1998. 7. 24. 선고, 96다42789 판결.

수 있는 신체적 특징에 관하여 함부로 촬영 또는 그림으로 묘사되거나 공표되지 아니하며 영리적으로 이용당하지 아니할 권리를 가지는데, 이러한 초상권은 헌법 제10조 제1문에 의하여 헌법적으로 보장되는 권리"[302]라고 하여 거듭 재확인되고 있다.

㈏ 하급법원의 견해

서울중앙지방법원은 소위 '로마켓 변호사 승소율 제공 사건'[303]에서 헌법 제10조와 제17조는 "개인의 사생활이 타인에 의해 침해되거나 함부로 공개되지 아니할 소극적인 권리는 물론, 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석되므로, 개인은 헌법상 보장되는 인격권의 일종으로서 자신에 대한 정보를 스스로 통제할 수 있는 적극적인 권리(이를 일응 '자기정보통제권'이라 부를 수 있을 것이다)를 가진다고 할 것이고, 이에는 국가 및 사인에 대하여 자신의 정보에 대해 수집 금지, 열람·정정을 청구할 수 있는 권리 외에 자신의 동의 없는 개인정보 이용행위에 대해 삭제·이용중지 등 금지를 청구할 수 있는 권리 역시 포함된다"고 하여 자기정보관리통제권의 헌법적 근거로 헌법 제10조와 제17조를 들고 있다.

그리고 또 다른 사건에서도 이와 같은 입장에서 헌법 10조와, 제17조의 규정은 "자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데 그 취지가 있으므로 정보통신서비스이용자들은 자신들의 의사에 반하여 개인정보가 함부로 공개되지 아니할 권리를 가지고, 위와 같이 헌법에 의하여 보장된 기본권을 보호하기 위해 제정된「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 이용자들의 개인정보를 수집・관리하는 정보통신서비스제공자로서는 이용자들의 개인정보가 누출되지 않도록 필요한 관리적 조치를 다하여야 할 주의의무를 부담한다"[304]고 하였다.

라) 소결

302) 대법원 2006. 10. 13. 선고, 2004다16280 판결.
303) 서울중앙지법 2007.7.6. 선고 2006가합22413 판결 【정보게시금지등】 항소 〈로마켓 변호사 승소율 제공 사건〉.
304) 서울중앙지법 2007.2.8. 선고 2006가합33062,53332 판결 【손해배상(기)】 항소.

위에서 살펴본 바와 같이 자기정보관리통제권의 헌법적 근거에 대하여는 여러 견해가 논의되고 있으나, 우리 헌법의 해석상 자기정보관리통제권의 실정법적 근거는 헌법 제10조의 인간의 존엄과 가치 및 행복추구권과 헌법 제17조의 사생활의 비밀과 자유의 양 조항에서 찾는 것이 보편적일 것이다.

자기정보관리통제권은 소극적인 자유권으로서의 성격뿐만 아니라 적극적인 청구권으로서의 성격[305]을 지니고 있기 때문에 헌법 제17조에서 자기정보관리통제권의 근거를 구하는 견해는 사생활보호에 관한 규정들의 관계를 규명하고 있다는 점에서 높이 평가할 만하다. 성낙인 교수도 헌법 제10조의 자기결정권은 그것의 보충적 권리성과 개별적 기본권과의 관련성에 비추어 좁은 의미로 해석해야 하고, 자신에 관한 정보의 흐름에 주도적으로 관여할 수 있느냐 하는 것은 기본적으로 사생활의 자유와 관련되는 문제이므로 결국 자기정보에 대한 통제권은 헌법 제17조로부터 찾아야[306] 한다고 한다.

사생활의 자유가 청구권적 성격을 지닌다고 하는 것과 관련하여서도 세심한 주의가 요망된다. 설령 자유권적 기본권이라 하더라도 부당한 공권력의 발동이 있을 경우 그로 인한 침해의 배제를 청구할 수 있는 것이다. 열람이나 정정을 청구할 수 있는 권리를 내포한다고 하여 그것이 곧 청구권적 기본권으로서의 성격을 가진다고 하는 것은 성급한 측면이 없지 않다. 오히려 그러한 권리가 자신에 관한 정보의 처리에 대해 적극적으로 감시하는 기능도 한다는 점에서 단순한 방해의 배제나 예방의 차원을 넘어선 적극적 성격의 방어권 정도로 이해하면 족할 것이다.[307]

이에 대하여 김철수 교수는 제17조의 위치로 보아 자유권적 기본권에 속하는 사생활의 비밀과 자유는 소극적인 방어권일 수밖에 없기 때문에 열람·정정청구를 내용으로 하는 적극적 성격의 자기정보관리통제권은 헌법 제10조에서 찾지 않으면 안 된다고 주장하다. 그러나 제10조의 규정이 기본권조항인가 하는 점에 대해서는 논란의 대상이 되고 있다. 그리고 적어도 1980년 헌법에서 사생활의 비밀과 자유의 조항이 신설되면서 종래 제10조에 의해 헌법에 열거되지 아니하는 기본권의 목록을 포섭해야할 실

305) 권형준, 앞의 주 255), 28면.
306) 성낙인, 앞의 책, 584면.
307) 권건보, 앞의 책, 109면.

익이 상당히 줄어든 것만은 부인하기 어려울 것이다. 개별적 기본권에 포섭되기 어렵던 다양한 사적 영역을 보장하기 위하여 협의의 인격권으로 설명해왔던 것 가운데 대부분이 사생활보호의 조항에 포섭될 가능성이 생겼기 때문이다. 자신에 관한 정보를 스스로 관리하고 통제할 수 있는 권리도 사생활의 자율적인 영위를 보장하는 사생활의 자유에 포섭될 수 있는 경우라고 할 수 있을 것이다.[308]

반면에 권형준 교수는 헌법 제17조의 사생활의 비밀과 자유 조항은 소극적인 자유권의 근거라고 해석할 수 있을지언정 적극적인 청구권의 근거라고 광의로 해석하기에는 무리가 있다고 한다. 왜냐하면, 우리 헌법은 프라이버시에 관하여 통신에 관한 부분은 헌법 제18조에서 규정하고, 주거에 관한 부분은 헌법 제16조에서 규정하고 있어서 헌법 제17조의 사생활의 비밀과 자유 조항에서 보호하고 있는 프라이버시의 영역은 통신과 주거에 관한 부분을 제외한 좁은 영역일 수밖에 없어 헌법 제17조를 프라이버시 일반에 관한 조항으로 확대해석하여 적극적인 청구권을 도출하는 것은 우리 헌법의 해석상 타당하다고 할 수 없다[309]고 한다.

하지만, 사생활의 비밀과 자유는 자신에 관한 정보를 타인에게 공개할지 말지 그리고 자신의 삶의 스타일에 대한 타인의 충고를 받아들일지 말지를 원칙적으로 스스로 결정할 수 있는 법적 능력을 전제로 하는 기본권이라 할 수 있다. 또한 공동체적 삶에의 편입 내지 참여의 기회를 제공한다. 특히 사생활의 자유는 공권력에 의한 부당한 간섭으로부터 개인의 자유영역을 보호하며, 나아가 공동체 속에서 자유로운 협력과 형성을 위한 전제조건들과 가능성을 보호한다. 이러한 점에서 자신에 관한 정보를 형성・관리・처분하는 데 관여할 수 있는 개인의 권리는 기본적으로 사생활의 자유와 형성을 자율적으로 결정 내지 통제할 수 있는 자유에서 나온다고 할 수 있다.

그리고 사생활의 비밀과 자유가 기본권이라는 이유로 소극적 권리로서만 이해되는 것은 옳지 않다고 본다. 오늘날 공권력의 침해로부터 방어할 수 있는 자유권에 있어서도 침해상태의 배제를 요구하는 소극적 청구권뿐만 아니라, 잠재적 침해요인의 금지 내지 침해의 예방을 위한 조치를 요구하는 적극적 청구권까지도 포함되는 것으로 이해해야 할 경우가 있다.

---

308) 권건보, 앞의 책, 111면.
309) 권형준, 앞의 주 255), 28면.

특히 개인정보보호와 관련하여서는 자신에 관한 정보에 접근하여 그것이 적절히 그리고 정확히 보유 또는 처리되고 있는지 확인하고, 그 결과 사실과 다른 부분이 있거나 잘못 관리되고 있는 경우 그것을 정정하거나 삭제할 것을 청구할 수 있는 권리의 보장이다.[310]

이러한 자기정보관리통제권의 일반적인 헌법적 근거는 먼저 사생활 보호에 관한 포괄적 성격을 고려하여 헌법 제17조에서 찾아야 한다고 본다. 왜냐하면 헌법 제17조는 어디까지나 헌법 제10조에 대해 특별법적 지위를 가진다고 보아야 하기 때문이다. 다음으로 자기정보관리통제권이 인간으로서의 존엄과 가치 및 행복추구권에 관한 헌법 제10조에 근거를 두고 있기 때문에 소극적인 자유권으로서 뿐만 아니라 적극적인 청구권으로서의 복합적인 성격을 지니는 자기정보관리통제권의 특성에 비추어 사생활의 비밀과 자유에 관한 헌법 제17조와 인간의 존엄과 가치 및 행복추구권에 관한 헌법 제10조가 종합적으로 그 실정법적 근거를 이루고 있다고 보는 것이 타당하다고 하겠다.

2) 자기정보관리통제권의 법적 근거

(1)「공공기관의 개인정보보호에 관한 법률」

「공공기관의 개인정보보호에 관한 법률」은 공공기관의 컴퓨터에 의하여 처리되는 개인정보를 보호하기 위한 일반법으로서 1994년 1월 7일 제정되고, 1995년 1월 8일부터 시행되고 있다.

이 법률은 공공기관의 컴퓨터에 의하여 처리되는 개인정보를 보호하기 위하여 각 행정기관이 개인정보처리시스템 내지 개인정보파일을 보유하고자하는 경우에 그 보유범위 및 절차를 규율하고, 개인정보파일에 수록된 개인정보를 이용하거나 제3자에게 제공하는 것에 대해 일정한 실체적 및 절차적 제한을 가하며, 정보주체에게는 열람 및 정정청구권을 인정한다는 것을 주된 내용으로 하고 있다(법 제2조 제4호). 따라서 이 법은 공공기관에서 컴퓨터로 처리되는 개인정보만을 대상으로 하고 있기 때문에 민간부문에서 컴퓨터처리로 이용되는 개인정보나 공공기관이라도 수기로 처리되는 개인정보 또는 다른 법률에 특별한 규정이 있는 경우 및 공공기관의 컴퓨터에 의하여 처리되는 개인정보 중 통계법에 의하여 수집되는 개인정

310) 김일환, 앞의 주 268), 98면, 김승환, 앞의 주 233), 166면; 권건보 앞의 책, 114면 등.

보와 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공・요청되는 개인정보는 이 법률의 대상에서 제외된다고 할 수 있다(법 제3조).

(2)「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

이 법은 정보통신망의 이용을 촉진하고 정보통신 서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다(법 제1조)고 하여 이 법의 제정목적에서 규정하고 있는 것처럼 민간부문의 개인정보 중에서 정보통신망을 통하여 이용하는 개인정보의 보호를 목적으로 제정되었다.

이 법은 원래 정보통신망에서 정보통신 서비스의 제공과 관련하여 수집・처리・이용・제공되는 개인정보를 일반적으로 보호하고자 하는 법률이다. 다만, 일부 오프라인 민간사업자(여행사업자, 호텔사업자, 항공운수사업자, 학원・교습소사업자, 기타 정보통신부령으로 정하는 자)가 재화 또는 용역을 제공하면서 수집・이용 또는 제공되는 소비자의 개인정보까지 보호한다. 그러므로「정보통신망 이용촉진 및 정보보호에 관한 법률」은 기본적으로는 온라인상에서의 개인정보를 보호하기 위한 개별법 성격을 가지지만, 일부 오프라인상에서의 개인정보도 포함하여 보호하고 있다고 할 수 있다.

이 법 제4장 제22조 이하에서 개인정보보호를 위한 구체적인 내용을 규정하고 있다. 정보통신 서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 일정한 사항을 이용자에게 알리고 동의를 받아야 한다(법 제22조 제1항). 그리고 정보통신 서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리・이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다. 정보통신 서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신 서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니된다(법 제23조 제1항 내지 제2항)고 하여 개인정보보호를 위한 규정을 두고 있다.

그리고 이 법은 정보통신이용자의 권리로서 자기정보관리통제권을 규정하고 있다. 즉, 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자는 정보통신서비스 제공자 등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있고, 이에 따라 정보통신서비스 제공자등은 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다. 그리고 이용자는 정보통신서비스 제공자 등에 대하여 본인에 관한 ① 정보통신서비스 제공자 등이 가지고 있는 이용자의 개인정보, ②정보통신서비스 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황, ③ 정보통신서비스 제공자 등에게 개인정보 수집·이용·제공 등의 동의를 한 현황에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다. 이 열람과 제공을 요구받은 정보통신서비스 제공자 등은 지체 없이 필요한 조치를 하여야 하고, 오류의 정정을 요구받으면 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알리는 등 필요한 조치를 하여야 하고, 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그 개인정보를 제공하거나 이용할 수 있다. 그리고 정보통신서비스 제공자 등은 위와 같은 동의의 철회 또는 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다(법 제30조)

한편, 정보통신망에서의 사생활 침해와 명예훼손 등 권리 보호와 관련된 자기정보관리통제권을 규정하고 있다. 즉 이용자는 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 정보통신망에 유통시켜서는 아니되며, 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 이러한 정보가 유통되지 아니하도록 노력하여야 한다(법 제44조).

만약 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재를 요청할 수 있으며, 이 요청을 받은 정보통신서비스 제공자는 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다(법 제44조의2 제1항 내지

제2항).

이와 같은 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 정보통신서비스 제공자는 해당 정보에 대한 접근을 임시적으로 차단하는 조치를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다(법 제44조의2 제4항). 이와 병행하여 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 임시조치를 할 수 있다(법 제44조의3).

3. 자기정보관리통제권의 보호영역

가. 익명권

익명권 또는 익명거래의 자유는 정보주체가 국가·기업·사인 등의 제3자와 온라인 교섭 또는 거래를 할 때 불필요하게 자신의 신원을 밝히지 않고 거래를 할 수 있는 권리를 말한다. 즉, 익명권은 타인의 관심과 식별로부터 벗어나서 개인의 내부영역에 홀로 머물고자 하는 인간의 안식욕의 표현이라고 할 수 있는 바, 개인의 이름이나 기타 개인을 식별할 수 있는 정보를 전부 혹은 부분적으로 익명화(Anonymisierung) 또는 가명화(Pseudonymisierung)함으로써 개인정보자기결정권의 침해 가능성이 최소화될 수 있을 것이다.[311]

오늘날 정보통신기술의 발전은 정치적 필요나 시장의 필요에 따라 모든 거래관계에 있어 놀라울 정도로 거래 당사자의 신원확인을 가능하게 하는 방향으로 나아가고 있으므로 신원확인에 제동을 거는 헌법상 장치로서 익명권이 보장되어야 할 것이다. 이러한 의미에서 익명권이야말로 개인정보자기결정권의 헌법정신을 실현함에 있어 전제가 되는 기본권이라 하겠다.[312]

도시사회 대중화현상의 하나로서 '이름을 숨긴다'는 의미를 갖는 것은

311) Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in Informationsgesell-schaft - Auf dem Wege zu einem neuen Konzept des Datenschutzes -, AöR, 123. Band, Heft 4, (1998), S. 535.

312) 이인호, 개인정보자기결정권의 한계와 제한에 관한 연구, 한국정보보호진흥원, 2001, 23면.

사회집단에서 개인이 불특정 다수의 일원이 되면 그 자주성과 개성적 요소를 상실하고 평균화되어 버리는 성질을 가리킨다. 정보사회에서 개인이 기계부속품화되어 사상·정서가 무시되고, 획일적 행동양식이 강요되기에 이르는데, 이러한 사회구조가 익명화를 초래하게 된다.

특히, 사이버 공간에서의 익명성은 인터넷의 형성 당시부터 태생적으로 정보에 대한 자유로운 접근 및 유통 그리고 표현의 자유를 보장하는 장치이기 때문에, 그것을 제한하거나 제거해야 된다는 것은 사이버공간이 자유를 상실한 공간이 된다는 것을 의미한다. 물론 익명에 의한 커뮤니케이션이 명예훼손이나 비방 등 범죄목적으로 악용되는 경우도 존재할 수 있고, 또 조직사회에서 개인은 자신을 숨기고 대중의 일원이 되는 익명성을 사회조직에서 요구받기도 하여 때로는 스스로 자신을 익명화시켜 사회적 책임을 회피하는 수단으로 삼기도 하여 익명성의 부정적 측면도 없지 않지만, 익명에 의한 커뮤니케이션의 긍정적 가치를 부정할 수는 없을 것이다.

이러한 맥락에서 미국과학발전협회(American Association for the Advancement of Science)는 1997년 11월 향후 인터넷에 대한 규제 시스템이나 규제정책들을 설계함에 있어서 온라인에서의 익명 커뮤니케이션(anonymous communication online)을 보장하기 위한 4가지 원칙을 다음과 같이 제시한 적이 있다.

첫째, 익명성은 도덕적으로 중립적이라는 원칙이다. 익명성에서 야기될 수 있는 양면성, 즉 순기능적 측면과 역기능적 측면을 구분하는 것이 중요하고, 역기능적 측면이 순기능적 측면을 불필요하게 제한하는 근거로 활용되어서는 안 된다는 것이다. 이 원칙에 입각하면, 익명성에 대한 도덕적 가치판단을 전제로 해서 모든 인터넷상의 일탈행위 내지 역기능의 원인이 익명성에 있고, 그 익명성을 제거하면 이러한 역기능이 해소될 것이라고 한다. 이것은 현행 인터넷 실명제의 기본철학이 되는 것으로서 굉장히 단순한 발상이자 논리의 비약이라고 할 것이다.

둘째, 익명커뮤니케이션은 강력한 인권(strong human right)이자 헌법상의 권리(constitutional right)로 간주되어야 한다는 원칙이다. 그 규범적 전거로 제시되고 있는 것이 1948년 유엔총회에서 채택된「인권선언(Universal Declaration of Human Rights)」제12조(사생활의 자유)[313] 및 제19조(표현의 자유)[314], 그리고 미국의 수정헌법 제1조이다.

셋째, 온라인커뮤니티에 대해서 익명 커뮤니케이션의 이용에 관한 자신만의 고유한 정책이나 조건을 설정할 수 있게 허용되어야 한다는 원칙이다. 즉 개인이 실명으로 의사표현을 하든 익명으로 의사표현을 하든 또한 게시판 등의 온라인커뮤니티를 운영하는 자가 실명제방식으로 그것을 운영하든 익명제방식으로 운영하든, 각 개별 주체에게 선택권을 보장해야 한다는 원칙을 의미한다.

넷째, 개별 인터넷이용자에 대해서 자신의 정체성이 온라인에서 어느 정도 공개되어 있는지에 관해 통지를 받아야 한다는 원칙이다. 즉 이용자는 자신이 이용하는 온라인 서비스가 어떠한 조건으로 익명성을 어느 정도까지 허용하고 있는지에 관해서 충분히 고지 받아야 한다는 것을 의미한다. 이러한 원칙을 투명성 원칙(principle of transparency)이라 할 수 있는데, 위의 자율성 원칙의 논리적 결론이라고 할 것이다.[315]

익명권에 있어서도 민감한 사항에 대한 비판이나 우회적인 여론의 동향을 파악하기 위해서는 인간 본연의 심리상 익명성이 요구되고 그 익명성은 자기결정권에 대한 책임의 인수가 전제되어야 한다는 점에서 가시적 익명권은 헌법 제10조, 제19조 및 제21조와의 관계에서 반드시 보장되어야 할 것으로 보인다.[316]

나. 자기정보 수집·제한통제권

자기정보수집통제권이란 정당한 수집목적을 위하여, 필요한 범위 내에서 공정하고 합리적인 방법으로 정보주체의 분명한 인식 또는 동의하에 개인정보가 수집되어야 하며, 수집목적의 정당성, 수집범위의 필요최소성, 수집방식의 합리성, 정보주체의 인식명확성 등의 요건에 대한 판단은 이익형량을 통해 결정되어야 한다는 것이다.[317]

---

313) 제12조 어느 누구도 그의 사생활, 가정, 주거 또는 통신에 대하여 자의적인 간섭을 받거나 또는 그의 명예와 명성에 대한 비난을 받지 아니한다. 모든 사람은 이러한 간섭이나 비난에 대하여 법의 보호를 받을 권리를 가진다.

314) 제19조 모든 사람은 의견의 자유와 표현의 자유에 대한 권리를 가진다. 이러한 권리는 간섭 없이 의견을 가질 자유와 국경에 관계없이 어떠한 매체를 통해서도 정보와 사상을 추구하고, 얻으며, 전달하는 자유를 포함한다.

315) http://act.jinbo.net/webbs/view.php?board=policy&id=1492 2009.12.3.방문.

316) 정준현, 정보통신망이용촉진및정보보호에관한법률 하위법령의 방향, 한국정보보호진흥원, 2001, 83면.

317) 이인호, “주민등록번호·지문날인과 개인정보자기결정권”, 인터넷법률 제8호, 법무부, 31면.

자기정보관리통제권의 핵심적 내용은 무엇보다도 자신에 관한 정보의 유통을 원칙적으로 정보주체의 의사에 따르도록 하는 것이라고 할 수 있는데, 정보주체는 자신에 관한 정보를 자발적으로 타인에게 알리거나 이용할 수 있게 할 수도 있고, 자신이 원할 경우 그 정보에 대한 타인의 접근이나 이용을 막을 수도 있다. 말하자면, 정보주체는 자신에 관한 정보에 대한 처분권을 가지고 있는 것이다. 이러한 정보주체의 권능은 일차적으로 정보수집에 대한 동의권을 통해서 나타난다.[318]

종래 국가가 자유롭게 수집할 수 있었던 국민의 개인정보에 대해서도 정보주체에게 일정한 통제권을 당연히 부여하여야 한다. 즉 자기정보관리통제권의 보장체계 하에서는 그 수집범위와 방법에 있어서 무제한적이고 무제약적인 국가의 개인정보수집권은 인정될 수 없는 것이다.[319] 더욱이 일단 정보가 수집되면 사후에 이용・유통・통합처리 등에 대한 통제는 사실상 용이하지 않다는 점에서 수집통제권은 중요성을 가지며, 국가의 불합리한 강제수집에 대한 방어권 내지 거부권으로서의 역할을 한다.[320]

만일 이러한 정보주체의 동의를 얻지 않고서 개인정보를 수집하려면 반드시 법률에 그 근거규정이 있어야 하는데, 법률유보원칙 내지 기본권 제한의 일반적 원칙에 비추어 볼 때 그것은 당연한 요청이라 하겠다.

정보주체의 동의는 정보주체의 자유로운 결정에 기초한 것이어야 한다. 그러기 위해서는 정보주체가 그 정보의 수집에 따라 발생할 수 있는 여러 가지 문제점들을 충분히 이해할 수 있는 상황이 전제되지 않으면 안 된다. 즉, 정보처리의 목적, 정보관리자와 정보수집자의 신원, 수집거부에 따른 피해, 향후의 정보처리과정에 있어서 정보주체의 관여권 등에 충분한 고지와 설명이 요구된다.

또한 민감한 개인정보는 수집단계에서부터 신중하게 제한할 필요가 있다. 개인의 사상, 신조 등에 관한 사항은 개인에게 대단히 민감한 정보라 할 수 있다. 이러한 정보는 수집 그 자체에 의하여 인간 내면의 자유의

---

318) 권건보, 앞의 책, 117면; 설령 개인의 동의에 의하여 정보를 제공하더라도 그 정보의 수집·처리·관리자는 그 정보에 대한 배타적 지배권을 가지는 것이 아니라 한정된 이용권만을 가지는 것이며, 이 이용권은 언제나 정보주체의 참여를 보장하는 한도 내에서만 행사되어야 한다. 한상희, 생체정보의 인권적 특성, “지문 등 생체정보이용, 무엇이 문제인가”, 토론회 자료집, 국가인권위원회, 2004. 11. 23. 51면.

319) 이인호,앞의 주 314), 54면.

320) 명재진, “국가에 의한 지문강제날인제도의 헌법적 문제점”, 공법학연구 제7권 제1호, 한국공법학회, 2006, 204면.

본질적 내용을 침해할 가능성이 아주 높다.[321]

한편 현행「공공기관의 개인정보보호에 관한 법률」제4조에서도 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니되며, 다만 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다고 규정하여 민감한 정보의 수집을 제한하고 있다.

다. 자기정보 열람·정정청구권

정보기술의 발달로 개인에 관한 정보가 대량으로 저장·처리되어 그것이 실존인격에 영향을 미칠 수 있는 정보사회에 있어서, 실수로 개인에 대한 정보가 잘못 입력되고 그것이 그대로 존속된다면 정보주체에게 뜻하지 않은 불이익을 초래할 수 있다. 그래서 이러한 가능성을 차단하기 위해 정보열람청구권이 보장되어야 한다.[322]

「공공기관의 개인정보보호에 관한 법률」제12조 내지 13조에서는 정보주체는 개인정보파일대장에 기재된 범위 안에서 본인에 관한 처리정보의 열람을 보유기관의 장에게 청구할 수 있고, 정보보유기관은 정당한 이유가 없는 한 열람을 허용해야 한다고 규정하여 자기정보열람청구권을 보장하고 있다.

자기정보열람청구권은 알 권리의 일환으로서 정보공개청구권으로 보장되기도 한다. 그래서 개인정보가 문서 이외의 필름·자기테이프·자기디스크 등에 수록되어 있는 경우에는 정보주체가 이해할 수 있는 형태로 사본을 작성하여 교부해야 한다.[323] 이러한 열람청구권은 자신에 관한 정보에 대한 액세스권 내지 자기정보에 대한 알 권리로서 이해될 수 있다.[324]

이와 같은 권리를 통해 정보주체는 자신에 관한 정보가 어떤 내용으로

---

321) 권건보, 앞의 책, 117면.

322) 김태현, 앞의 논문, 89-90면.

323)「공공기관의 개인정보보호에 관한 법률」 제12조 및 제13조 참조. 현행 실정법상 청구인에게 형사확정소송기록을 열람·복사할 수 있는 권리를 인정한 명문규정이 없다는 것만을 이유로 하여 위에서 본 바와 같이 요구되는 검토를 구체적으로 행함이 없이 무조건 청구인의 복사신청을 접수조차 거부하면서 복사를 해줄 수 없고 한 행위는 헌법 제21조에 의하여 보장되고 있는 청구인의 알 권리를 침해한 것이므로 위헌이라 할 것이고, 따라서 피청구인의 거부행위는 취소되어야 할 것이다(헌법재판소 1991. 5. 13. 90헌마133 결정).

324) 권건보, 앞의 책, 120면.

기록·보유되고 있는지, 어떠한 목적을 위해 이용되고 있는지, 그 관리상의 안전상태는 어떤지 등에 대해 열람·확인할 수 있어야 한다.

또한「공공기관의 개인정보보호에 관한 법률」제14조에서 규정하고 있는 자기정보정정청구권은 정보주체가 자신에 관한 정보를 열람한 결과 정보내용이 부정확하거나 불완전한 것일 경우 이에 대한 정정을 요구할 수 있는 권리이며, 정보주체의 정정요구가 있을 경우 정보보유기관은 잘못된 부분을 정정하고 정보주체에게 그 사실을 통보해야 한다. 여기서 말하는 부정확하거나 불완전하다는 것은 내용이 잘못된 경우뿐만 아니라 문맥상 오해의 소지가 있는 경우도 포함된다.

정보서비스업자 등 정보보유기관이 개인정보에 객관적으로 명백한 오류가 있다고 판단하는 경우에는 당사자의 청구를 기다리지 않고, 지체 없이 정정하고 그러한 사실을 당사자에게 통지하여야 한다.[325] 나아가 서비스 제공자 등은 제3자에게 이용자의 개인정보를 제공한 경우에는 정정처리결과를 제3자에게 지체 없이 통지하고 해당 정보의 정정 여부를 확인하여 이용자에게 그 결과를 통지하는 것이 바람직하다.[326]

이처럼 잘못된 정보를 정정하는 절차는 행정의 현실적응성을 위해서도 필요한 것이지만, 개인정보에 대한 자율적 통제의 중요성을 감안할 때 정보주체의 권리로서 인식하지 않을 수 없다. 만일 이러한 정정청구권이 보장되지 않는다면 열람청구권은 아무런 의미가 없을 것이다.[327]

라. 자기정보 차단·분리·삭제청구권

정보보유기관이 법률에 규정된 의무를 위반하거나 법률의 취지에 반하여 개인정보를 부당하게 이용하고 있으면, 정보주체는 자기정보의 무단공표·이용의 금지 내지 사용중지 또는 삭제를 요구할 수 있고, 정보보유기관은 당해 청구에 대하여 타당성 여부를 조사·판단하고, 타당성이 있다고 인정하면 그 정보의 사용중지·삭제 여부의 결과를 통보해야 한다.[328]

그리고 개인정보의 저장이나 보유가 허용되지 않거나 정보보유자의 직무수행에 더 이상 필요하지 않게 되는 경우에도 정보주체는 정보보유자에

325) 정준현, 앞의 주 313), 129면.
326) 구재군, "인터넷 이용자의 개인정보 자기결정권", 정보화정책 제10권 제3호, 2003, 146면.
327) 이상명, 앞의 주 226), 232면.
328) 권영성, 앞의 책, 455면.

대하여 자신에 관한 정보를 삭제할 것을 청구하거나 그 정보가 다시는 이용될 수 없도록 차단해줄 것을 청구할 수 있다.

정보주체의 이러한 청구에 이유가 있는 경우에는 정보보유자는 그에 따라야 한다. 하지만 법적으로 혹은 현실적으로 삭제가 불가능하거나 곤란한 사정이 있는 경우에는 정보주체의 삭제청구에도 불구하고 정보보유자는 그 정보를 차단할 수 있을 것이다. 만일 보유하고 있는 개인정보에 대해 정보주체가 정확성 여부에 관하여 이의를 제기하고 그것이 정확한지 여부를 확인할 수 없는 경우에도 그 정보는 차단되어야 한다.[329]

이밖에도 진위 여부에 대해 다툼이 있는 기간 동안 해당정보에 일반인의 접근금지를 요구할 수 있는 권리[330]와 개인의 사생활에 관련된 것이나 본인의 의사에 반하여 타인에 의해 일방적으로 게시된 정보에 대한 일반인의 접근을 차단하는 권리도 인정된다. 차단된 정보에 대해서는 당사자의 동의가 있는 경우를 제외하고는 원칙적으로 제공·이용 또는 접근을 금지해야 할 것이나 다만 학술목적, 입증곤란의 해소, 기타 저장기관 또는 제3자의 우월적인 이익을 위하여 필요불가결한 경우에는 엄격한 요건 하에서 예외를 인정하여야 할 것이다.[331]

4. 자기정보관리통제권의 제한과 한계

가. 자기정보관리통제권의 제한

자기정보관리통제권도 기타의 모든 기본권과 마찬가지로 어떠한 상황에서도 혹은 그 어떠한 이유로도 결코 제한할 수 없는 절대적인 의미를 가질 수는 없다.

왜냐하면 개인정보가 절대적인 통제권을 가진다면 다음과 같은 면에서 사회적인 비용을 수반하게 되기 때문이다. 첫째, 개인 또는 다른 기관이 사실과 다른 오류 또는 허위를 발견하는 것을 훨씬 어렵게 함으로써, '틀린 정보의 유통'을 용이하게 한다. 둘째, 예를 들어 근로자가 자신의 업무수행에 영향을 미치는 건강상태를 공개하지 않는 경우처럼, 관련된 진실

329) 독일 연방데이터보호법 제20조 내지 제4항 참조; 권건보 앞의 책, 121면 등.
330) 독일 연방데이터보호법 제20조.
331) 정준현, 앞의 주 313), 129-130면.

한 정보의 유통을 억제시킨다. 셋째, 기업이 신속하고 정확한 결정을 내리거나 또는 그들 제품이나 서비스를 효율적으로 광고할 수 있는 정보의 수집·처리·저장을 방해한다. 넷째, 자기정보관리통제권은 예를 들어 특정 개인이 아동학대나 성범죄의 경력 또는 전염성질환의 병력을 가지고 있는 경우에 일반 대중이 자신들을 보호하기 위해 그러한 정보에 접근하는 것을 방해함으로써 일반 대중의 신체적 안전을 위협할 수도 있다.[332]

따라서 자기정보관리통제권도 자기의 정보에 관한 절대적인 지배권을 개인에게 부여하는 것은 아니고, 국가안전보장·질서유지·공공복리 등을 위하여 불가피한 경우에는 제한을 받게 된다. 다만 그 제한을 법률에 의하되 그 조건·범위·제한의 내용 등이 명확하게 그리고 한정적으로 규정되어야 하고 과잉금지의 원칙이 존중되어야 한다.[333] 자기정보관리통제권도 공동체 관련성 내지 공동체 구속성을 가지는 한도에서 중대한 공익을 위하여 일정 정도 후퇴하지 않으면 안 되는 것이다.

자기정보관리통제권의 제한은 주로 국방, 경찰, 수사, 재판, 통계, 조세, 복지 등을 위한 공권력의 발동과 관련하여 일어날 수 있으며, 정보의 자유, 알 권리 등 타인의 기본권과 충돌되는 경우에 일정한 제약을 받을 수 있다. 다만 이러한 자기정보관리통제권의 제한에 있어서는 법률유보의 원칙과 과잉금지원칙 등과 같은 기본권 제한의 일반원칙이 충족되어야 함은 물론, 목적구속의 원칙, 수집제한의 원칙, 익명성의 원칙 등과 같은 개인정보보호에 관한 특수원칙에도 합치되어야 한다.[334]

오늘날과 같은 정보사회에서 공동체 구성원들 사이의 의사소통에는 타인의 존재를 인정하고 배려하는 자세가 반드시 요구된다. 여기에는 무엇보다도 타인에 대한 기본적인 이해가 수반되어야 한다. 비록 자신에 관한 정보라고 하더라도 그 정보를 자신의 지배권 하에만 가둬두고 타인에게는 그에 대한 한 치의 접근도 허용하지 않는다면 그것은 공동체의 일원이기를 거부하는 자세이다. 따라서 개인은 누구나 자신의 필요에 따라 타인에 관한 정보를 수집하고 이용 또는 전달할 권리를 헌법상 보유하고 있다고 할 수 있다.[335] 이는 인간의 의사소통에 필수적인 기본권으로서 표현의

332) 이인호, 앞의 주 314), 58면.
333) 권영성, 앞의 책, 452면.
334) 이인호, 앞의 책, 41면.
335) 권건보, 앞의 책, 147면.

자유에 속하는 것이다. 근대 입헌민주국가에 있어서 언론의 자유 내지 표현의 자유는 그 정치 사회질서의 중추신경에 해당하는 기본권[336] 또는 개인의 자유로운 인격발전 및 민주주의적 정치질서에 있어서 결코 빠뜨리거나 양보할 수 없는 전제조건[337] 등으로 평가될 만큼 입헌민주체제의 핵심적인 요소이다.[338]

하지만 이러한 정보의 자유도 그 정보주체가 자신에 관한 정보의 차단이나 그 이용의 통제가 시작되는 곳에서 끝이 난다. 정보의 자유는 자신의 임의대로 접근을 할 수 없는 정보로 변화되도록 하는 헌법상의 요술지팡이가 결코 아니기 때문이다. 만약 자신에 관한 정보들 가운데 어떠한 것이 어떠한 경우에 누구에게 알려지는지 충분하고도 확실하게 알 수 없거나 의사소통의 상대방이 무엇을 알고 있는지 충분히 판단할 수 없다면 개인은 독자적인 자기결정에 따라 계획하고 결정할 수 있는 자유를 심각하게 위협받게 될 것이다. 국가나 사회에 의한 부당한 개인정보의 처리는 개인의 인격발현의 기회는 물론이고 공공복리까지도 저해할 수 있다. 이러한 점에서 오늘날 국가나 사회가 자신에 관한 어떤 정보를 수집·처리해도 되는지를 결정·통제할 수 있는 권리를 개인에게 부여하는 것은 반드시 필요하다.

또 다른 한편으로 자신에 관한 정보라고 하더라도 그에 관한 개인의 통제력은 어떠한 상황에서도 혹은 어떠한 이유로도 결코 제한할 수 없는 절대적인 의미를 가질 수는 없다. 개인의 자신에 관한 정보의 통제권도 공동체의 존립이나 유지 또는 발전을 위하여 일정 정도 후퇴되지 않으면 안되는 것이다. 가령 국가안전보장, 사회질서의 유지, 공동체 구성원 전체의 조화적 공존 등을 위하여 혹은 표현의 자유, 알 권리 등 타인의 기본권과의 관계에서 자신에 관한 정보에 대한 개인의 통제권도 일정 정도 제약될 수 있다. 이러한 점에서 자신에 관한 정보의 통제권의 그 내포와 외연을 획정하는 작업은 매우 중요한 의미를 가질 수 있을 것이다.[339]

자기정보관리통제권에 관한 제한은 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위에서 인정될 수 있는 바,[340] 먼저 국가안

336) 허영, 한국헌법론, 박영사, 1994, 511면.
337) 권영설, "언론의 자유와 공익의 문제", 언론중재 제12호, 언론중재위원회, 1984, 12면.
338) 성낙인, "표현의 자유 -기본권의 개념과 범위에 관한 연구-", 헌법재판연구 제6권, 1995, 169면.
339) 권건보, 앞의 책, 147-148면.

전보장을 위한 제한으로 반국가적 범죄에 대한 수사, 신원조사, 대공·방첩을 위한 사찰 등의 활동을 생각할 수 있다. 이러한 임무를 수행하는 기관으로는 검찰, 경찰, 국가정보원, 군검찰, 헌병, 국군기무사령부 등이 있다.

또한 질서유지를 위한 제한으로는 전과조회, 계좌추적, 범죄수사, 성범죄자의 신상공개, 공직자 등의 병역사항이나 재산내역의 공개, 공직선거후보자의 전과공개, 주민등록제도 등이 있다.

끝으로, 공공복리를 위한 제한으로는 국민건강보험의 시행을 위한 의료정보의 조사, 복지혜택의 여부를 위한 소득 등의 조사, 전염병의 예방을 위한 질병조사, 사회생활지표의 작성을 위한 통계조사 등이 있다.[341]

1) 제한의 정당화기준

사회공동체의 이익이 자기정보관리통제권의 제한을 언제나 정당화하는 것은 아니다. 중요한 것은 기본권의 본질로부터 도출되는 자기정보관리통제권의 제한 가능성이 아니라 자기정보관리통제권에 대한 제한이 어떠한 요건에서 허용되며, 이에 관한 규정은 어떻게 형성되어 있어야 하는가 하는 점이다.

우선 자기정보관리통제권에 대한 제한은 법률의 근거를 필요로 하며 당해 법률상의 제한의 요건과 범위를 명확하게 하여 국민이 인식할 수 있고, 따라서 규범명확성의 법치국가적 원칙을 충족하여야 한다. 또한 입법자는 이를 규율함에 있어서 과잉금지의 원칙을 준수하여야 한다.[342]

(1) 법률유보와 규범명확성의 원칙

공권력에 의하여 이루어지는 개인정보의 조사, 저장, 제공, 공개 등은 자기정보관리통제권이라는 기본권의 제한이라 할 수 있는데, 이 제한은 헌법 제37조 제2항에 의거 법률로서 제정되어 있는 경우에만 가능하다. 즉, 자기정보관리통제권을 제한함에 있어서도 반드시 법률의 수권이 있어

340) 헌법재판소 2005. 5. 26. 99헌마513 결정, 판례집 17-1, 682면.

341) 백윤철, "헌법상 개인정보자기결정권에 관한 연구", 법조 제51권 제58호, 2002, 194; 이상명, "주민등록제도에 대한 헌법적 평가 -주민등록번호와 지문날인을 중심으로-", 박사학위논문, 한양대학교 대학원, 2007, 65-66면.

342) BVerfGE 65, 1 (44).

야 한다. 이는 공권력의 발동에 법률상의 근거를 요구하는 법률유보의 원칙으로서 이해될 수 있다. 이 경우의 법률은 국회가 제정한 형식적 의미의 법률로서 그 절차나 내용상 합헌성이 인정되어야 한다. 그리고 정보조사 기타 정보처리는 관련자가 명시적으로 목적이 구체화된 정보처리에 동의한 경우에만 인정되며, 그 동의 없이 국가안전보장, 사회질서유지, 공공복리를 위하여 제정한 법률에 근거하여서만 할 수 없다.[343]

그런데 개인정보의 처리를 허용하는 법률이 있다고 하더라도 그것은 법치국가원리에서 도출되는 명확성의 요청을 따라야 한다. 특히 개인정보의 수집·처리와 관련지어 보면 이러한 규범명확성의 원칙은 자신에 관한 정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 해당 개인이 명확하게 인식할 수 있어야만 한다는 것이다. 여기서 의도된 데이터 처리의 목표는 물론 그 범위의 영역별로 법률에 명확하게 규정되어야 한다.[344] 따라서 조직법적·절차법적인 예방책들, 관할기관들의 통지의무, 관련자의 포괄적인 설명청구권 등에 관하여 법률이 명시적으로 규정하여 누가, 언제, 어디에서 어떤 경우에 자기에 관한 정보를 가지고 있는지를 국민들이 알 수 있도록 하여야 한다. 특히 관련자가 법규정으로부터 그 개인정보가 어떤 구체적인 행정목적을 위하여 필요한지를 명백히 인식할 수 있어야만 한다. 하지만 입법자가 각 개인의 법률상 의무에 대하여 구체적 목적까지 그 법률에서 밝힐 필요는 없고, 일반적으로 그 목적이 당해 법률의 체계 및 입법취지 등에 비추어 그 의미가 분명해질 수 있다면 그 법률은 이미 충분히 명확하다고 할 수 있다.[345]

(2) 목적구속성의 원칙

목적구속의 원칙(Grundsatz der Zweckbindung)은 비례의 원칙에서 유래한 것으로서 개인정보의 처리에 있어서 그 목적이 수집단계에 이미 명확히 특정되어 있어야 할 뿐만 아니라 그 이후의 처리단계에 있어서도 수집시의 특정된 목적과 일치되게 저장 또는 이용되어야 한다[346]는 것이다.

343) 권건보, 앞의 책, 102면.
344) BVerfGE 65, 1 (44,46).
345) BVerfGE 65, 1 (54).
346) Klaus Vogelgesang: Grundrecht auf informationelle Selbstbestimmung? Nomos Verlagsgesellschaft. Baden-Baden (1987) ISBN 3-7890, S. 71.

개인정보의 수집은 법률에 의하여 특정된 목적범위 내에서만 허용되어야 하며, 이 목적은 규범명확성의 원칙에 따라 일반인이 당해 법률로부터 자신의 개인정보가 왜 필요한 것인지 분명하게 알 수 있도록 특정된 것이어야 한다. 이는 한편으로는 개인정보의 처리목표를 확정하고 다른 한편으로는 그 처리범위를 한정하는 역할을 한다.[347]

또한 불특정한 목적 또는 아직 확정할 수 없는 목적을 위해 개인정보를 미리 수집하는 것은 목적구속의 원칙에 반한다. 그러나 정보의 저장은 그 개념상 장래의 사용을 위하여 준비해 놓는다는 의미가 내포되어 있으므로 미리 정보를 수집하는 것 자체가 금지되는 것은 아니다. 단지 사용목적이 명확하지 않다는 점이 문제되는 것이므로 법률에 의하여 사용목적이 구체적으로 특정되고 정보의 사용이 그에 한정된다면 장래의 목적을 위한 정보의 저장도 허용될 수 있다[348]고 할 수 있다.

이 원칙에 따르면 개인정보의 처리목적이 명확하게 특정되거나 특정될 수 있는 경우에 그 수집이 정당화될 수 있으며, 수집 당시에 정보주체에게 설명되거나 법률에 규정된 그러한 목적에 따라서만 수집된 정보를 저장·이용·전달 등의 처리를 할 수 있다. 그런데 불확정적이거나 혹은 확정될 수 없는 목적을 위하여 익명화되지 않은 데이터를 축적하는 것은 허용될 수 없다.[349] 그리고 다양한 임무를 가진 행정기관들 사이의 데이터 전달을 통한 목적일탈은 목적이 불확정적이거나 확정할 수 없는 경우와 다를 바 없다.[350] 따라서 당초의 목적과 달리 그 정보를 이용하거나 전달하는 것은 그 별도의 목적이 법률에 정해져 있거나 정보주체에게 다시 설명하여 동의를 얻지 않는 한 정당화될 수 없다. 한편 당해 목적이 달성되었거나 그 목적을 달성하는데 더 이상 도움이 안 되는 경우에는 그 개인정보는 파기되어야 한다.[351]

다만, 헌법상의 과제를 수행하기 위한 통계 등 행정조사와 같이 불가피하게 경제적·생태적·사회적 관련성에 관한 포괄적이고 지속적으로 현실화되는 정보가 필요한 경우가 있을 수 있다. 이러한 경우에도 구체적인

---

347) Spiros Simitis, “Von der Amtshilfe zur Informationshilfe”, NJW 1986, S. 2796.
348) Franz-Ludwig Knermeyer, Datenerhebung und Datenverabeitung im Polizeirecht, NVwZ 1988, S. 194.
349) BVerfGE 65, 1 (46).
350) BVerfGE 65, 1 (46, 69).
351) 영국 데이터보호법 제5원칙 참조.

개개의 정보마다 목적구속성이 엄격히 요구된다고 하기는 어렵다.[352]

2) 비례의 원칙

우리 헌법재판소의 결정에 의하면 헌법 제10조와 제17조에 근거를 두고 개인은 자신에 관한 정보를 스스로 관리·통제할 수 있는 권리 등을 내용으로 하는 헌법상 기본권에 해당하는 인격권적인 자기정보관리통제권을 가진다. 그러나 특히 제3자의 기본권과 충돌하는 경우 등과 같이 그 제한이 필요할 경우, 정보의 종류·성격·수집목적·이용형태·처리방식 등에 따라 개인정보에 대한 자기결정권을 제한[353]할 수 있다.

한편 개인정보보호권도 헌법상 보장되는 기본권인 이상, 국가의 공권력에 의해 자기정보관리통제권을 제함함에 있어서도 기본권 제한의 일반원칙인 비례의 원칙 또는 과잉금지의 원칙이 준수되어야 하는 것은 당연하다. 우리 헌법재판소도 법률의 위헌성 여부를 판단함에 있어서, 과잉금지원칙의 구성요로서 목적의 정당성, 방법의 적절성, 피해의 최소성, 법익의 균형성의 네 가지 요소를 들고 있다.[354]

사실 이러한 방법을 적용하여 보호하려는 공익과 침해되는 사익이 최소화한다고 해도 법익을 보호하는 규정들이 그 내용상 미치는 범위에 있어서 상호 중복되거나 충돌하는 경우, 기본권제한은 원칙적으로 실제적 조화(praktische Konkordanz)의 실현이어야 하며, 실제적 조화의 과제는 기본권과 기본권을 제한하는 법익간의 비례성을 요한다. 즉, 헌법적 제한 또는 법률유보에 근거한 제한을 해석할 때 중요한 것은 기본권과 그 제한하는 법익이 최적의 실효성을 얻도록 하는 것이다. 기본권이 법률유보하에 있는 경우에도 헌법질서의 본질적 구성부분에 있는 것이므로, 결코 하나의 기본권적 보장으로부터 공동체의 생활에서 갖는 그 실효성을 필요 이상으로 혹은 완전히 박탈해버리는 방식으로 비례관계가 이루어져서는 안된다. 따라서 기본권의 제한은 그 목적이 법익보호를 실현하는데 적합하여야 하며, 법익보호를 위하여 필요한 것이어야 하므로 보다 약한 제한수단으로 충분한 목적의 달성이 이루어질 때는 비례의 원칙[355]에 위반된다

352) BVerfGE 65, 1 (47); 권건보, 앞의 책, 220-221면 참조.
353) 서울중앙지법 2006.3.2. 자 2006카합147 결정[각공2006.4.10.(32),1038].
354) 헌법재판소 1992. 12. 14. 선고 92헌가8 결정 판례집 4, 878-879면.
355) Konrad Hesse, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20.

고 할 수 있다.

자기정보관리통제권 역시 헌법상 인정될 수 있는 기본권이므로, 그 제한에 있어서 기본권 제한의 일반원칙인 과잉금지원칙이 준수되어야 마땅하다. 다만 과잉금지의 원칙상 정보의 중요도에 따라 그 제한의 정도에 차이가 있을 수 있다.[356] 전술한 바와 같이 영역이론은 개인정보보호의 한계원리로서 인간생활의 여러 국면을 가장 내밀하고 비밀스러운 것으로부터 공개적인 부분에 이르기까지 상이한 취급을 받게 되는 영역으로 세분화하여 각 영역마다 공공과 개인의 관계를 달리 취급하여야 한다는 것이다.[357] 하지만 오늘날과 같은 정보사회에 있어서 인격의 영역별 범주화에 따른 보호의 차등화는 점차 의미를 상실해가고 있다고 하겠다. 예컨대 성별, 주소, 직업, 학교 등과 같은 개인정보는 사회적 영역에 속하는 사항이라 할 수 있지만, 이들 정보가 자동검색절차를 통하여 다른 개인식별정보와 결합될 때는 개인의 내면적 사항까지 추출해낼 수 있는 열쇠로서 기능을 할 수 있다. 따라서 어떠한 영역에 속하는 정보인가에 지나치게 얽매이기보다는 구체적인 정보처리의 위험성을 고려하여 개별적으로 비례원칙의 준수 여부를 검토하는 것이 더 바람직할 것으로 여겨진다.[358]

비례의 원칙은 법치국가의 원리에서 당연히 파생되는 헌법상의 기본원리의 하나로서, 국가가 국민의 기본권을 제한하려면 그 정당성이 인정되어야 하고(목적의 정당성), 그 목적의 달성을 위하여 그 방법이 효과적이고 적절하여야 하며(방법의 적정성), 기본권제한의 조치가 설사 적절하다 할지라도 보다 완화된 형태나 방법을 모색함으로써 기본권의 제한은 필요한 최소한도에 그치도록 하여야 하며(피해의 최소성), 그 보호하려는 공익과 침해되는 사익을 비교형량할 때 보호되는 공익이 더 커야 한다(법익의 균형성)는 원칙이다. 우리 헌법 제37조 제1항에는 입법권의 한계로서 비례원칙을 명문으로 인정하고 있다.[359]

헌법재판소와 각급 법원의 판례도 비례의 원칙을 채택하여 자기정보관리통제권의 제한의 위헌 또는 위법여부를 심사하고 있다. 첫째, 자기정보관리통제권을 제한하기 위해서는 그 목적이 정당하여야 한다. 즉 정보주

Aufl., (1995) Rn. 317ff.

356) BVerfGE 65, 1(45).

357) 박윤흔, 앞의 주 273), 540면.

358) 권건보, 앞의 책, 217면.

359) 헌법재판소 1992. 12. 24. 선고, 92헌가8 결정, 판례집 4, 878-879면.

체의 동의를 얻지 아니하고 개인정보를 취급하는 경우 그것이 법률의 규정에 의한 것이라 하더라도 각 단계별로 달성하고자 하는 목적이 정당하여야 한다. 예컨대 정보주체의 동의를 얻지 아니한 개인정보의 수집이나, 열람거부 또는 목적 이외의 개인정보의 사용 등에서 목적정당성이 문제될 수 있다. 그러나 헌법 제37조 제2항에 의하여 사용되어지는 것은 정당성이 있다고 보아야 할 것이다. 둘째, 자기정보관리통제권을 제한하는 조치가 그 목적의 달성을 위하여 그 방법이 효과적이고 적절하여야 한다. 그러므로 개인정보의 비밀수집이나 공개 등의 조치를 취하더라도 해당 목적을 달성하는 데 별로 도움이 되지 않는 경우 방법이 적절하다고는 할 수 없다. 셋째, 기본권제한의 조치가 설사 적절하다 할지라도 보다 완화된 형태나 방법을 모색함으로써 기본권의 제한이 필요한 최소한도에 그치도록 해야 한다. 예컨대 공공기관간의 행정정보공유가 필요한 경우라 하더라도 개인정보보유기관은 그 개인정보가 무한대로 전달·이용 또는 오·남용의 조처를 사전에 충분히 예방해야 한다. 넷째, 자기정보관리통제권의 제한이 불가피하여 제한하는 경우라 하더라도 그 보호하려는 공익과 침해되는 사익을 비교형량하여 보호되는 공익이 더 커야 한다. 즉 보호이익과 피해이익 사이의 형량에 의하여 개인정보에 대한 침해의 성질, 강도, 민감성 등을 충분히 고려하여야 한다.

그러나 아무리 비교형량하여 얻어지는 공익이 침해받는 사익보다 크다고 할지라도 자기정보관리통제권의 본질적인 내용을 침해하여서는 아니된다. 자기정보관리통제권은 사회공동체의 일반적인 생활규범의 범위 내에서 사생활을 자유롭게 형성해 나가고 그 설계 및 내용에 대해서 외부로부터의 간섭을 받지 아니하는 것이고, 그 중에서도 사생활의 비밀은 사생활과 관련된 사사로운 자신만의 영역이 본인의 의사에 반해서 타인에게 알려지지 않도록 할 수 있는 권리이므로 그 본질적 내용은 전적으로 사적인 의견 교환과 내밀한 마음에 관한 것[360]이라고 할 수 있다.

3) 정보분리의 원칙

일정한 목적을 위하여 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 원칙적으로 통합되지 않고 분리된 상태로 유지되

360) 헌법재판소 2001. 8. 30. 선고, 99헌바92 결정.

어야 한다. 따라서 어떤 기관이 보유하고 있는 개인정보를 데이터베이스를 구축 ·통합하거나 다른 기관에 제공한다든가 자동검색시스템을 통해 개인정보를 공동으로 활용한다든가 하는 것은 원칙적으로 금지된다.

이러한 내용은 독일 연방헌법재판소가 인구조사판결에서 언급한 정보상 권력분립(informationelle Gewaltenteilung)[361]의 원칙과 같은 것이라 할 수 있다. 이 판결에서 헌법재판소는 국가권력이 정보통일체로서 단일화되는 것은 용납되지 않는다고 선언하였는데, 이는 국가행정조직이 다른 목적으로 개인정보를 이용할 소지가 있는 개별 행정부서들에 의한 정보접근이 차단되도록 구성되어야 할 것을 요청하는 의미를 가지는 것으로 이해되고 있다.[362]

4) 시스템 공개의 원칙

정보주체의 동의나 법률의 규정에 의하여 개인정보를 수집하게 되더라도 수집된 개인정보가 어떤 방식으로 축적 또는 보관되는지, 누구에 의해 현실적으로 관리되는지, 얼마 동안 보유될 것인지 등을 감추지 않고 투명하게 제시함으로써 개인정보의 보유와 처리를 둘러싼 오해를 불식시킬 필요가 있다. 이처럼 개인정보의 처리 시스템에 대하여 공개를 일반화함으로써 개인정보의 존재와 성격 및 주요한 이용 목적을 명확히 하여 그 권한의 소재를 밝히기 쉽도록 하는 것을 시스템 공개의 원칙이라 한다.

이는 어떠한 개인정보를 보유하고 있는지를 공개하도록 함으로써 개인정보의 처리에 대한 검증과 감시를 할 수 있게 하고, 정보주체의 열람·정정청구 등 제반 권리행사를 용이하게 하기 위한 것이라고 할 수 있다. 따라서 개인정보의 보유자, 보유상태 등은 물론이고 그 이용현황을 일반인이 알아볼 수 있도록 제시되어야 하며, 권리의 행사에 있어서 지나치게 많은 시간이나 경비가 소요되지 않도록 하여야 할 것이다.[363] 그리고 정보 검색 또는 정보기술이 부족한 개인들을 위한 편의 시스템도 개발하여 서비스를 제공하여야 할 것이다.

---

361) BVerfGE 65, 1(69).

362) 김성태, "개인관련정보에 대한 경찰작용 -독일 주경찰법에서 규율-", 현대공법학의 과제(최송화교수 화갑기념논문집), 박영사, 2002, 976면.

363) 권건보, 앞의 책, 223면.

나. 자기정보관리통제권의 한계

사생활의 비밀과 자유도 무제한으로 보장되는 것이 아니라, 타인의 권리를 침해하는 것이 아니어야 하고 사회윤리(道德律)나 헌법질서에 위반되는 것이 아니어야 한다. 여기에 사생활의 비밀과 자유의 한계가 있다.[364]

개인은 사회적 의사소통 범위 내에서만 자기의 역할을 결정할 수 있는 다수의 사회적 관계 속에서 움직인다. 의사소통은 가치중립적이거나 객관적인 것이 아니라, 내용과 형식에 있어서 의사소통은 상대방에 의존한다.[365]

사생활의 자유와 비밀에서 확장된 개념인 개인정보권 및 자기정보관리통제권의 대상이 되는 개인정보의 결정과 개인정보권이 미치는 범위 등을 설정함에 있어서 모든 개인정보에 대하여 그 수집 및 처리 등에 관한 법률적 근거를 구체적으로 명확히 하도록 하여야 한다. 더구나 개인정보보호권이 정보사회의 위험성에 따라 나타난 것이라면 개인정보를 전자화하고 컴퓨터에 의하여 처리하는 것은 더욱 세밀한 부분까지도 개인정보보호권이 미친다고 하여야 한다.[366]

그러나 현실적으로는 사회생활과 국가생활이 개인정보와 연계되지 아니한 것이 없고, 그 위험성도 선험적으로 결정되는 것이 아니라 구체적 상황에 따라 다르게 나타난다는 것이 문제이다.[367]

결국 개인정보보호권은 무한히 확장되거나 절대적인 것이 될 수 없고, 상대적이고 제한이 불가피한 것으로 인식될 수밖에 없다. 개인정보권의 한계설정을 위해서는 프라이버시권이라고 하는 권리의 태동과 그 배경 및 이론을 살피는 것도 한 방편이 될 수 있다. 개인정보보호권의 원형이라고 인식되고 있는 프라이버시권은 미국 등 서구의 법리에서 발달하였다.[368] 그리고 이러한 제도의 근저에는 공적 영역과 사적 영역을 구분하는 영역적 분리 관념이 있다. 서구 문명에서 공적 영역과 사적 영역이 차별적으

364) 권영성, 앞의 책, 456-457면.
365) 권건보, 앞의 책, 145면.
366) 정태호, “개인정보자기결정권의 헌법적 근거 및 구조에 대한 고찰”, 헌법논총 제14집, 헌법재판소, 2003, 443-444면; 권헌영, 앞의 주 255), 324면.
367) 정태호, 앞의 주 363), 447면; 권헌영, 앞의 논문, 325면.
368) 권헌영, 앞의 논문, 325-326면.

로 취급된 것은 철학적 배경에서 매우 오래된 것으로 공적 영역은 소규모 공동체로부터 국가와 국제사회에 이르기까지 공개적인 영역으로 취급되지만, 사적 영역은 개인이나 가족을 위하여 불가침의 은둔 공간으로 인식된다.[369] 그리고 프라이버시권은 공적 영역을 인정하고 나서 그 공적 영역 중에서 다시 사적 영역의 존재를 찾아내는 논리구조를 가지고 있다.

한편, 개인의 사생활에 속하는 사항이라도 그 성격에 따라 인격적 가치에 미치는 의미가 다를 수 있다. 가령 개인적으로 비밀로 하고 싶어 하는 내용이라 하더라도 그것이 누구에게 알려지면 인간으로서의 존엄성이 심대하게 훼손되는 경우가 있는가 하면, 특정한 집단에게만 알려지지 않는다면 상관이 없는 경우나 혹은 세상에 알려지더라도 그것이 사회 전체의 이익을 위해 감수해야만 하는 상황도 있을 것이다.

독일의 인격영역이론(Sphärentheorie der Persönlichkeit)에 따르면 인격의 영역을 가장 폐쇄적 성격이 강한 영역에서 가장 개방적 성격이 강한 영역으로 단계화하여, ㉮ 내밀영역, ㉯ 비밀영역, ㉰ 사적영역, ㉱ 사회적 영역, ㉲ 공개적 영역 등으로 나누고, 관계되는 인격적 가치가 이들 가운데 어디에 속하는가에 따라 사적 영역에 대한 국가적 개입의 정도나 사생활에 관한 언론보도의 한계 등을 다르게 파악하고 있다. 즉, 내밀영역에 관한 사항은 그 폭로에 대하여 가장 강력한 보호를 받게 되나, 공개적 영역에 관해서는 그 보호가 인정되지 않는다. 가령 혼인관계·가족관계·성관계·건강기록 등과 같은 사적 영역은 국가의 간섭이 허용되는 것으로 본다. 이러한 영역이론은 비례원칙의 구체화로서 이해될 수 있다.

하지만 인격의 영역을 정밀하게 세분하기가 쉽지 않다는 점에 이론적 난점이 있다. 인간의 내부 공간이 사회적 체험과정을 통하여 구성된다고 할 때 이러한 공간을 사회적 접촉과 사회적 영역에서 적당히 구획하는 것은 매우 어려운 문제다.[370]

따라서 개인정보는 이미 공적 영역에서 사회적·국가적으로 의미 있는 공적 정보이며, 그 중에서 개인정보의 대상이 되는 개인정보는 무한히 확장되는 것이 아니고 현실적 환경에서 사회적 공동체의 구성원으로서 공적 영역에 스스로 존재하는 한도에 있어서의 정보활동은 개인정보권의 개념

369) Shils, Edward, "Privacy: Its Constitution and Its Vicissitudes." Law and Contemporary. Problems 281(1966), pp.281-83.
370) 성낙인, 앞의 책, 588-590면.

내재적 한계로 이해할 수 있다.[371] 이러한 점에서 본다면 자기정보관리통제권과 관련한 모든 상황에서 정보주체의 인식과 동의를 지나치게 확장하여야 하는 개인정보 관련규제는 합리적 한계를 설정할 수 있을 것이다.

제2절 개인정보공동이용에서 자기정보관리통제권의 확보방안

1. 개인정보공동이용의 정당화 조건

가. 개인정보수집과정

1) 공동이용의 목적 구체화

「공공기관의 개인정보보호에 관한 법률」제10조 는 “보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니된다”고 규정하여 사전에 공시된 개인정보파일의 보유목적이 아닌 다른 목적으로 처리정보를 이용하거나 제공하는 것을 금지하는 목적구속의 원칙을 규정하고 있다.

이와 같이 개인정보를 공동이용하고자 하는 경우에는 그의 목적이 구체화되어 있어야 할 것이다. 이러한 공동이용의 목적은 크게 행정적인 목적과 연구적인 목적이 있을 수 있는데, 특히 연구적인 목적을 활성화할 수 있도록 할 필요는 있다. 이러한 연구적인 목적의 활성화는 공동이용에 대한 효율성을 제고하기 위한 대안의 수립에 유용한 정보를 제공할 수 있을 것이다.

이러한 목적의 구체화는 공동이용 계획의 수립과정에서 제시되게 된다. 공동이용하고자 하는 조직은 공동이용을 정당화하기 위하여 다음과 같은 것을 제시하여야 할 것이다. ① 데이터의 공동이용을 하지 않을 경우의 잠재적인 위협이나 결과를 명확히 하고, ② 공동이용하고자 하는 개인정

371) 권헌영, 앞의 주 255), 324-326면 참조.

보와 처음 수집한 목적과의 연계성을 확인하고, ③ 공동이용 방법 이외의 대안적인 방법은 없는지에 대한 분석이 있어야 할 것이다. 그리고 공동이용을 정당화하기 위한 비용편익분석 등이 수행될 필요가 있다.[372]

2) 제3자로부터 수집활동

「전자정부법」 제11조는 "행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다"고 규정하고 있다.

공동이용체제는 필요한 개인정보를 개인으로부터 직접 수집하기보다는 제3자로부터 수집하는 간접수집방법을 주로 사용하게 된다. 이 경우 법률의 규정에 의하거나 개인의 동의가 전제가 되어야 한다. 그러나 전국민을 대상으로 하는 데이터베이스를 활용하고자 하는 경우에 개인의 동의를 얻는다는 것은 거의 불가능하다고 할 수 있다. 즉 부동산 투기를 방지하기 위하여 특정 지역의 세대별 주민등록표를 연결하여 위장전입을 식별하는 경우 특정 지역주민 모두의 동의를 얻어야 하는데 이것은 비능률적인 방법이 될 것이다. 이에 대한 통제의 방법은 매번 개인에게 통고하여 동의를 얻는 방법과 이러한 수집을 관보 등에 공고하는 방법간의 연속체 선상의 중간방법을 활용하게 된다고 할 수 있다. 이러한 동의의 한 방법으로 행정기관이 개인정보를 수집할 경우 신고서에 구체적인 공동이용의 내용을 명시하여 개인들이 인지하고 이에 동의를 구하는 방법이 주로 활용될 수 있다.

3) 수집내용

수집 정보내용에 대한 통제는 통합정보관리체계에서 더욱 그 중요성이 확대되고 갈등을 가지는 부분이다. 엄격한 수집제한은 개인정보의 사적가치는 확보할 수 있을지는 몰라도 공적가치나 상업적 가치의 실현을 저해할 수도 있다.

「공공기관의 개인정보보호에 관한 법률」에 의하면 공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의가 있거나 다른 법

372) 박홍윤, 앞의 책, 118-119면.

률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다. 그리고 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 문서 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있도록 안내하여야 한다.

자기정보관리통제권의 보장을 위한 출발점은 수집 단계에서 이루어져야 하고, 그렇기 때문에 그 파생원칙의 하나로서 수집제한의 원칙이 요구된다. 이 원칙은 ① 정당한 수집목적을 위하여(수집목적의 정당성), ② 필요한 범위 내에서(수집 범위의 최소성), ③ 공정하고 합리적인 방식으로(수집방식의 합리성), ④ 정보주체의 분명한 인식 또는 동의하에(정보주체의 인식명확성) 수집되어야 한다는 것을 의미한다.[373]

4) 주민등록번호 문제

개인정보공동이용에 있어서 가장 중요한 정보는 통합식별인자인 주민등록번호라 할 수 있다. 우리나라의 경우 시·군의 주민을 등록하게 함으로써 주민의 거주관계를 파악하고, 상시로 인구의 동태를 명확히 하여 행정사무의 적정하고 간이한 처리를 도모할 목적과 개인정보의 수집·이용·제공을 규율하기 위하여 1962년에 주민등록법이 제정되었다. 이 법률은 전국민의 성명, 성별, 생년월일, 세대주와의 관계, 본적, 주소, 주소이동상황 등의 개인정보를 신고하게(법 제10조) 하고, 개인에게 강제 부여되는 주민등록번호를 표준개인식별인자(universal personal identifier)로 하여(법 제7조 제3항) 이들 개인정보를 전산처리하도록 하고 있다(법 제7조의2).[374] 이 주민등록번호는 공적인 정보로서 공공부문뿐만 아니라 민간부문에서도 공통으로 사용하고 있다. 특히 인터넷 상에서도 거의 제한 없이 사용하고 있다. 이러한 관행은 네트워크화 되고 있는 상황에서 제고할 필요가 있다.

특히 민간부문에서 활용하는 경우 일정한 규제를 가할 필요가 있고, 민간부문의 대규모화된 데이터베이스에서 이를 주요한 필드로 사용하는 것들은 제한되도록 하여야 한다. 또한 주민등록번호 체제도 장기적으로는 제고되어야할 것이다. 또한 주민등록번호가 개인의 프라이버시와 연결될

373) 이인호, 앞의 주 213), 22면.
374) 위의 책, 32면.

수 있는 생년월일이나 발급지와 연계되어 부여되는 것은 개인의 프라이버시 보호의 차원에서 새로운 번호체계로 전환될 필요가 있다.[375]

5) 목적구체성 문제

자기정보관리통제권에 포함되는 목적구속의 원칙이란 ① 개인정보를 수집하는 목적(목적의 특정성)은 특정되어야 하고, ② 그 후의 이용은 이 특정된 수집목적과 일치되어야 한다(목적일치성)는 요청이다. 이 원칙은 개인정보 수집기관 이외에 제3자에 대한 제공을 통제하기 위한 것이다. 물론 이 원칙이 절대적일 수는 없고, 법률이 명시적으로 허용하는 예외가 있을 수 있다. 다만, 제3자 제공의 경우에도 수집제한의 원칙이 적용되기 때문에 제공목적의 정당성, 제공범위의 필요최소성, 제공방식의 합리성, 정보주체의 인식명확성이 요구된다.[376] 그리고 수집목적 이외에 확대되는 공동이용에서 목적의 구체화는 개인 참여 및 통제의 전제가 된다는 점에서 보다 명확히 제시될 필요가 있다. 수집목적의 구체화는 개인정보 침해의 여부를 판단하는 중요한 기준이 된다는 점에서 가능한 한 구체적으로 명시될 필요가 있다. 그러나 개인정보를 이용하는 조직들은 이에 대하여 추상적이고 포괄적인 목적을 제시하여 이용의 제한을 피하려고 한다. 이를 방지하기 위하여 조직의 개인정보 수집을 조직의 목적과 관련하여 최소한의 범위에 한하도록 하는 방안이 요구된다. 목적구체성을 확보하기 위해서는 정부나 조직을 하나의 단위로 생각해서는 안 되며, 기능적으로 분리하여야 할 것이다.

그러나 공동이용체계에서는 개인정보를 관련 부서의 자원으로보다는 조직의 자원으로 이해하는 경향이 많다. 이를 제한할 수 있는 구체적인 방법은 업무를 기능별로 분리하여 개인정보의 이용을 해당기능에 한하여 이용하게 하여야 한다.[377]

나. 개인정보관리

1) 개인정보의 질 확보

375) 박홍윤, 앞의 책, 120면.
376) 이인호, 앞의 책, 23면.
377) 박홍윤, 앞의 책, 121면.

개인정보공동이용의 환경에서는 기술적인 시스템의 질보다 데이터의 질에 더 관심을 기울여야한다. 이는 공동이용과정에서 발생하는 오류의 대부분이 정당한 이용과정에서 잘못된 데이터에 의하여 발생되기 때문이다. 또한 공동이용 과정에서는 오류를 확인하거나 검증하는 것이 더욱 어렵기 때문이다.

데이터의 질을 확보하기 위해서는 개인정보 데이터베이스에 탑재된 데이터 질에 대한 성과평가와 감사활동이 활성화될 필요가 있다. 현실적으로 이들에 대한 감사가 상당부분 이루어지고 있지 못한 상태에서 일상적인 행정감사의 한 부분으로 이들 시스템에 대한 질감사가 포함될 필요가 있다.

데이터 질을 확보함에 있어서 개인정보의 최신성을 확보하는 것도 질과 밀접한 관계를 가진다. 최신성을 확보하기 위해서는 공동이용 기관간의 데이터 전송이 온라인으로 이루어져야 한다. 잘못된 정보에 대한 신속한 정정작업이 이루어지도록 할 필요가 있다. 공동이용에서는 다른 기관이 제공한 정보를 바탕으로 의사결정을 하게 되는데 이 경우 다른 기관의 정보가 잘못된 것으로 밝혀진다고 하더라도 이를 수정하고 새로이 개인정보를 받는다는 것은 매우 어려운 일이다. 이러한 문제를 해결할 수 있는 제도적 장치가 마련되어야 한다.[378]

2) 개인정보의 안전성 확보

「공공기관의 개인정보보호에 관한 법률」공공기관의 장은 개인정보를 처리하거나 개인정보파일을「전자정부법」제2조 제7호에 따른 정보통신망에 의하여 송·수신하는 경우 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 강구하여야 한다. 그리고 공공기관의 장은 개인정보의 처리에 관한 사무를 다른 공공기관 또는 관련 전문기관에 위탁할 수 있으며, 이 경우 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 취하여야 한다(법 제9조 제1항 내지 제2항). 이 조항은 개인정보 파일의 안전성, 정확성, 최신성의 확보는 손해배상 책임, 벌칙 등의 실효성 확보를 위한 방안이 뒷받침되지 않았기 때문에 선언적 조항의 성격에 불과하다.[379]

---

378) 박홍윤, 앞의 책, 122-123면.

공동이용에 의하여 기하급수적으로 증대하는 시스템의 안전성 문제를 해결하여 위하여 적절한 위기관리 시스템의 구축과 가외성 있는 시스템의 운영이 요구된다. 일반적으로 개인정보 유출의 대부분은 비인간적인 요인에 의하기보다는 인간에 의하여 더욱 많이 발생하고, 외부인보다는 내부인에 의하여 안전성이 위협되는 정도가 크다. 그러나 우리의 경우는 주로 비인간적인 것과 외부자의 차단에만 관심을 기울이고 있다. 개인정보공동이용체계 이외에 행정관리 차원에서 인적·관리적인 보안활동이 강화될 필요가 있다.[380]

다. 개인정보 이용

1) 공동이용의 제한

「공공기관의 개인정보보호에 관한 법률」에 의하면 보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니된다(법 제10조 제1항). 그러나 보유기관의 장은 일정한 경우에는 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있다. 다만, 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다(제10조 제2항).

그러나 여기서 '부당하게 침해할 우려' 여부는 당해 보유기관의 장에게 판단의 여지가 있다고 보아야 하기 때문에 법원에 의한 엄밀한 사법적 평가를 기대하기 어려운 것으로 보이고, 그 만큼 이 제한 요건은 개인정보의 남용을 통제하는 효과적인 장치로 보기 어렵다. 더구나「전자정부법」이 공동으로 이용을 강제하고 있는 규범상태에서는 더욱 그러하다.[381] 다음으로 예외사유 제10조 제2항 제1호 내지 제7호는 2007년 개정 전에는 제1호 내지 제8호까지였으나 2007년 개정으로 제8호는 삭제되었으며, 지금은 어느 정도 문제의 소지가 해결되었다. 그러나 제6호 범죄의 수사와 공소의 제기 및 유지에 필요한 경우에서 '필요성'은 인정되어야 하지만

379) 홍준형, 앞의 주 138), 26면.
380) 박홍윤, 앞의 책, 125면.
381) 이인호, 앞의 책, 213면.

법원의 엄격한 판단의 해석이 요구된다. 제7호의 법원의 재판업무수행을 위하여 필요한 경우로서 법원의 재판업무수행의 '필요성'은 법원의 제출명령이 있는 경우로 한정되어야 한다.

그리고 이 법에서는 보유목적을 넘어선 제3자 제공에 대한 절차를 달리 규정하고 있지 않다. 다만 이 법 시행령에서 보유기관은 임의로 제공할 수 없고, 수령기관이 그 이용목적 및 이용하고자 하는 정보처리의 범위를 명시하여 보유기관의 장에게 문서로 요청하도록 하고 있다. 그리고 이에 따라 제공하는 경우 보유기관의 장은 관련사항을 처리정보제공대장에 기록하고 이를 관리하여야 한다(시행령 제11조). 특히 보유기관의 장은 '정보통신망을 이용하여' 정보제공을 하는 경우에는 정보제공의 항목을 한정하고, 위 처리정보제공대장에 기록되는 사항을 행정안전부장관 또는 관계중앙행정기관의 장에게 통보하여야 한다(시행령 제12조 제1항)고 규정하고 있다. 그러나 이러한 절차적 제한만으로는 자기정보관리통제권의 헌법정신을 충족시키는 것은 아니다. 자기정보관리통제권에 포함된 정보주체의 인식명확성의 요건은 자신에 관한 정보가 어떤 법적 근거하에서 어떤 목적을 위하여 어떤 기관에 어떻게 이용될 것인지를 당해 정보주체가 명확하게 인식할 수 있을 것을 요구한다. 그러나 현행법에서는 정보주체 이외의 제3자에게 개인정보를 제공하는 경우 달리 정보주체의 동의를 받거나 그에게 통지하도로 요구하고 있지 않다.[382]

2) 의사결정의 제한

컴퓨터 기술의 발달은 하나의 커다란 오류를 만들고 있다. 많은 사람들은 컴퓨터는 언제나 정확하고 인간은 잘못을 범할 수도 있다는 생각을 가지게 하였다. 그 결과 우리의 조그만 실수가 개인의 삶에 막대한 영향을 미칠 수 있는 세계가 되어 버렸다. 따라서 인간은 종종 디지털 의사결정과정에서 철저히 소외되고 있다.

이용의 제한은 이러한 인간의 오류를 통제하기 위한 것으로서 크게 정당한 이용의 제한과 부당한 이용의 제한으로 구분될 수 있다. 반면에 주로 이용의 남용과 관련된 정당한 이용제한은 상대적으로 많은 연구와 통제가 이루어지고 있지 못하다. 그래서 개인정보공동이용 체계에는 개인정

382) 이인호, 앞의 주 213), 26-27면.

보 남용가능성이 확대되게 된다.

개인정보 이용체계에는 수집목적 외 사용증가로 비맥락적인 의사결정의 가능성이 증가한다. 이러한 문제를 해결하기 위하여 컴퓨터 매칭, 컴퓨터 프로파일링 및 신원조회 등과 같은 단순한 결과만 가지고 의사결정을 하는 것을 제한하는 메커니즘이 필요하다. 특히 공공기관이 관리하는 대부분의 개인 데이터의 정확성이 결여되어 있고, 질이 문제시되고 있는 상황에서 공동이용에 의하여 공공기관의 서비스 제공 여부를 결정하거나 규제의 대상으로 선정하는 것은 매우 신중을 요하는 부분이다.[383]

그러므로 이러한 공동기법을 활용하여 결정을 하고자 할 경우에 관련당사자에게 소명의 기회를 제공하는 절차적 제도가 마련되어야 한다.

라. 개인정보 통제

1) 책임 문제

「공공기관의 개인정보보호에 관한 법률」에 의하면, 공공기관의 장은 소관 처리정보의 보호 및 관리를 위하여 개인정보관리책임관을 지정하여야 한다. 개인정보관리책임관의 자격요건·지정 및 운영 등에 관하여 필요한 사항은 대통령령에 위임하고 있다. 그러나 전자적 방법을 통한 정보의 공동이용에서는 개인 데이터를 공동으로 이용하고 목적 외 이용이 증가됨으로써 발생하는 문제에 대한 책임소재를 명확하게 설정하기가 곤란하다. 특히 네트워크화는 기밀정보에 대한 어느 한 조직을 책임을 감소시키고 다른 조직이나 컴퓨터에 책임을 전가시키는 경향이 있다. 공동이용의 사용자 환경은 온-라인 체계로 특정 지을 수 있다. 이 온-라인 체계에서 사용자는 데이터의 입력·출력·의사결정을 한 사람에게 집중되도록 하여 사용자의 책임이 더욱 증대하게 된다. 특히 최종 사용자의 윤리적인 책임이 커지게 된다고 할 수 있다. 이와 더불어 일선 관리자와 감독의 역할이 더욱 중요시되게 될 것이다.

그러나 현실적으로 컴퓨터 매칭, 프로파일링, 신원조회 등이 가장 많이 이루어지고 있고, 개인의 기본적인 권리를 침해할 위험이 가장 많다고 할 수 있는 국가정보원, 경찰, 검찰의 활동과 국세청의 활동이 공동이용 및

383) 박홍윤, 앞의 책, 128면.

예외적인 조항에 해당되어 무제한으로 이용될 수 있는 소지가 많다고 할 수 있다.[384]

2) 공개문제

자기정보관리통제권의 파생원칙인 시스템공개의 원칙은 '개인정보처리시스템의 설치여부, 설치목적, 정보처리방식, 처리정보의 항목, 시스템운영책임자, 처리시스템에 의한 자동결정이 이루어지는지 여부 등이 일반에게 투명하게 공개되어야 한다'는 요청이다.[385] 개인정보 데이터의 개발 및 활용 정책들을 일반에게 공개하기 위해서는 개인 데이터의 존재와 성격, 그리고 주요한 이용목적 및 데이터의 통제자를 명확히 하고, 권한과 책임의 소재를 명확히 해야 한다.

일반적으로 관료제의 특성 중의 하나는 특히 통제업무와 관련하여 법률에 의하여 그들의 활동이 통제되지 않는다는 것이다. 관료들은 법이나 시민단체의 가시와 같은 외적인 통제에 대하여 다양한 형태의 술책을 사용하여 시민단체들의 활동에 대한 통제력을 감소시킨다. 이러한 술책으로 들 수 있는 것이 자신들이 무엇을 행하는지를 명확하게 알리지 않는 방법이다. 또 다른 방법은 완곡어법을 사용하여 개인정보의 전산화와 이를 활용하는 것이다.[386]

우리의「공공기관의 개인정보보호에 관한 법률」도 시스템 공개에 대해 애매하고 포괄적인 예외를 지나치게 넓게 인정하고 있는 것으로 판단된다. 이 법률에 의하면, 개인정보파일을 보유하고자 하는 공공기관은 그 처리내역을 중앙행정기관의 장에게 통보하고, 관계중앙기관은 이를 종합하여 행정안전부장관에게 협의하도록 하고(법 제6조 제1항), 관계중앙기관과 행정안전부장관은 이들 처리내역을 연1회 이상 관보에 게재하도록 규정하고 있다(법 제7조). 또한 각 보유기관의 장은 그 처리내역을 개인정보파일별로 기재한 대장(개인정보파일대장)을 작성하여 일반인이 열람할 수 있도록 하여야 한다(법 제8조).

그러나 이러한 조항은 시스템공개에 대한 예외가 지나치게 넓다. 즉 일정한 유형의 개인정보파일은 관계중앙기관에의 통보 및 행정안전부장관에

384) 박홍윤, 앞의 책, 104-105면.
385) 이인호, 앞의 주 213), 27-28면.
386) 박홍윤, 앞의 책, 102-103면.

의 제출이 요구되지 않고(법 제6조 제1항), 따라서 관보게재에 의한 공고대상에서처음부터 제외되며(법 제7조), 일반인의 열람대장에서도 제외된다(법 제8조).

이 같은 광범위한 예외는 시스템공개의 원칙과 부합될 수 없다. 위 법률조항에 의한 통보, 공고 및 열람의 대상이 되는 정보의 구체적인 개인정보가 아니라 처리내역 정보이다. 이러한 처리내역 정보가 공개된다고 해서 개인의 사적정보가 공개되는 것이 아니다. 오히려 처리내역정보의 공개는 국가기관에 의한 은밀한 개인정보처리를 막음으로써 개인의 인격과 존엄을 보장하고 민주적 정부운영을 위한 기본적인 전제조건이다. 따라서 중대한 공익에 의해 불가피한 사정이 존재하지 않는 한, 모든 개인정보처리시스템의 운용 및 활용상황이 일반에게 공개되어야 한다. 따라서 위 법률조항의 예외는 정당화되기 어려운 것이다.

더 나아가 이 법 제12조에서는 정보주체는 개인정보파일대장에 기재된 범위 안에서 본인에 관한 처리정보의 열람을 청구할 수 있도록 되어 있다.[387] 이 규정은 공공기관의 처리에 대하여 당해 정보주체 및 사회일반에게 감시의 기회를 제공함으로써 자기정보관리통제권을 구체화하고자하는 이 법의 취지를 무색하게 만드는 것이다. 또 이 규정의 범위 밖에 있는 개인정보파일에 탑재되어 있는 본인과 관련된 개인정보의 처리에 대하여는 결국 처리한 내역을 공개하지 않겠다는 뜻인데, 이 경우에는 국가기관이 개인에 대한 감시 또는 비밀리에 조사한 내역에 대해서는 정보주체인 당사자에게 공개하지 못할 합당한 이유를 밝혀야 할 것이다. 이러한 점에서 본다면 국가는 시민이 전혀 알지 못하는 상태에서 국가가 개인정보를 자유롭게 처리할 수 있고 그에 대한 아무런 책임도 지지 않겠다는 것이다. 이는 시스템 공개의 원칙을 위반하여 자기정보관리통제권을 위헌적으로 침해하고 있는 것이 아닌가 하는 생각이 든다.

3) 개인 참여 문제

정보의 주체는 정보의 통제자 또는 관리자로부터 자신과 관련된 자료를 얻거나 그 밖에 자신에 관한 정보를 데이터 통제자가 가지고 있는지를 확인할 권리를 가지고 있어야 한다. 또 데이터 통제자는 정보주체의 공개

387) 이인호, 앞의 책, 28-29면.

또는 열람청구에 응할 의무를 져야 한다. 이때 통제자가 공개를 거절하면 이의신청을 할 수 있는 권리가 있어야 하며, 이의신청이 합당할 경우에 데이터를 삭제, 수정, 보완, 정정할 권리가 주어져야 한다. 그러나 개인정보의 전산처리는 조직이 개인에 대하여 보다 많은 권력을 행사하게 하고, 결정이 내려진 맥락을 이해할 수 없도록 하기 때문에 개인은 결정이 이루어진 후에야 비로소 부당한 처리가 있었음을 알게 되거나 혹은 모르고 지나간다.

기존의 프라이버시 보호를 위한 법률체계들은 개인에게 자신의 정보를 보호하도록 많은 책임을 부여한다. 그러나 조직의 개인정보의 전산화와 통합관리는 개인의 책임과 개인의 조직을 감시하는 능력간에 격차를 증대시킨다. 이러한 불균형은 개인의 자기정보에 대한 통제권 행사를 더욱 어렵게 할 것이다. 개인통제의 전제인 알 권리와 관련하여 개인정보의 조직간 이동의 확대, 목적 외 이용 가능성의 확대는 조직에서의 개인정보의 처리와 이용에 대한 개인의 인지를 더욱 어렵게 한다. 특히 온-라인에 의한 프런트 엔딩(front-ending)이나 다른 응용기술의 활용은 개인정보의 교환 규모 및 속도에 있어서 급격한 변화를 초래하기 때문에 개인이 자신의 정보가 어떻게 사용되고 있는지를 모니터 한다는 것은 거의 불가능하게 된다.

더욱이 컴퓨터 매칭이나 프로파일링의 기법은 법체계 내에서 개인의 권리를 보호하는 합법적인 절차를 위반할 가능성을 확대시킨다고 할 수 있다. 이에 의하여 개인 의사결정이 이루어진 후에야 개인이 부당한 처리를 당했음을 알게 될 것이다.[388] 이러한 환경에서는 개인의 참여기회는 박탈당할 것이고, 참여민주주의 여망은 점점 소원해지는 것이다.

2. 자기정보관리통제권의 확보방안

가. 개인정보관리통제와 사전 동의

정보통신기술의 발달로 데이터베이스화된 개인정보는 정보주체도 인식하지 못한 상태에서 정부나 기업의 수준에서 수집, 처리, 이용, 제공될 수

388) 박홍윤, 앞의 책, 103-104면.

있게 되었다. 개인정보를 축적 처리하는 기관은 개인에 대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이다. 그리하여 이들 개인정보를 토대로 개인의 성향과 동태를 파악할 수 있다. 이것은 때로 특정 부류의 사람들에 대해 사회적 낙인을 가능하게 만들고, 이를 통해 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수도 있다.

따라서 개인정보공동이용에 있어서 정보처리의 위험성과 필요성 사이의 균형을 맞추는 일은 매우 중요한 과제라 할 수 있다. 그 균형추로서 기능하는 것이 헌법에서 보장하는 '자기정보관리통제권'이라는 정보인권이다. 이를 통해 정보주체는 자신에 관한 정보가 누구에 의해 어떤 목적으로 어떻게 수집・이용・제공되는지를 명확하게 인식하고 그러한 정보처리의 과정에 함께 참여할 수 있어야 한다.[389]

「공공기관 개인정보보호에 관한 법률」은 공공기관의 장은 사상・신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다(법 제4조 제1항)고 규정하고 있다.

하지만 이러한 정도의 내용으로는 사실상 어는 정도가 현저하게 인권을 침해하는 것인지, 언제 자신의 정보를 수집하는지 전혀 알 수가 없는 일반 추상적인 규정이라 할 수 있다. 또 정보주체가 사전 동의 없이 자신의 정보가 수집되었다고 하더라도 재판을 받아보지 않고는 그 사전 동의의 대상을 확정할 수 없는 상태라 할 것이다. 이러한 권리는 개인정보의 취급에 있어서 정보수집 당시의 동의권과 제3자 제공시 동의권을 분리하여 정보취급자의 의무를 통해 확보되어야 하기 때문에 이는 정보취급자의 의무규정으로 다루어야 할 사안이다.

현재로서는 공공기관에서 개인정보처리 과정에서 침해문제가 있을 경우, 개별적으로 개인정보침해에 대한 행정심판을 요구하거나 또는 시민단체 등을 통해 소송을 제기함으로써 공공기관의 개인정보보호조치에 대한 구제절차 및 감시와 평가가 이루어지고 있다고 할 수 있다.

389) 윤영민, 개인정보와 사생활의 비밀과 자유 보호를 위한 정책 연구, 한양대학교, 2004, 8면.

나. 개인정보 정정·삭제 절차 개선

「공공기관의 개인정보보호에 관한 법률」은 제12조에 따라 본인의 처리정보를 열람한 정보주체는 보유기관(다른 기관으로부터 처리정보를 제공받아 보유하는 기관을 제외한다. 이하 이 조에서 같다)의 장에게 문서로 당해 처리정보의 정정 또는 삭제를 청구할 수 있다. 다만, 다른 법률에 당해 처리정보가 수집대상으로 명시되어 있는 경우에는 그 삭제를 청구할 수 없다. 보유기관의 장은 제1항의 규정에 의한 정정 또는 삭제청구를 받은 때에는 처리정보의 내용의 정정 또는 삭제에 관하여 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다. 보유기관의 장은 제2항의 규정에 의한 조사를 함에 있어 필요한 때에는 당해 청구인으로 하여금 정정 또는 삭제청구사항의 확인에 필요한 증빙자료를 제출하게 할 수 있다(법 제14조 제1항 내지 제3항)고 규정하고 있다. 또 조사결과 정보주체의 정정요구에 이유가 없다고 판단되면 거부처분에 대한 불복신청의 방법을 통지해야 할 것이다.

또 개인정보의 저장이나 보유가 허용되지 않거나 정보보유자의 직무수행에 더 이상 필요하지 않게 되는 경우에는 정보주체는 정보보유자에게 자신에 관한 정보를 차단해 줄 것을 청구할 수 있다. 정보주체의 이러한 청구에 이유가 있는 경우에는 정보보유자는 그에 따라야 한다. 하지만 법적으로 혹은 현실적으로 삭제가 불가능 하거나 곤란한 사정이 있는 경우에는 정보주체의 삭제 청구에도 불구하고 정보보유자는 그 정보를 차단할 수 있을 것이다. 만일 보유하고 있는 개인정보에 대해 정보주체가 정확성 여부에 관하여 이의를 제기하고 그것이 정확한지 여부를 확인할 수 없는 경우에도 그 정보는 차단되어야 할 것이다.[390]

다. 개인정보보호 사전영향평가제도 도입

전자정부에서의의 개인정보 및 프라이버시 보호를 위해서는 무엇보다도 개인에 대한 프라이버시 침해가 있기 전에 이를 미연에 예방할 수 있는 장치를 마련하는 것이 중요하다. 특히 행정정보공동이용 활성화로 개인정

390) 독일 연방데이터보호법 제20조 제2항 내지 제4항 참조; 권건보, 앞의 책, 121면.

보공동이용도 또한 급증함에 따라 대량의 개인정보를 보유하고 있는 정부기관에 의한 개인정보의 오·남용과 그에 따른 프라이버시 침해 가능성으로 인해 정보화사업에 대한 일반 국민의 관심은 그 어느 때보다 높다고 할 수 있다. 또한 세계적인 추세도 앞다투어 전자정부의 구축과 아울러 프라이버시 영향평가제도를 도입하고 있는 실정이다.

먼저 사전영향평가제도는 북미에서 시작되어 그 용어가 프라이버시영향평가(Privacy Impact Assessments)로 사용되는 경우가 많기 때문에 여기서는 프라이버시 영향평가로 사용한다. 프라이버시 영향평가제의 도입에 관해서는 도입의 절차에서부터 적용방법 등 많은 문제들이 있지만 여기서는 간략하게 의의 정도만 살펴보고 프라이버시 영향평가제도가 먼저 시작되고 현재 잘 이용되고 있는 캐나다와 미국의 예와 우리나라의 도입에 관하여 논하기로 한다.

1) 사전영향평가제의 필요성

프라이버시 영향평가를 실시함으로써 정보화사업 계획단계에서부터 개인정보 및 프라이버시 보호를 위한 대책을 사전에 마련하게 되면, ① 정부기관에 의한 개인정보 및 프라이버시 침해 가능성을 처음부터 최소화할 수 있고, ② 이를 통해 정보화에 대한 일반 국민의 불신감을 해소할 수 있으며, ③ 정보화사업이 추진된 후에 개인정보 등의 침해를 이유로 당해 정보화사업을 도중에 중단하거나 변경하게 됨으로써 발생하는 국가예산의 낭비를 미연에 방지할 수 있다.

2) 프라이버시 영향평가의 개념[391]

프라이버시 영향평가(Privacy Impact Assessments)라 함은 정부기관이 각종 정보화사업을 추진하는 과정에서 개발하거나 도입하게 되는 정보시스템 등이 개인정보의 수집 및 관리 등의 업무와 밀접한 관계가 있는 경우, 당해 정보시스템 등이 개인정보와 프라이버시에 어떠한 영향을 미치는지를 파악하여 프라이버시 침해 여지가 있다고 판단되는 경우, 사전에 그 대책을 마련함으로써 정부기관에 의한 프라이버시 침해 가능성 자체를

391) 이에 관해서 자세한 설명은 구병문, "프라이버시 영향평가제도 도입의 쟁점과 추진방향", 서울대학교행정대학원 한국정책지식센터, 2004, 1-8면 이하 참조.

최소화하는 일련의 절차를 말한다. 현재 우리나라는 개인정보의 수집, 관리, 이용 등 개인정보의 취급 전반에 관해서는「공공기관의 개인정보보호에 관한 법률」등에서 이를 규정하고 있으나 그 이전 단계인 개인정보 관련 정보시스템의 도입 및 개발 등에 대해서는 별도의 프라이버시보호 장치를 마련하고 있지 않다.

3) 프라이버시 영향평가의 대상

프라이버시 영향평가는 원칙적으로 개인정보 또는 프라이버시와 관련된 모든 정보화사업을 대상으로 하여야 한다. 다만, 현실적으로는 프라이버시 영향평가제도의 신규 도입에 따른 시행착오나 기타 각 기관의 수행능력 등을 고려할 때 모든 정보화사업에 대하여 프라이버시 영향평가를 실시한다는 것은 사실상 불가능한 일일 수 있다. 그러나 적어도 전자정부 로드맵 31대 과제와 같이 주요한 전자정부사업에 대해서는 반드시 프라이버시 영향평가를 실시하여야 할 것이다.

한편 개인정보뿐만 아니라 법인, 단체 등에 관한 등록 및 관리정보 등과 같은 기업 비밀이나 업무상 비밀에 미치는 영향에 대해서도 평가범위를 확대할 필요가 있다. 특히 전자정부가 활성화되면서 개인정보는 물론 이거니와 기업 등에 대한 대량의 업무상 비밀정보가 공공기관에 의해 전자적으로 수집·관리되고 있어 각종 역기능이 적지 않게 나타나고 있다. 이러한 현실에 비추어 볼 때 영업상·업무상 비밀에 대해서까지도 프라이버시 영향평가를 실시하는 것은 그 타당성이 충분히 인정된다고 할 수 있다. 따라서 각종 법률 등에 의해 보호되는 영업상·업무상 비밀 등에 대해서도 영향평가의 적용범위를 확대하는 방안을 검토할 필요가 있다.

4) 프라이버시 영향평가의 내용

기본적으로 프라이버시 영향평가는 수집 및 처리되는 개인정보의 내용 그 자체에 관한 사항, 당해 개인정보를 수집하는 이유 및 용도, 개인정보 공동이용·공개·제공의 대상 및 범위, 개인정보의 주체 또는 관련 당사자의 개인정보 수집·이용 등에 관한 동의 확보 여부 또는 그러한 사실에 대한 고지 여부, 개인정보 및 프라이버시 보호를 위한 관리적·기술적 대책, 프라이버시 보호에 관한 법령의 준수 여부 등을 중심으로 개인정보

및 관련 정보기술의 관리 프로세스 전반에 걸쳐 종합적으로 이루어져야 한다.

5) 입법방식

프라이버시 영향평가제도를 법제화하는 방법으로는, 현행「공공기관의 개인정보보호에 관한 법률」과 같은 프라이버시 보호 관련 법률에 명문 규정을 두는 방법,「전자정부법」등 정보화사업추진 또는 정보시스템 관리 관련 법률에 명문 규정을 두는 방법,「환경·교통·재해 등에 관한 영향평가법」과 같이 별도의 단독 법률로 제정하는 방법 등이 있다.

필자의 견해로는 만약 우리나라가 프라이버시 영향평가제를 도입한다면 현재의「공공기관의 개인정보보호에 관한 법률」이 공공기관 개인정보보호법이기는 하지만, 개인정보의 침해 문제가 가장 많이 발생하는 것은 전자정부 운용에 따른 공공기관의 행정정보공동이용에서 발생하므로 미국에서처럼「전자정부법」에 명문규정을 둘 수도 있겠지만, 아마도 가장 이상적인 방법은 행정정보공동이용법을 제정하여 그 법률의 규정에 명문을 두어 활용하는 것이 좋은 방법이라 생각된다.

라. 캐나다의 프라이버시 영향평가제도

1) 개요

캐나다는 최초로 프라이버시 영향평가제도를 도입한 나라이다.[392] 캐나다는 프라이버시와 관련된 내용이 포함된 모든 연방정부기관의 프로그램과 서비스에 대해 정보영향평가를 의무화하고 있다. 캐나다 프라이버시 영향평가의 특징은 프로그램의 설계와 개선과정에서 프라이버시와 관련된 문제를 확인하고 해결하기 위한 일관된 분석틀을 제공하는데 있다.[393]

---

392) 이에 관하여는 Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners-Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online, in Global Internet Policy Initiative, (2003), p.7; 홍준형, 앞의 주 138, 142-148면 참조.

393) 캐나다에서 프라이버시 영향평가제도를 도입하게 된 배경은 다음과 같다. ① 정부기관은 당해 기관이 제공하는 프로그램 및 서비스 구상, 분석, 고안, 개발, 시행 및 사후 검토에 이르기까지 전 과정에 걸쳐 개인정보의 수집, 이용 및 공개 등과 관련하여 프라이버시법 및 프라이버시 보호원칙을 준수하고 있음을 명백히 밝힐 책임이 있다. ② 정부기관은 또한 개인정보의 수집이유, 이용 및 공개방법 등에 관하여 일반 국민과 지속적으로 의견을 교환해야 하며, 신

2) 내용 및 특징

영향평가의 주체는 각 정부기관이다. 이들 정부기관이 평가하는 대상은 원칙적으로 정부기관이 제공하는 모든 프로그램 및 서비스이다.[394] 그러나 이 정책의 시행 전에 추진된 프로그램이나 서비스의 경우에는 전자정부의 특성상 개인정보의 수집, 이용 또는 공개되는 형태 등에 있어 본질적인 부분에 대한 변경이 있는 경우에만 프라이버시 영향평가가 적용된다.

캐나다의 프라이버시 영향평가제도의 주요 특징은 ① 프라이버시 영향평가제도를 내용으로 하는 별도의 법률 제정 없이 프라이버시에 관한 일반법을 근거로 하여 정책적으로 프라이버시 영향평가를 실시하도록 하고 있다. 그러나 이는 국가기관 및 공공기관에 대한 강제력은 어느 정도 담보할 수 있으나, 대국민 권리보호 차원에서는 그 정도가 미흡하다는 단점이 있다. ② 보다 간소한 절차의 예비적 프라이버시 영향평가를 통해 프라이버시 영향평가가 실시에 따른 불필요한 예산낭비 및 사업지연 등을 방지하고 있다. ③ 정책, 기술 전문가 등 프로그램 및 서비스 관련자들에

규 프로그램 및 서비스를 제공하는 경우에는 동 프로그램 및 서비스가 프라이버시에 미치는 영향 및 그 해결방안에 대해 설명할 책임이 있다. ③ 따라서, 프라이버시 영향평가 정책 및 지침을 발표 및 시행함으로써 정부의 프로그램이나 서비스의 구상에서부터 시행에 이르기까지 모든 단계에 걸쳐 프라이버시가 보호되도록 하고, 프라이버시 문제에 대한 이해를 바탕으로 철저한 검증을 거쳐 정책이나 시스템 등을 도입할 수 있도록 정책결정자에 대하여 필요한 정보를 제공하고, 사업추진 후에 프라이버시 보호를 이유로 사업을 중단하거나 변경하는 위험을 감소시키고, 정부기관이 이용하는 개인정보와 관련된 업무절차 및 흐름을 문서화하여 일반 국민관의 대화를 위한 기초 자료로 활용하고, 프라이버시위원회 및 일반 국민에 대하여 프라이버시 침해 가능성이 있는 신규 또는 변경된 프로그램 및 서비스 계획에 대한 정보를 제공하여 프라이버시 보호에 관한 인식을 고취시킬 필요가 있다: 구병문, 프라이버시 영향평가제도의 국내법적 도입방안-공공부문의 중심으로, 제3회 개인정보보호 정책 포럼 자료, 2004.6, 8-11면.

394) 이에 관하여 캐나다 프라이버시 영향평가 정책 및 지침은 프라이버시 영향평가가 필요한 경우로서 ① 개인의 동의 여부를 불문하고 개인정보를 신규로 수집, 이용, 공개하거나 기존 개인정보의 수집, 이용, 공개 범위를 확대하는 경우 ② 개인정보 수집대상을 확인하는 경우 ③ 개인정보 수집방법을 직접적인 방법에서 간접적인 방법으로 변경하는 경우 ④ 프로그램의 통합, 관리 등을 목적으로 개인정보의 수집을 확대하는 경우 ⑤ 프로그램간, 정부기관간, 공공·민간부문간 개인정보의 정확성을 유지하기 위한 경우 또는 이를 공동 이용하는 경우 ⑥ 공통된 개인식별자를 신규 개발하거나 사용을 확대하는 경우 ⑦ 개인정보의 문리적·논리적 구분과 관계있는 업무절차나 업무시스템 또는 개인정보에 대한 접근을 관리 및 통제하기 위해 사용되는 보안체계에 중대한 변화가 있는 경우 ⑧ 계약 등을 통해 프로그램이나 서비스를 다른 정부기관이나 민간부문으로 이전하는 경우 등을 들고 있다.

대해 공동책임을 부담시킴으로써 대국민 프라이버시보호에 관한 책임을 강화하고 있다.[395]

마. 미국의 프라이버시 영향평가제도

1) 개요

미국은「2002년 전자정부법」에서 '개인적으로 확인가능한 정보를 수집하거나 이와 관련된 기술을 채택하고 개발하기 전에 연방정부 기관 프라이버시 영향평가를 실시하여야 한다. 이에 따라 각 정부기관은 일반 개인으로부터 신원확인이 가능한 정보를 수집하거나 이와 관련된 정보시스템 등을 개발·조달하는 때에는 수집되는 개인정보와 그러한 정보를 수집하는 이유 및 그 용도, 수집된 개인정보를 공유하고자 하는 대상과 정보보호에 관한 사항 등에 대하여 프라이버시 영향평가를 실시하고 평가결과는 평가의 대상이 된 개인정보의 성격 등에 비추어 가능한 범위 내에서 웹사이트나 연방관보 등에 최대한 공개하고, 전자정부 기금의 출연이 필요한 경우에는 관리예산처(OMB)에 평가결과를 제출하여야 한다.[396]

2) 내용 및 특징[397]

프라이버시 영향평가의 주체는 모든 연방정부 기관이다. 여러 부처에 관련된 전자정부사업은 사업의 주관기관이 평가하도록 되어있다. 이들 기관이 평가해야 하는 개인정보는 정부기관을 대신하여 정보기술을 이용해 업무를 수행하는 자를 포함한 모든 정부기관이 보유한 것으로 신원확인이 가능한 개인정보로서, 특정 개인에 대하여 물리적 또는 온-라인 접속을 허용하는 신원확인이 가능한 모든 정보가 포함된다. 이러한 개인정보를 수집, 유지 및 관리 또는 유포하기 위한 정보기술을 개발하거나 개인정보를 새로이 수집하는 경우에는 프라이버시 영향평가를 한다. 다만, 당해 개인정보가 정부기관 내부 업무처리와 관계있는 경우에는 프라이버시 영향평가와 유사한 평가를 실시한 적이 있는 경우, 새로운 프라이버시 문제가 발생하지 아니한 경우에는 프라이버시 영향평가를 실시하지 않을 수 있

395) 이규정·구병문, 공공부문 프라이버시 영향평가제도, 한국전산원, 2003, 19-20면.
396) 구병문, 앞의 주 388), 3면.
397) 위의 책, 3-6면.

다.

이 법의 특징은 ① 모든 정부기관으로 하여금 전자정부사업에 대한 프라이버시 영향평가를 실시하도록 함으로써 전자정부에서의의 개인정보보호 및 프라이버시 보호를 강화하고 있다. ② 프라이버시 영향평가 기준 및 내용의 제시, 평가결과의 보고 등을 통해 각 정부기관에 대한 관리예산처의 프라이버시 보호·감독을 강화하고 있다. 특히, 영향평가의 결과를 전자정부 기금에 반영하도록 함으로써 프라이버시 영향평가의 실효성을 담보하고 있다. ③ 각 정부기관에 대하여 프라이버시 영향평가에 관한 자율권을 부여하되, 여러 부처의 전자정부사업은 주관기관이 프라이버시 영향평가를 실시하도록 함으로써 프라이버시 보호에 관한 책임소재를 명확하게 하고 있다.[398]

바. 우리나라에서의 프라이버시 영향평가제도 논의

자기정보관리통제권의 보장을 위한 절차적 보장으로서 프라이버시 영향평가제도의 도입 문제는 정보프라이버시보호법제에 관한 논의에서 가장 빈번하게 제기되는 강력한 주장 중의 하나이다. 정부가 정보화 정책이나 사업을 추진함에 있어 사전 계획 수립단계에서부터 정보프라이버시 또는 개인정보에 대한 영향평가를 실시하도록 하여 그 결과를 정책이나 제도에 미리 반영하도록 하는 제도가 필요하다. 또 이를 제도화함으로써 예기치 못한 사회적 갈등과 행정비용의 낭비를 미연에 방지할 수도 있다. 이러한 제도는 과연 필요한가, 필요하다면 어떤 방향으로 도입해야 하는가. 특히 주된 문제는 전자정부사업 추진시 기획 및 설계단계에서 개인정보침해영향 사전평가제를 실시해야할 것인지 여부이다.[399]

사전영향평가제도는 발생할 수 있는 개인정보침해의 사전예방제도로서 적은 비용으로 큰 효과를 거둘 수 있는 제도이다. 이 제도는 이미 성공한 선진국의 사례를 충분히 검토하여 우리 실정에 맞게 적용하여 개인정보침해를 최소화할 수 있는 제도라고 생각한다. 해외 각국은 사전영향평가제도를 명문으로 별개의 항목으로 규정하기도 하고, 보호기구의 권한 부분에 포함시켜 규정하기도 하였다. 우리의 경우는 개인정보보호에 관한 기

398) 이에 관한 자세한 설명은 홍준형, 앞의 주 138), 142-148면 참조.
399) 위의 책, 147면.

본법이 제정되지 않고 공공부문과 민간부문으로 분리하여 개인정보를 개별적으로 보호하고 있다. 그리고「전자정부법」은 행정정보공동이용을 주된 업무로 하여 개인정보를 공동으로 가장 많이 활용하고 있지만, 정작 개인정보보호에 관한 사항은「공공기관의 개인정보보호법」에 일임하고 있다. 이러한 이원화된 체계로서는 행정정보공동이용 환경에서 개인정보보호가 제대로 이루어지기는 어렵다. 따라서 개인정보를 보호하기 위해서는 행정정보공동이용을 위한 법을 제정하고, 그 법 조항에 사전영향평가 내용을 규정하는 것이 가장 효율적인 방법이라 생각한다.

사. 개인정보보호기구 설치

1) 개인정보보호기구 설치의 필요성

개인정보보호를 위한 훌륭한 법제가 잘 정비되어 있고 개인의 권리를 충분히 법적으로 보장하고 있다고 하더라도 그 법제운용이 미숙하거나 권리실현이 사실상 불가하거나 어려운 경우 개인정보보호의 이념은 충분히 실현될 수 없다. 그리하여 선진국들은 앞다투어 이러한 문제점들을 보완하여 개인정보를 보호하기 위하여 독립된 개인정보보호기구를 설치하고 있다. 물론 법률규정에 자기정보에 대한 열람청구권 등 자기정보관리통제권을 형식적 내지는 구체적으로 보장하고 있다고 하더라도 그 실현을 위한 이니셔티브(initiative)는 각 정보주체에게 있기 때문에 일정한 한계를 지닐 수밖에 없다. 감독기구설치의 필요성과 존재이유를 정리하면 다음과 같다.[400]

① 개인정보보호와 관련한 문제의 심각성은 당해 정보주체가 인식하지도 못한 상태에서 개인정보가 정부나 기업에 의해 광범위하게 수집・축적・처리・제3자 제공 내지 공유되고 있다.

② 설령 개인정보처리의 원칙 중 수집제한의 원칙과 시스템공개의 원칙이 잘 지켜져 개인정보의 수집과 처리에 대한 정보주체의 인식이 있었다 하더라도, 처리기관 내부에서 이루어지는 위법적인 상황을 외부자인 정보주체가 충분히 파악할 수 없을 뿐만 아니라 조사할 수도 없다. 기술적으로 복잡한 처리 과정이나 은밀하게 이루어지는 목적 외 이용 및 제3자 제

400) 이에 관한 자세한 설명은 이인호, "개인정보보호를 위한 감독기구의 설립방향", 국회도서관보 제45권 제9호 통권 제352호, 국회도서관, 2008, 28-29면 참조.

공에 관한 상황을 외부의 비전문가인 정보주체가 제대로 알 수 없기 때문이다.

③ 더 나아가 설령 그것을 정보주체가 충분히 파악했다고 하더라도, 자신의 노력과 주도하에 법원을 통한 그 복잡하고 장기적인 소송절차를 밟아서 권리구제를 받는다는 것은 결코 쉬운 일이 아니다. 또한 법원을 통한 권리구제는 언제나 사후적인 것이고, 이에 따르는 비용이나 시간을 감당할 수 있어야 가능하기 때문이다.

④ 정보의 공동이용환경에서 개인정보의 적정한 이용을 허용하면서 동시에 다른 한편에서는 안전장치를 마련하여 정보주체의 권리나 이익이 함부로 침해되지 않도록 보호하여야 한다.

⑤ 감독을 하는 자와 감독을 받는 자가 기능적으로 분리되어야 함은 물론이고, 개인정보보호 기관은 감독기구와 피감독기구로부터 독립하여 독자적으로 감독업무를 수행할 수 있어야 한다. 개인정보보호의 가치는 개인정보처리를 통해 얻어지는 효율성의 가치와 본질적으로 양립하기 어렵다. 이 양 가치는 서로 상반된 관계에 있기 때문이다. 따라서 이 상반된 가치들은 단일의 특정기관과 함께 추구한다는 것은 사실상 불가능한 일이다. 어느 한 쪽으로 균형이 기울어질 수밖에 없다.

⑥ 통상 개인정보 데이터베이스에 의한 개인정보처리는 특정 개인이 아니라 수많은 개인들을 대상으로 하는 것이기 때문에 위법적인 개인정보처리의 영향은 그들 모두에게 똑같이 미칠 수 있다. 따라서 위법적인 개인정보처리에 따르는 피해는 대규모적이고 집단적인 성격을 가진다.

2) 세계 각국의 독립된 감독기구의 설치 현황

유럽연합은(EU)은 개인정보보호 일반법인「1995년의 개인정보보호지침(Directive 95/46/EC)」에서 회원국으로 하여금 개인정보의 수집・관리・이용활동 등을 모니터하고 조사할 수 있는 권한을 가진 독립적인 기구를 설치하도록 의무화하고 있다.

유럽평의회(Council of Europe)의 개인정보보호협약의 2001년 추가의정서는 그 전문(Preamble)에서 효율적인 개인정보보호를 위한 한 요소로서 완전히 독립적인 기능(functions in complete independence)을 수행하는 감독기구(Supervisory authorities)가 필요함을 인정하고 있다. 따라서 이

의정서 제1조에 “각 가입국은 이 협약 제2장 및 제3장, 그리고 이 의정서에 규정된 원칙들을 구현하는 국내법상의 조치들을 준수하도록 하기 위하여 그에 대한 책임을 지는 한 개 또는 그 이상의 감독기구를 마련하여야 한다”고 규정하고 있다.

그리고 국제연합(UN)은 1990년 12월 14일 총회결의로「컴퓨터화된 개인정보파일의 규율에 관한 가이드라인(Guidelines for the Regulation of Computerized Personal Data Files)」을 채택・공포하였다. 이 가이드라인은 모두 10개의 개인정보보호원칙을 담고 있는데, 그 중 8번째 원칙(감독과 제재)에서 “위에 열거된 원칙의 준수여부를 감독할 독립된 기관을 설치하여야 하고, 이들 원칙이 위배된 경우에 적용할 수 있는 처벌규정 및 개인보호규정을 제정하여야 한다”고 하여 개인정보보호원칙을 감독할 독립된 기관의 설치를 요구하고 있다.

위와 같은 요구에 부응하여 세계 각국은 유럽연합 개인정보보호지침(95/46/EC)의 영향하에서 공공부문과 민간부문을 통합하여 감독하는 단일의 개인정보감독기구를 설립하는 추세를 보이고 있다. 이 추세는 비단 유럽연합이나 유럽평의회 회원국에 한정되는 것이 아니고 비회원국들도 새로운 개인정보보호법을 제정하면서 독립된 통합기구를 설립하고 있다.

3) 우리나라에서의 도입 논의

우리나라 현행법에서는 개인정보의 이용촉진과 규제사항이 동시에 규정되어 있고, 입법 목적이 혼재되어 있을 뿐만 아니라 거기에 따라 각 담당부서에 이중적 역할이 부여되어 있다. 특히 행정안전부나 정보통신부는 자신의 영역에서 개인정보의 보호 및 감독을 위해 자기 산하의 기존 기구를 강화하는 방식을 제시하고 있다. 그러나 이것은 정보이용촉진과 개인정보보호 임무라는 두 역할을 동시에 갖는 것을 의미한다. 이와 같이 실행 및 집행부서가 감독의 권한까지 갖는 것은 권한의 집중을 불러일으키고, 따라서 개인정보처리의 감독 역할을 제대로 수행할 수 없게 된다. 즉, 창과 방패를 동시에 갖게 해서는 아니된다. 오히려 외부에 규제 권한을 부여함으로써 해당 공공기관에 대한 경쟁과 견제의 역할을 수행할 수 있도록 하여 견제와 균형을 이루어야 한다.[401]

401) 윤영민, 앞의 주 386), 22면.

지난 17대 국회에 발의되어 자동폐기된 3건의 개인정보보호법안들은 개인정보감독기구의 독립성을 확보하기 위하여 개인정보보호위원회를 국무총리소속하에 두거나, 국가인권위원회 성격의 독립성을 제안하고 있었다. 다시 2008년 6월 27일 행정안전부가 개최한 제1차 개인정보보호법(안) 공청회에서 제시된 법안설명에서는 행정안전부장관이 개인정보보호법의 집행 및 감독책임을 지는 주무부처이고 그 소속하에 분쟁조정기능만을 주된 업무로 하는 개인정보분쟁조정위원회를 두도록 하고 있었다.[402] 이에 대해 진보넷 등의 시민단체와 일부 논자들은 법안이 개인정보보호감독기구의 독립성을 포기한 것이라고 비판하였다. 비판의견을 수렴한 행정안전부는 같은 해 8월 12일「개인정보보호법 제정법률(안)」을 정식으로 입법예고하고 8월 28일 제2차 공청회를 열었다.

입법예고된 법률안에 의하면, 여전히 행정안전부장관이 집행 및 감독을 책임지는 주무부처이고 개인정보분쟁조정위원회가 분쟁조정기능을 수행하되, 몇 가지 사항에 대해 심의기능을 하는 개인정보보호위원회를 신설하여 국무총리 소속하에 두는 것으로 하고 있다. 이 법안의 개인정보보호위원회를 개인정보감독기구라고 볼 수 있는지, 그리고 법안상의 집행 및 감독체계를 독립된 감독체계라고 볼 수 있는지가 문제[403]가 되고 있으며, 아직까지 이에 대한 어떠한 결말은 나지 않고 있다.

지난 2009년 12월 22일 국회에서 개인정보보호법 제정 논의가 지지부진한 가운데, 공공과 민간 영역에서 개인정보가 과도하게 수집, 유통되고 있어 이를 규제할 법제정비 등 대책이 시급하다는 지적이 나왔다. 국가인권위원회는 진보네트워크에 의뢰해 실시한 '개인정보 수집・유통 실태조사' 결과 보고회와 정책토론회를 열고, 공공, 경찰, 교육, 의료 등 사회 전반에서 개인정보 수집・유통, 제3자 제공이 방대하게 이뤄지고 있지만 개인정보보호를 위한 법체계가 미비한 영역도 존재해 시급한 법제정비가 요구된다고 밝혔다

이 연구 결과는 공공분야에서 추진되고 있는 정보화 사업에서 국민의 프라이버시와 개인정보보호 침해 우려가 크고, 독립적인 개인정보감독기구 필요성이 있다는 것이 강조됐다.

---

402) 행정안전부, "개인정보보호법 제정을 위한 공청회 자료집, 2008. 60. 27. 27면 참조.
403) 이인호, 앞의 주 398), 24면.

3. 관련 법제의 개선방안

지금까지 고찰한바, 전자정부 구축과 동시 전자행정을 위하여 행정정보 공동이용은 필수 핵심적인 사항이다. 문제는 그 행정정보 속에 있는 개인정보도 함께 이용하게 됨으로써 개인정보침해의 문제가 대두되었다. 그 중에서도 기본권에서 보장하고 있는 자기정보관리통제권을 어떻게 보장받을 것인가가 가장 큰 문제이다.

자기정보관리통제권은 정보처리의 모든 단계에서 정보주체가 자신에 관한 정보를 주체적으로 관리·통제할 수 있는 권리를 말한다. 여기에는 개인정보의 수집에 대한 사전 동의권, 자기정보 열람 청구권, 자기정보 정정·보완 청구권, 자기정보 삭제·사용중지·차단청구권, 개인정보의 제3자 이용제공에 대한 동의권 등을 포함하다. 전자정부 구축에 따른 행정정보 공동이용에 있어서 개인정보에 대한 자기정보관리통제권의 보장은 정보주체의 정보인권의 핵심으로서 이를 어떻게 보장할 것인가에 따라 전자정부의 성공여부가 달려있다.

자기정보관리통제권과 행정정보공동이용을 동시에 만족할 수 있을 것인가에 대해서 각국의 개인정보보호 입법례와 우리나라의 개인정보보호법제 등을 비교하여 고찰한바, 입법체계와 보장방식은 다소 차이가 있으나 개인정보 보장을 위해 노력하고 있다.

우리나라의 경우 행정정보공동이용에 있어 그에 관한 개인정보보호에 관해서는 사실상「공공기관의 개인정보보호에 관한 법률」에 일임하고 있는 셈이다. 따라서 우리나라의「공공기관의 개인정보보호에 관한 법률」은 행정정보공동이용을 위한「전자정부법」의 특별법 내지는 절차법의 역할을 하는 위치에 놓여 있다고 볼 수도 있다. 이러한 점에서 현행의「공공기관의 개인정보보호법」다음과 같은 내용으로 국제규범과 국내 실정에 맞는 수준으로 제정되어야 한다고 본다.

첫째, 현재의 이원적·부문별·개별법에 산재해 있는 법률체계는 민간부문과 공공부문을 통합하여 국제규범에 충족하며, 우리나라 실정에 맞는 일원적 통합기본법을 제정하고, 필요에 따라 새로 제정된 기본법에 근거하여 특별법 제정 또는 현행 개별법 조항을 활용할 수 있다.

둘째, 개인정보의 수집과 관련하여 ① 수집 목적의 정당하고, 수집절차는 합법적이어야 하며, 정보주체의 사전동의 내지는 분명한 인식하에서

수집되어야 한다.

셋째, 수집할 당시에 수집목적이 구체화되고 특정되어 있어야 하며, 이후에도 수집당시의 목적과 일치한 목적하에 사용되어야 한다.

넷째, 개인정보는 언제나 최신성, 적시성, 정확성을 유지하여 데이터의 질을 높여야 하고, 처리과정에 있어서도 부당하게 변경되거나 관리소홀로 훼손되어서는 아니된다.

다섯째, 민감정보와 비민감정보에 대한 분리처리의 원칙, 민감정보의 경우는 수집 또는 사용시 필히 본인의 자필서명으로 사전동의를 받은 후 수집 또는 제공하여 최대한의 인격을 존중해야 한다.

여섯째, 개인정보를 관리하는 정보보유자의 책임을 명확히 하여 적절한 관리가 이루어지도록 안전조치 또는 보안장치를 통하여 불법적인 접근·사용·공개 등의 위험으로부터 보호되어야 한다.

일곱째, 정보주체는 자신에 관한 정보의 소재에 자유롭게 접근하여 정보의 내용을 확인할 수 있어야 한다. 그리고 틀린 정보나 잘못된 정보는 수정·보완·삭제청구를 할 수 있어야 한다.

여덟째, 개인정보가 합법적으로 이용 또는 공동활용되었을 경우 정보주체가 통보를 받아 알 수 있어야 한다.

아홉째, 위와 같은 방법으로 개인정보를 공동 이용하였다면 처리정보의 결과에 대하여 일반에게 투명하게 공개되어야 한다.

열 째, 개인정보를 보호하기 위한 독립된 감독기구를 설치할 필요가 있다.

열한 째, 개인정보를 수집할 필요성이 존재하는지에 대한 사전영향평가제를 도입할 필요가 있다.

그리고 마지막으로 이 모든 조치를 다 취하였음에도 불구하고 개인정보의 유출사실이 확인되면 지체 없이 해당 정보주체에게 관련사실을 통보하여 피해의 확산방지 및 최소화할 수 있는 신속한 조치를 강구해야 한다.

제3절 자기정보관리통제권과 개인식별번호제도의 개선

1. 서설

정보사회에 있어서 자기정보관리통제권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 개인정보는 정보소유자 차원에서는 자기 자신을 의미하는 정보단위에 불과하지만, 국가 차원에서는 관리해야 할 주요한 자원이다. 그 이유는 오늘날 개인정보가 자원적인 특성을 지니고, 모든 국가는 자국민들에 대한 통계사항을 확보하고 관리하여 병력, 조세 등 국가 운영에 필요한 자원을 확보하기 때문이다.

날로 발전해 가는 정보통신기술을 발달에 힘입어 정부는 입력된 정보를 시공을 초월하여 처리·보관하게 되었으며 하루가 다르게 발전하는 정보기술을 활용함으로써 개인의 신상정보를 포함하여 각종의 정보를 데이터베이스화하고, 전문화된 관료조직을 활용하여 정보를 분석하고 처리할 수 있는 능력을 확보하게 되었다.

정보사회 이전의 근대민족국가는 국민 개인에 대한 정보수집과 일정 정도의 사회적 통제 메커니즘의 발전과 더불어 형성되었다. 국가는 그 형성과정에서 일반 대중을 국가라는 하나의 틀로 묶는 응집성과 통합성을 유지하기 위해 국민 개인에 대해 구체적인 정보의 수집과 관리를 해야 할 필요성이 절실했으며,[404] 그 수집된 개인정보를 이용하여 국가권력의 합법성과 권위를 유지해왔음을 부인할 수 없다. 즉, 국가는 하나의 행정단위로서 민족의 영토를 구성하고 규칙을 제정하고 강화하며, 법률과 질서를 유지하고, 자원할당에 대한 분쟁을 심판하며, 과세와 세출을 통하여 자원을 재배분하고, 자본주의 기업에 대하여 사회적·경제적인 산업기반을 제공하여야 하는데, 이 모든 것을 이루기 위해 국가는 국민을 감시·감독하는 능력을 필요로 하였다.[405]

더욱이 권위주위적 산업화 과정은 중앙집권적인 국가관료체제를 통해 시민사회의 성장을 억압하는 각종의 사회통제 메커니즘을 활용함으로써

404) 조화순, "정보사회의 국가권력과 개인정보 -한국의 전자주민카드 도입논의를 중심으로-", 한국정치학회보 제39집 제2호, 한국정치학회, 2005, 450면.

405) Reg Whitaker, The End of Privacy: How Total Surveillance Is Reforming A Reality, The New Press, New York, (1999), pp.40-41.

가능하였다. 즉 국가가 본연의 기능을 위해 국민의 정보를 필요로 하는 행위자임과 동시에 효율성을 우선시하는 전통 속에서 시민사회를 억압하는 통제자였다. 이와 같이 정부가 강력하게 국민 통제를 할 수 있는 수단은 국민이 개인의 신상정보를 법률에 의하여 의무적으로 국가에 등록하게 하는 '주민등록제도'였다.[406]

이 주민등록제도는 개인의 정체성을 식별하기 위해 성명, 생년월일, 성별, 주소, 사진 등을 많이 활용하였다. 그러나 이러한 것들은 얼마든지 중복되거나 변동될 가능성이 있다. 이러한 단점을 극복하기 위하여 개인마다 일련번호를 부여하는 방식이 고안되어 왔다. 흔히 이 일련번호를 개인식별번호(Personal Identification Number; PIN)라고 한다. 특히 모든 국민에 관한 데이터베이스가 같은 개인식별번호를 사용하여 구축되고 그 번호를 통해 다른 데이터베이스와 연결되어 각 개인의 신상정보를 검색할 수 있는 것을 표준통일식별번호(Universal Identification Number)라고 한다.[407]

우리나라 국민은 모두 이러한 표준통일식별번호에 해당하는 주민등록번호를 강제로 부여받고 있다. 이 주민등록번호는 부여 대상자 가운데 중복되는 경우가 없고, 평생에 걸쳐 변경되는 일도 없다. 또한 다양한 행정목적을 위하여 광범위하게 이용되고 있을 뿐만 아니라, 민간의 거래에 있어서도 주민등록번호의 기재나 고지를 요구받는 일이 일상화되어 있는 실정이다.

따라서 현행 주민등록번호제도하에서 개인은 항상 신원이 노출될 수 있는 위험에 처해 있다고 해도 과언이 아니다. 이는 모든 국민이 사실상, 잠재적인 감시와 관리의 대상이 될 수 있음을 의미한다.

2. 외국의 개인식별번호제도에 관한 비교법적 고찰

가. 개관

대부분의 국가에서는 우리나라의 주민등록번호와 같은 국민고유번호를

406) 조화순, 앞의 주 402), 451면.
407) 권건보, 앞의 책, 250-251면.

제도적으로 금지하고 있다. 또한 국가기관은 물론이고 민간기관도 신분을 나타내는 일련번호를 데이터베이스에서 인적사항을 추출하거나 여러 데이터베이스의 연결고리로 사용할 수 없도록 명시적으로 규정하고 있다.[408]

개인을 식별하기 위한 방법에는 이름, 외양, 생체적 특징, 사회적 특성, 증표(token-based identification), 번호 등이 있다. 이 중에서 개인식별번호 외의 식별방법은 효과적인 방법으로 활용하려면 여러 가지 어려운 점들을 각각 내포하고 있으므로, 인위적으로 부여한 개인식별번호가 현재 가장 널리 이용되는 방법이라 할 수 있다. 개인식별번호의 경우는 번호의 유일독자성을 확보할 수 있고 발급사항도 통제할 수 있다.[409] 전술한 바와 같이 개인식별번호가 사회에서 공통적으로 이용될 경우에는 이를 표준 통일식별번호라고 한다. 우리나라의 주민등록번호나 미국의 사회보장번호(Social Security Number: SSN), 스웨덴, 덴마크 등의 북유럽제국, 프랑스, 싱가포르 등 <표 16>에서 보는 바와 같이 주민등록제도 등을 기초로 본인확인제도를 구축하여, 개인식별번호를 다른 행정분야에서 활용하는 방식을 채택하고 있다.[410]

408) 정연수・김희은, “주민등록번호 도용의 문제점 및 개선방안”, 인터넷법제연구 제3권 제2호, 한국인터넷법학회, 2004, 199면.

409) Roger Clarke, "Human Identification in Information Systems : Management Challenges and Public Policy Issues", Information Technology & People, Vol. 7, No. 4, 6-37, (1994), p.13.

410) 이상명, “주민등록제도에 대한 헌법적 평가 -주민등록번호와 지문날인을 중심으로-”, 박사학위논문, 한양대학교 대학원 , 2007, 104면.

<표 16> 각국의 개인식별번호제도

국가명	번호의 종류	실시시기	부여대상자	부여주체	이용분야
미국	사회보장번호	1936년	전체시민, 영주권자, 노동허가 받은 외국인	사회보장청	세무, 사회보험, 연금, 운전면허 등
캐나다	사회보험번호	1964년	전국민	인재관리개발부	세무, 실업보험, 연금 등
덴마크	주민등록번호	1968년	전국민	내무성 중앙개인등록국	세무, 연금, 주민관리, 통계, 교육등
스웨덴	주민등록번호	1947년	전국민	국가조세위원회	세무, 사회보험, 주민관리, 통계, 교육 등
노르웨이	주민등록번호	1970년	전국민	등록청	세무, 사회보험, 주민관리, 통계, 교육 등
싱가포르	주민등록번호	1948년	전국민과 영주권자	내국인: 국민등록국, 외국인: 입국관리국	각종 행정분야
한국	주민등록번호	1962년	한국 국적을 가진 모든 자	행정안전부 (사무처리는 각 동사무소)	각종 행정분야
이탈리아	납세자번호	1977년	납세자	재정성	세무, 인허가 등
호주	납세자번호	1989년	소득세부과 대상자와 사회보장 수급자	국세청	세무, 사회보장 등

* 정연수・김희은, "주민등록번호 도용의 문제점 및 개선방안", 인터넷법제연구 제3권 제2호, 한국인터넷법학회, 2004, 204면 참조.

그러나 개인식별번호를 두고 있지 않은 나라에서도 대부분 효율적 행정을 위하여 이를 도입하고자 하는 시도가 끊임없이 나타났으며, 그때마다 각계의 반대여론에 직면하여 그 시도가 실패로 돌아가는 상황이 되풀이되었다.[411] 이하에서는 주요 국가들의 개인식별번호의 도입에 대한 논란과 현행 법제를 살펴보고자 한다.

나. 개인식별번호 인정국가

1) 프랑스

프랑스의 신분등록제도는 정부가 1946년 국립통계연구소(National

411) 권건보, 앞의 주 102, 258면.

Institute of Statistics and Economic Studies)를 설립하여 이 연구소에 주민등록업무를 담당하게 함으로써 시작되었으나,[412] 강제적인 주거등록 제도는 시행하지 않고 있었다.[413]

그런데 프랑스는 가장 일찍, 그리고 정열적으로 정보사회에 진입하고자 노력하였지만 프랑스 사람들은 새로운 정보통신기술이 개인의 자유 및 사생활에 미칠 수 있는 위험을 인식하였다. 그래서 1975년 언론이 모든 개인기록을 연결하려는 행정부계획을 보도한 이후에 공적·사적 영역에서 시민의 사생활 자유 및 다른 자유 등을 존중하는 정보처리발전을 보장하기 위한 위원회를 법무부에 설치하였다.[414]

그런데 재경부(the Ministry of Economy and Finance) 관할하에 있는 통계와 경제에 관한 국가조사청(the Institute of Statistics and Economic Studies)은 이미 약 5000만 명에 달하는 사람에 관한 정보를 담고 있는 국가신분(확인)기록(National Identification Register: NIR)을 갖고 있었다. 이 자동화된 국가신분기록은 국민들에 관한 기록을 저장하는 국가기록소로서 기능을 하기 시작하였다. 특히 프랑스에서 태어나는 모든 사람들에게 부여되는 13자리 숫자는 결국 국가적인 개인확인번호였다. 이와 같은 번호는 1970년대 말까지 행정부에서 다양한 목적으로 사용되었으나 1982년에 정부는 이러한 기록에 개인이름, 출생일과 출생장소, 姓, 개인확인번호만을 포함하도록 하고, 개인의 주소, 혼인 여부, 자녀의 이름 등을 제외시켰다. 따라서 다른 법률에서 이 기록을 사용하도록 허용하는 규정이 존재하지 않는 한, 이러한 기록은 어떤 개인을 찾기 위하여 사용될 수 없다.[415]

한편, 일련번호는 개인을 확인하는 수단으로 이용되는 것은 사실이지만, 이 번호는 사람에게 부여되는 것이 아니라 신분증에 부여되는 것이고 새로운 신분증을 발급할 때마다 새로운 번호가 부여된다. 따라서 각 개인에 평생 수반되는 고유식별인자로서 기능을 하지는 않는다. 또 일련번호에는 생년월일이나 성별 등의 인적사항 등을 추정할 수 있는 내용을 담을 수

412) David H. Flaherty, Privacy in Colonial New England, Charlottesville: Univ. Press of Virginia. (1972), p. 230.
413) 김일환, 앞의 주 233), 313-314면.
414) James Michael, Privacy and Human Rights, Dartmouth: UNESCO Publishing, (1994), p.65.
415) David H. Flaherty, supra note 410), p.229.

없도록 하고 있다. 그리고 공공부문은 물론 민간부문에 있어서도 그 일련번호를 데이터베이스에서 개인정보를 추출하거나 혹은 여러 데이터베이스 자료를 연결하는데 사용할 수 없도록 하고 있다.

이러한 프랑스의 주민등록 시스템은 강제적인 것은 아니어서 국민은 자발적으로 자신의 정보를 등록하고 개인식별번호를 부여받게 된다. 하지만 거의 대부분의 국민들이 주민등록 시스템에 등록하고 있다[416]고 한다.

2) 스웨덴

스웨덴의 주민등록제도는 30여년 전에 교회에 의해서 시작되었다. 오늘날 주민등록업무를 총괄하는 부서는 국세청이다. 스웨덴의 표준통일식별번호가 도입된 것은 국가적 차원에서 주민등록 시스템을 교체한 1947년의 일이다. 당시에는 생년월일 여섯 자리와 발급번호 세 자리의 숫자로 구성되어 있었다. 1976년 주민등록 시스템을 전산화하면서 뒤의 세 자리 숫자 앞에 하나의 숫자를 더 추가하였는데 이는 검증번호(check digit)로서 표준통일식별번호 입력시 발생할 수 있는 오류를 체크하기 위한 것이었다. 이에 따라 스웨덴의 표준통일식별번호는 YYMMDD-CXXX의 형태를 띠게 되었다. 이러한 표준통일식별번호는 주민등록제도에서 시작된 것이지만, 그 후로 많은 행정조직들이 행정업무의 효율성과 비용절감을 위해서 채용하기 시작했고, 조세·사회보장·병무행정 등에 광범위하게 사용되고 있다.[417] 어쨌든 스웨덴에서 일단 개인식별번호가 존재하게 된 이후로 원래의 목적과는 다른 목적을 위하여 사용되고 연결되었다. 이것은 개인식별번호가 일단 어떤 사회에서 존재하는 한 의회나 정보감독위원회가 그 사용을 제한한다는 것은 매우 어렵다는 것을 의미한다.

스웨덴에서 독특한 제도 중 하나가 정보감독위원회(DIB)의 지원하에 의회가 1976년 만든 SPAR(Register of Names and Addresses)이라고 알려진 정보 시스템이다. 이 정보 시스템이 설치됨에 따라서 개인의 성명과 주소를 국가적으로 기록하게 되었다. 본래 이러한 정보 시스템은 기업이

416) David Lyon, “British Identity Cards: The Unpalatable Logic of European Membership?”, 62 The Political Quarterly, 62(3), (1991), pp.377-385.

417) E. Hallman, “The Personal Identification Number System In Sweden”, in OECD, Policy Issues In Data Protection and Privacy, Paris: OECD Informatics Studies No. 10, (1976), pp. 106-111.

나 신용조사기관 등이 사적 영역에서 국민 전체에 관하여 조사하고 기록할 위험성을 통제함으로써 개인의 사생활을 보호하고자 한 것이었다. 그러나 역설적으로 이러한 정보 시스템은 실제로 단일한 국가정보은행이기 때문에 거꾸로 국민을 감시할 능력을 확대한 결과가 되었다. 이에 따라서 개정된「정보법」은 정보 시스템에 관한 규정을 두고 있다.[418] 이 규정에 의하면 정당한 목적들을 위하여 특정한 개인정보를 구하는 사람들은 다른 곳에서 보다 SPAR에서 이러한 정보를 우선 획득하여야만 한다. 그런데 이 정보 시스템에 담긴 정보는 스웨덴에서 은밀한 것으로 여겨지지 않는 개인 이름, 개인식별번호, 국적, 혼인여부, 추정소득, 조세능력, 부동산 소유 등이다. 결국 스웨덴에서 국민의 사생활을 보호하기 위해 계획되었던 정보 시스템이 역설적으로 다른 서구국가들이 피하고자 했던 감시의 상징이 되어버렸다.[419]

이러한 상황에서 개인식별번호가 계속적으로 원래의 목적과는 다르게 이용되고 결합되면서 그 사용을 중단해야 한다는 주장이 제기되었다. 이에 1978년 의회의 개인정보보호법개정위원회(Parliamentary Commission on Revision of the Dat Act)는 이러한 개인식별번호가 당초의 목적과는 달리 이용됨으로써 개인의 사생활을 부당하게 침해할 가능성이 있다는 것을 인정하였다. 그러면서도 이 위원회는 개인식별번호를 폐지할 경우에 초래될 현실적인 곤란함과 그에 소요되는 비용의 막대함을 들어 개인식별번호의 사용을 계속 허용하는 것으로 결론을 내렸다.[420] 다만 이러한 개인식별번호가 요구되어야만 하는 상황을 제한하는 방안을 제시하였다.[421]

다. 개인식별번호 불인정 국가

1) 미국

원래 미국에는 거주등록, 개인식별번호, 국가신분증 등과 같은 제도가 없었고 출생기록이 곧 국적기록이 되었다. 국적 취득에 있어서도 속지주의를 채택함으로써 이러한 제도의 시행을 뒷받침하고 있다. 이와 함께 개

418) 정보법, 제26조-28조.
419) David H. Flaherty, supra note 410), p.150.
420) Ibid.
421) 권건보, 앞의 책, 258-259면.

인의 출생, 사망, 혼인 등 사건별로 기록부가 작성되며, 개인별로만 기록하고 가족관계는 기록하지 않을뿐더러 각 기록간에 연결요소도 없으므로, 개인 신분사항을 한 번에 알아볼 수 없다. 그리하여 누군가가 사망하여 상속이 시작되었을 경우 그 자녀가 몇 명인지 누가 진정한 상속인인지 여부를 확인하려면 각자에 대한 출생증명서를 일일이 확인하는 수밖에 없다.[422] 이와 같이 다소 느슨한 형태의 신분등록제도를 갖고 있어도, 주거제도는 물론 전국민에게 가장 엄격한 국민등록제를 유지하고 있는 스웨덴 등과 가장 유사한 제도를 갖고 있다고 한다. 그 이유는 바로 사회보장번호(Social Security Number) 때문이다.[423]

미국의 사회보장번호는 1935년「사회보장법(Social Security Act)」이 제정되면서 도입되어 현재까지 사용되고 있다. 이 제도를 제정한 목적은 1935년 노동자의 수입을 추적하여 노인이나 장애인에 대해 사회보장의 혜택을 부여할 목적으로 창안되었다. 이러한 사회보장번호는 조세부과와 납세자의 확인을 위하여 필요하거나 도움이 되는 적당한 수단이나 장치를 고안할 수 있다[424]고 규정한 사회보장법(Social Security Act, of 1935)에 근거하여 행정부가 부여하기 시작하였다.[425]

이러한 사회보장번호의 발급 대상은 ① 이민이나 취업을 위해 합법적으로 입국하는 외국인, ② 연방복지프로그램 수혜 대상자, ③ 사회보장국(Social Security Administration)의 신원확인조사를 거친 후 자격을 취득한 사람 등이다.[426]

사회보장번호는 9자리의 숫자로 구성되며 3부분으로 나누어진다. 첫 번째 3자리 수는 신청할 때의 거주지역을, 중간 2자리 수는 특별한 의미 없이 편의에 의해 나누어진 구역을, 마지막 4자리 수는 발급순서를 나타낸다(XXX-YY-ZZZZ). 이것은 범죄에 이용되는 등 특별한 사정이 없는 한 평생 동안 사용하도록 되어 있다.[427] 사회보장번호을 발급받기 위하여 제

422) 장영아, 호적제도의 개선방안에 관한 연구, 한국여성개발원, 1996, 10, 37면.
423) 김기중, 국가의 국민관리체계와 인권, 21세기의 인권, 한길사, 2000, 401면.
424) Social Security Act, § 807(b), 49 Stat. at 637.
425) William H. Minor, “Identity Cards and Databases in Health Care: The Need for Federal Privacy Protection,” 28 Columbia Journal of Law and Social Problems 262 (1995).
426) 양창진, “전자정부시태 개인정보 관리 제도에 관한 연구 -전자주민증 제도의 도입과 그 정치적 함의를 중심으로-”, 박사학위논문, 한국학중앙연구원 한국학대학원, 2005, 58면.
427) 행정자치부, 각국의 신분증제도, 행정자치부, 1998, 1-4면 참조.

공하여야 하는 개인정보는 본명, 사무소 주소, 생년월일, 현재 연령, 전화번호 등이다.[428]

이 사회보장번호는 개인의 신청에 의해 부여하고 있으며,[429] 각종 복지혜택을 향유하기 위하여 거의 필수적으로 요구되고 있지만 강제성은 없고, 그 신청과 번호부여를 개별적 의사에 맡기고 있다.[430] 다만 각 개인마다 고유한 번호가 할당되어 있고, 미국의 일상적 생활에 있어서 필수적으로 이용하기 때문에 사회보장번호는 주민등록과 개인식별번호를 부여하는 것과 사실상 동일한 효과를 낳고 있다. 오늘날 사회보장번호는 상당수의 18세 미만 거주자와 수입이 있는 모든 성인거주자에게 부여되고 있다.[431]

2) 독일

독일에서 국민들의 신분등록은 신분법(Personenstandsgesetz)에 의하여, 주거등록은 각주의 법률에 의하여, 국가신분증은「신분증명법(Gesetz über Personalausweise)」에 의하여 규율된다.[432]

독일에서도 우리나라와 마찬가지로 일정 연령 이상의 모든 국민들에게 신분을 증명하기 위한 플라스틱 카드를 발급하고 그 소지를 의무화하고 있다. 이 신분증에는 일련번호(Seriennummer)가 기재되고 있지만, 이는 개인의 고유식별번호와 다르다.[433]

원래 독일에 거주하는 사람들은 해당 거주지역의 관청에 신고를 하여야 하였다. 신고하도록 하는 이유는 본인 및 주소를 확인하고자 하는 것이 일차적인 목적이나, 그 외에 조세부과나 선거인명부 등을 작성하기 위한 것도 있다. 그런데 이것은 주의 관할사항이었기 때문에 주마다 신고사항

428) 권건보, 앞의 책, 267면.

429) 행정자치부, 앞의 주 424), 2면: 사회보장번호의 신청은 연령, 국적에 관계없이 미국의 시민권자, 영주권자, 합법적으로 체류하는 외국인은 누구나 적법한 절차를 거쳐 신청할 수 있다. 그러나 최근 사회보장번호를 취급하는 연방의 주무관청인 사회보장청(Social Security Administration)은 사회보장번호의 발급을 1997년 하반기부터 외교관에게 부여하는 A1비자 소유자와 미국에서 직업을 가질 수 있는 H1비자 소유자에게만 사회보장번호를 부여하는 등 사회보장번호를 제한하고 있다.

430) 이상명, 앞의 주 338), 112면.

431) Philip Redfern, "Population Registers : Some Administrative and Statistical Pros and Cons," 152 Journal of Royal Statistical Society 4 (1989), p.4.

432) 김기중, "국가의 국민관리체계와 인권: 호적과 주민등록 제도를 중심으로", 세계인권선언 50주년 기념행사 학술세미나(1999. 2. 26.-3. 1.) 발표논문.

433) Philip Redfern, supra note 428), p.6.

등에 관하여 많은 차이를 보이고 있으므로 연방의회는「신고(기록)법(Melderechtsrahmengesetz)」[434]을 제정하였고, 이에 따라서 주의 해당 관청은 거주자의 신고를 기록하고 이를 보관해야만 했다. 이 법 제11조에 따라 어떤 지역으로 이사를 오거나 이사를 가는 사람은 모두 해당 관청에 신고를 해야만 했다. 제3자는 해당지역에 거주하는 특정인의 이름과 주소만 물어볼 수 있고, 다만 정당한 이해관계를 갖는 사람만이 좀 더 자세한 정보를 해당 관청으로부터 얻을 수 있다. 물론 해당 관청에 신고된 개인연방정보는 법적 근거가 있어야만 조사, 처리 또는 이용이 가능하다. 그리고 이 법에는 정보저장, 목적구속, 정보조사에 관한 규정과 아울러 공무원의 비밀의무, 관련자의 권리 등이 규정되어 있다. 하지만 이「신고법」에는 개인식별번호에 관한 규정은 없다. 결국 이 법에 따라 해당 관청은 선거준비, 조세카드발급, 여권발급, 병역사항 등을 위하여 이러한 기록을 사용할 수 있을 뿐이었다.[435]

그런데 1971년 연방 차원에서 모든 국내 거주자에게 12자리 숫자로 구성된 개인식별번호를 도입하고 연방주거등록청의 설립 및 연방과 주 사이의 주거등록전산망을 서로 연결하는 것을 목적으로 하는 법률안이 의회에 상정되었다. 그러나 이러한 개인식별번호가 헌법상 보장되는 개인의 인격권을 근본적으로 위협한다는 비판이 쏟아졌고,[436] 결국 의회는 개인식별번호를 기초로 한 정보처리 시스템은, 그에 상응하는 보호조치가 마련되지 않는 한, 설치되어서는 안 된다고 하면서 그 법안을 부결시켰다.[437]

이후 1984년 11월에 플라스틱 신분증(Plastik-Personalauweis)을 교부하려고 하였으나 또 다시 논란이 빚어졌다. 여기에는 종전과 달리 성명, 국적, 출신지, 생년월일 등 구체적인 사항들이 기재되고 사진까지 첨부되며 이러한 신분증은 컴퓨터에 연결되어 치안당국에 중요한 정보수단으로 활용될 수 있도록 예정되어 있었다. 이에 대하여 당시의 여당이던 독일기독교민주연합(Christlich-Demokratische Union Deutschlands; CDU) 등 연립정부가 이러한 전자신분증의 도입에 적극적이었던 반면에, 녹색당은 신분증제도 자체의 도입을 반대하였고 사회민주당은 전자신분증의 도입에 반

434) BGB1. I. 1429.
435) 김일환, 앞의 주 233), 319면.
436) Philip Redfern, supra note 428), p.4.
437) David H. Flaherty, supra note 410), p.77.

대하는 입장이었다.

그러나 1986년 4월 21일 제정된「신분증법(Gesetz über Personalausweise)」에 따라 현재 독일에서는 플라스틱으로 제작된 신분증을 국민의 신분확인의 수단으로 활용하고 있다. 이 신분증의 앞면에는 사진, 성명, 출생지, 생년월일, 국적, 유효기간, 서명이 기재되어 있고, 생년월일과 일련번호 등은 컴퓨터로 판독할 수 있다. 뒷면에는 주소, 신장, 눈의 색깔, 발급기관, 발급일자 등이 기재되며, 주소의 변경 시에는 스티커로 변경사항을 수정하고 있다. 국경관리자는 신원확인수단으로 이 신분증의 제시를 요구할 수 있고, 경찰과 사회보장청도 제한된 조건하에서 신분증에 의해 정보를 수집할 수 있다. 또한 민간영역에 있어서 시민들도 신분확인의 수단으로서 이를 사용할 수 있다.[438]

현재 독일에서는 이와 같은 신분증 외에도 정부기관이 자신들의 고유한 업무를 수행하기 위하여 각종의 카드를 발급하고 있지만, 그 번호는 각기 달리 부여되어 각각의 고유한 목적을 위해서만 이용되고 있다. 가령 사회보장제도에 사용하기 위한 연금보험번호라는 것이 있지만, 미국의 사회보장번호와 달리 다른 용도로 널리 이용할 수 있는 표준통일식별번호는 아니다. 생년월일 기타 개인정보를 포함하는 알파벳과 숫자로 구성되어 있는 이 연금보험번호는 노인연금의 수급을 위해서만 사용될 뿐이다.[439]

3) 일본

일본에서는 신분등록제도로 호적제도를, 주거등록제도로 주민기본대장제도를 두고 있으나, 국민에 대한 개인식별번호제와 국가신분증제도는 채택하지 않고 있다. 1970년 2월에 일본정부는 개인고유번호제의 도입을 추진하려고 입안한「정보처리 고도화 운영방침」중 전국적으로 하나로 통일된 개인코드를 부여하려는 정부의 계획이 알려지면서 전국전기통신노동조합을 중심으로 '국민총배번제(國民總背番制)에 반대하고 프라이버시를 지키는 중앙회의'가 결성되어 코드는 더 검토하지 않기로 하였다는 발표를 하기에 이르렀다.[440]

---

438) David H. Flaherty, supra note 410), p.79.
439) Ibid. p.78.
440) 堀部政男, プライバシーと高度情報化社會, 東京: 岩波文庫; 1988; 신구현 옮김, 프라이버시와 고도정보화사회, 청림출판, 1995, 62-64면.

현재 일본은 과거 식민지에서 실시했던 국민수장제 경험을 바탕으로 제도화 된 주민기본대장을 주민에 관한 행정사무 처리의 수단으로 삼고 있다. 주민기본대장이란 시(市), 구(區), 정(町), 촌(村) 등 전국 지방자치단체가 보유한 일종의 주민명부로서, 해당지역 주민의 성명, 생년월일, 성별 등의 정보가 일정한 형식으로 기재되어 있는 문서이다. 이 주민기본대장은 지방자치단체장이 작성하며, 개인을 단위로 하여 주민표가 작성되고, 이름, 출생일, 성별, 세대주, 호적의 표시, 주소, 以前의 주소, 국민보건보험과 국민연금 관련 사항 등이 추가로 기재되어 통합 관리되며, 선거인명부 작성 등에 활용된다.[441]

2002년 8월 5일, 일본은 이 주민기본대장 제도를 바탕으로 주기넷(住基Net)이라 불리는 주민기본대장 네트워크 시스템을 시작했고, 2003년 8월 25일 2차 서비스를 시작했다. 이 네트워크는 e-Japan 전자정부・전자자치제 구축을 위한 축으로서 주민의 주소, 성명, 생년월일, 성별 등 4가지 정보와 주민코드가 IC카드에 기록된 주민기본대장카드를 근간으로 일본의 중앙정부와 모든 지방자치단체의 행정망을 연결한 것이다. 이 주민기본대장카드는 국가가 관리하지 않고 각 지역 자치단체가 관리한다. 그러나 여기에 기록된 정보는 전용회선으로 연결된 컴퓨터에 의해 관리되며, 전국적으로 공유함으로써 전국 어디서나 본인 확인이 가능하게 된다는 점에서 사실상 국가통합주민카드라고 할 수 있다.[442]

이러한 전산처리를 통해 공유하는 주민등록정보는 기본사항(성명, 주소, 생년월일, 성별)인데, 공유하는 정보를 서로 구별하기 위해 각 개인에게 무작위로 작성된 10단위의 숫자와 1단위의 검증번호로 조합된 11단위의 고유번호로 구성된 일종의 표준개인식별번호인 주민표코드를 부여하였다. 주민표코드의 이용과 관련하여 엄격한 제한이 가해지고 있는데,「주민기본대장법」제30조의41 제1항에서 시・정・촌장은 이 법에서 규정하는 사무 등을 처리함에 있어서 필요한 경우를 제외하고는 누구에 대해서도 당해 시・정・촌의 주민 이외의 자에 관한 주민표코드를 요구할 수 없다고 규정하였으며, 제30조의43에서는 민간부분에 있어서도 누구도 자기와 동일한 세대에 속하는 자 이외의 자에 대하여 당해 제3자 또는 당해 제3자

441) 日本の“住民基本臺帳法”-昭和42年(1967) 7月 25日(法律 第81号), 最終改正 昭和60年(1985年) 法第76号.

442) 한국정보보호진흥원, 2002 개인정보보호백서, 한국정보보호진흥원, 2002, 305면.

이외의 자에 대한 주민표코드를 고지하도록 요구하지 못하며, 주민표코드가 기재된 데이터베이스는 제3자 제공이나 목적 외의 이용을 예정하고 있는 경우 그 구축이 제한된다고 규정하고 있다.

또한 주민표코드는 민간이용이 금지될 뿐만 아니라 해당 주민의 신청에 따라 언제든지 변경될 수 있다는 점에도 불구하고(법 제30조의3), 정부의 주민기본대장 네트워크 계획은 PIJ(Privacy International Japan)를 중심으로 한 시민사회단체의 반대에 부딪혔다. 시민사회단체 주장의 논지는 행정사무의 효율화 등의 편리함과는 반비례로 개인정보의 보호측면에서는 상당한 위험성을 내포하고 있다는 것인데, 주민기본대장 네트워크에 의해 공유되는 정보는 본인확인정보에 불과하지만 개인에게 부여된 주민표코드에 의해 정보가 일괄적으로 관리되어 개인의 수입 및 대출금, 도서관 사용내역, 가족구성, 병력, 학력 등 여타의 개인정보에 접근할 수 있다는 것이다.[443]

라. 분석 및 시사점

외국의 개인식별제도를 고찰한 바, 대부분의 국가에서는 각 나라의 고유한 신분증제도를 운영하고 있으며 그 중에서도 크게는 통합개인식별번호를 인정하는 국가와 통합개인식별번호를 인정하지 않는 국가로 구분할 수 있다.

통합개인식별번호는 인정하는 국가로는 프랑스와 스웨덴이 있는데 이 중 스웨덴은 앞서 고찰한 바, 2008년 실시한 전자정부평가에서 전자정부 준비지수 순위에서 1위를 차지하고 전자적 참여지수 순위에서는 상위권에 들지 못하였다. 이와 같은 점에서 본다면 통합 개인식별번호제도가 국가통치작용에서는 상당한 효과가 있음은 분명하다. 반면에 국민의 정치참여나 개인정보보호차원에서는 별로 효과를 발휘하지 않는다고 할 수 있다.

스웨덴의 주민등록제도는 원래 교회에 의하여 시작되었지만 오늘날 주민등록업무를 총괄하는 부서는 국세청이다. 따라서 개인정보침해라는 차원에서 많은 논란이 있었지만 아직 쉽게 바꾸지 못하고 있는 실정이다. 어쨌든 개인을 식별할 수 있는 통합적인 정보체계가 마련이 되면 국가는

443) 이상명, 앞의 주 338, 111면; 금봉수・장우영・조용혁, 전자신분증 추진동향과 시사점, 한국전산원, 2005, 23면.

그것을 단일한 정보 시스템체계를 구축하고 국가정보은행에 저장·보유하면서 국민을 통치하는데 혹은 국민을 감시·감독하는 능력을 확대시키게 되어있다.

프랑스는 스웨덴의 경우처럼 통일식별번호제도를 인정은 하지만 강제성은 없으며, 개인을 확인하는 수단에 이용되는 것은 사실이지만 우리나라와 같이 고유불변한 체계는 아니고, 국민이 자발적으로 자신의 정보를 등록하고 있다. 따라서 평생 수반되는 고유식별인자로서의 기능은 하지 않는다.

한편 개인식별번호를 인정하지 않는 국가들도 나름대로 개인을 확인하거나 주민관리의 차원에서 국민에게 고유번호를 부여하여 사용하고 있다. 그러나 이들은 모두 통합개인식별번호를 부여하거나 국가 신분증제도는 도입하지 않고 있지만, 그럼에도 불구하고 주민관리체계가 정확하게 이루어지고 있는 것은 사회보장과 관련하여 다양한 이익을 제공함을 목적으로 하기 때문이라 본다.

이러한 점에서 우리의 경우 강제부여와 동시 영구불변한 통합개인식별번호제도는 제고해보아야 할 것이다.

3. 우리나라의 주민등록제도

가. 개인식별번호로서의 주민등록번호

우리나라에서 전국민을 대상으로 신분증제도를 실시한 주목적은 자주 발생한 전쟁에 필요한 병력 확보에 있다. 또 호구와 장정의 수를 명백히 파악하여 세금은 물론 직업과 계급에 따른 신분을 명확히 구분하고, 병역의 의무와 부역의 기준을 정하는 것이었다.

이러한 신분증제도가 처음 실시된 것은 조선 태종대에 실시된 호패법으로 알려진다. 호패란 조선시대 16세 이상의 남자가 차고 다닌 것으로써 오늘날의 신분증명서와 같은 것이다. 이 호패는 왕실, 조관으로부터 서민 공사천에 이르기까지 16세 이상의 모든 남자가 소지하도록 의무화되었다.[444]

444) 태종실록, 제26권, 태종 13년 9월 1일.

이후 일본의 보호국이 되면서 1906년부터는 호적의 등록사무를 경찰관서에서 담당하고, 헌병과 순사가 실지조사를 하여 호적에 등록하였다. 1909년에는「민적법」이 제정되고 1922년 더 세밀한 조항을 규정한「조선호적령」이 제정됨으로써 일본의 호적과는 확실히 구별되는 호적체계가 만들어졌다. 더 나아가 조선총독부는 1942년 9월 26일, 본적지를 떠나 90일 이상 거주할 사람들에게 관청에 강제적으로 등록하도록 하는「조선기류령(朝鮮寄留令)」과「조선기류수속규칙」을 공포하였다.

이와 같은 법규들의 제정목적은 병역자원의 파악과 주민통제에 있었던 만큼, 총독부는 후속조치로 이미 조직되어 있던 애국반 반장이나 임시 조사원을 동원하여 호적 정비 및 기류 신고 촉진 운동이나 일제조사를 통해 대대적으로 조선인을 기류부에 등록시켰다.[445]

해방과 6.25전쟁 전후에는 국내 질서가 혼란해졌고, 법적인 근거도 미비한 채로 도민증을 발급하였다. 도민증의 발급 대상자는 현역군인 및 국가공무원・지방공무원으로서 도민증 발급을 원하지 않는 자 또는 만 13세 미만 자 등을 제외한 모든 도민으로 하였다.

현행 주민등록제도는 박정희 전대통령 집권 초기에 처음으로 도입되었다. 1962년 1월 15일 국가재건최고회의는 1가구별 1용지의 기류부에 본적지 이외의 일정한 장소에 30일 이상 주소 또는 거소를 정한 자에게 신고의무를 부과하는「기류법(寄留法)」을 제정하였다. 이어 1962년 5월 10일에 는 기류법이「주민등록법」으로 대체되었다.

이「주민등록법」은 주민의 거주관계를 파악하고 상시로 인구의 동태를 명확히 하여 행정사무의 적정하고 간이한 처리를 도모하는 것을 목적으로 하며(법 제1조), 30일 이상 거주할 목적으로 일정한 장소에 주소 또는 거소를 갖는 주민은 모두 주민등록을 하여야 한다(법 제6조).

즉 성명, 성별, 생년월일, 세대주와의 관계, 본적, 주소, 전입 또는 퇴거의 경우에는 전입전의 주소 또는 행선지와 그 연월일을 '하나의 세대에 속하는 자의 전원이 거주지를 이동한 때에는 세대주 또는 그 대리인은 이동의 날로부터 14일 이내에 구거주지를 관할하는 시장 또는 읍, 면장에게는 퇴거신고를, 신거주지를 관할하는 시장 또는 읍, 면장에게는 전입신고'(법 제14조 제1항)를 의무적으로 하도록 하였다. 또 하나의 세대에 속

445) 당대비평 편집부, "국가는 왜 국민을 '등록'시키려 하는가", 당대비평, 제20호, 2002.

하는 자의 일부가 거주지를 이동한 때에는 구거주지를 관할하는 시장 또는 읍, 면장에게 퇴거신고를 한 후 퇴거증명서를 첨부하여 신거주지를 관할하는 시장 또는 읍, 면장에게 전입신고를 하여야 한다(제15조 제1항)고 하여 주민등록의 퇴거신고와 전입신고를 의무화시켰다.

이「주민등록법」은 현재까지 20차례에 걸쳐 개정되었는데, 1970년 1월 1일 제2차 개정 때에는 주민등록증에 관한 사항을 추가하였고, 1975년 7월 25일 제3차 개정으로 주민등록제도를 개선하고 과태료와 벌칙규칙을 강화하였다. 그리고 1977년 12월 31일 제4차 개정으로 세대별 주민등록표 외에 개인별 주민등록표를 작성하도록 하고 개인별 주민등록표는 주민등록번호순으로 편재하였다.

나. 주민등록번호의 체계와 특징

주민등록번호는 지역표시번호와 성별표시번호 및 개인표시번호를 차례로 배열하여 작성하되, 지역표시번호 다음에 "-" 표시를 하여 성별표시번호 및 개인표시번호와 연결한다. 성별표시번호는 남자는 "1"로, 여자는 "2"로 하며, 개인표시번호는 주민등록의 일시순과 주민등록표에 등재된 순위에 따라 차례로 일련번호를 부여하되 성별표시번호에 연결하여 6자리의 숫자로 배열한다. 주민등록번호는 1인 1번호로 하여야 하며, 이미 사용한 번호는 이를 다시 사용하지 아니하므로 주민등록번호는 발급 당시부터 고유번호가 정해진다.

이처럼 우리나라에서는 주민등록번호가 주민등록증을 최초로 발급할 때부터 발급대상자 전원에게 고유한 번호가 부여되었다.[446] 앞에서 본 바와 같이 초기의 주민등록번호는 6자리씩 두 부분으로 나뉘어 모두 12자리 숫자로 구성되어 있었다. 여기서 앞부분의 6자리 숫자는 지역을, 뒤의 6자리 숫자는 거주세대와 개인번호를 나타내었다. 대표적인 예로서 1968년 11월 당시 박정희 대통령 부부에게는 110101-100001과 110101-200002가 각각 부여되었다. 그러나 이 번호부여의 방식은 1975년 생년월일, 성별, 지역을 표시하는 현행의 숫자 체제로 바뀌었다.

이러한 주민등록번호의 부여는 원래「주민등록법」에 근거가 없었으나, 2001년 개정된「주민등록법」에 시장・군수 또는 구청장은 주민에 대하여

446) 권건보, 앞의 책, 254-256면 참조.

개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다(제7조 제3항)고 하는 조항을 신설함으로써 법률적 근거를 마련하였다. 이 조항을 신설한 이유는 허위의 주민등록번호를 생성하여 행사하는 등 주민등록제도와 관련된 각종 범법행위를 엄중하게 처벌하도록 하여 주민등록증 및 주민등록제도의 신뢰성을 제고하는 한편, 기타 현행 제도의 운영상 나타난 일부 미비점을 개선·보완하기 위한 것이다. 이에 근거하여 「주민등록법시행규칙」에서는 주민등록번호를 생년월일·성별·지역 등을 표시할 수 있는 13자리의 숫자로 작성하도록 규정하고 있다.

우리나라의 주민등록번호 체제는 외국의 예에 비추어 매우 많은 자리수와 독특한 조합체계를 가지고 있다. 주민증록번호는 <표 17>에서 보는 바와 같이 전체가 13자리의 숫자로 구성되어 있으며, 앞의 6자리의 숫자는 백년 대를 뺀 생년월일로 이루어지며, 뒤의 7자리 숫자는 출생 년대와 성별, 최초 주민등록번호 발급지 등으로 조합된다.

<표 17> 주민등록번호 조합표

위치	번호순서							내 용
앞	Z	Z	Y	Y	Z	Z	-	생년월일 : 백연대수를 제외한 6자리
뒤	A							출생년대, 성별 구분
		B	C	D	E			최초주민번호발급지역코드
						E		동일한 성을 가진 지역주민 중 접수순위
							F	오류 수정 번호

*정연수·김희은, "주민등록번호 도용의 문제점 및 개선방안", 인터넷법제연구 제3권 제2호, 한국인터넷법학회, 2004, 198면 참조.

이 가운데 뒤의 첫째 숫자는 출생연대와 성별을 나타내는데, 1800년대에 태어난 남자는 9번, 여자는 0번, 1900년대에 태어난 남자는 1번, 여자는 2번, 2000년대에 태어난 남자는 3번, 2000년대에 태어난 여자는 4번이 부여된다.

그리고 둘째 자리부터 다섯째 자리까지의 네 자리 숫자는 최초 주민등록번호 발급기관(관할 시·군·구청)의 고유번호인데, 이를 통해서 최초의 발급지 내지 출생신고가 된 지역이 어디인지를 알 수 있다.

여섯째 자리 숫자는 출생신고의 순서를 나타내는데, 구체적으로는 신고

당일 같은 지역의 같은 姓을 쓰는 사람들 중에 몇 번째로 신고가 되었는지를 표시한다.

일곱째 숫자는 검증번호(check digit)로서 소지하고 있는 주민등록번호가 올바른 번호인지를 확인하는 도구로 쓰이는데, 이를 통해 위조된 번호이거나 잘못 기재된 번호임을 확인할 수 있다. 주민등록번호의 몇 자리 숫자를 조합하여 일정한 연산과정을 거친 후 구해지는 숫자가 검증번호와 일치하는지를 통해 주민등록번호의 진위 여부를 판별하게 된다.[447]이렇게 정교하게 고안된 우리의 주민등록번호는 부여 대상자 가운데 중복되는 경우가 없고, 일생동안 변하지도 않아서 개인을 정확하게 인식하는 수단으로 완벽한 것이다.[448] 더구나 다른 자료의 도움 없이 그 자체만으로 생년월일, 나이, 출신연대, 성별, 주민등록증 최초 발급지역, 신고순위, 번호의 위조 여부까지 확인할 수 있다. 이처럼 일련번호 하나만으로 수많은 개인정보가 노출될 수 있기 때문에 그 자체로서 개인의 사생활에 대한 위험을 초래할 수 있으며, 특히 전산망의 발전에 따라 개인정보 확인의 키워드 역할을 함으로써 중요한 위치를 차지하게 되어 그 위험성을 날로 증가하는 추세에 이르고 있다.

한편 지역번호의 경우는 업무관장지역의 폐치 또는 분합이 발생할 경우 시장·군수 또는 구청장이 절차를 거쳐 특별시장·광역시장 또는 도지사를 거쳐 행정안전부장관에게 지역표시번호의 조정을 요청하도록 되어있다. 따라서 주민등록번호의 지역번호의 경우는 행정구역의 변경에 의하여 변화가 있을 수 있으나 이미 주민등록증을 부여받은 자와는 별 관계가 없고 다만, 행정처리 과정이나 변경 이후에 주민등록을 하는 자의 주민등록번호에 영향을 줄 뿐이다.[449]

---

447) 예컨대 주민등록번호가 701385-8568789라고 가정하면, 이 중에서 맨 뒷자리 수(9)를 빼면 나머지 번호 701385-856878이 남게 된다. 각 번호별로 2,3,4,5,6,7,8,9,2,3,4,5를 곱하고(즉, 2×7, 3×0 4×1, 5×3, 6×8, 7×5, 8×8, 9×5, 2×6, 3×8, 4×7, 5×8), 각각의 합을 더하면 329라는 값이 나온다. 329를 11로 나누면 몫이 29, 나머지가 10이 나오는데, 몫을 버리고 11에서 나머지 10을 다시 빼준다(즉 11-10=1). 이렇게 해서 나온 1이라는 숫자가 주민등록번호의 맨 뒷자리 번호와 일치해야만 이 주민등록번호가 올바른 번호임을ㄹ 나타낸다. 그러나 여기서 나온 1은 위에서 가정한 주민등록번호 9라는 숫자와 일치하지 않으므로 위 주민등록번호는 허위이다. 정연수·김희은, "주민등록번호 도용의 문제점 및 개선방안", 인터넷법제연구 제3권 제2호, 한국인터넷법학회, 2004 199면 참조.

448) 주민등록체계가 완벽하다고는 하나 이미 인터넷 등을 통해 많은 사람들에게 알려져 있고, 주민등록번호 생성기기 이러한 조합방식을 프로그램으로 만들어 활용함에 따라 무작위의 주민등록번호가 용이하게 생성되고 있다.

다. 주민등록번호와 자기정보관리통제권

주민등록제도는 개인의 거주지를 기준으로 생활을 공동으로 하는 개인의 거주이전 실태를 등록·관리하는 제도인데, 개인정보의 국가등록제도 중에서 가장 기본적인 제도이고, 가장 포괄적인 범위에 걸쳐 국민의 개인정보를 수집하는 제도라 할 수 있다. 현행 주민등록제도에 의해 주민등록표에 기재되는 개인정보는 140개 항목에 달하며, 이 정보 중 78개 항목은 다시 주민등록전산망이라 불리는 데이터베이스에 수록되어 중앙정부인 행정안전부가 통합관리한다.[450]

문제는 이렇게 통합되어 데이터베이스화된 주민등록정보가 범용현상을 일으켜 자기정보관리통제권과의 충돌이 발생한다는 것이다.

전술한 바와 같이 우리나라의 주민등록번호는 종신불변성, 유일독자성, 편의성 등 표준식별번호로서의 특징을 가지고 있다. 이러한 특수성은 개인식별 또는 신원확인이 필요한 사회 모든 분야에서 주민등록번호를 광범위하게 사용하고자 하는 의욕을 가지게 한다. 그런데 주민등록번호는 사회 모든 영역에서 광범위하게 사용됨에 따라 그 만큼 개인정보의 보호가 원만하게 이루어지는가의 문제와 주민등록번호의 남용현상을 어떻게 제어할 것인가의 문제가 불가분의 상관관계를 가지게 된다.[451]

주민등록제도의 본래의 목적은 시·군 또는 구의 주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것(「주민등록법」 제1조)이다. 그러나 현재의 주민등록제도는 주민등록번호와 지문날인제도로 인하여 본래의 수집목적을 넘어 국민을 통제하고 감시하는 수단으로 사용될 뿐만 아니라 과도한 사용으로 인한 인권침해, 재산상을 피해가 속출하고 있는 실정이다.

특히 자기정보관리통제권과 관련하여 개인정보는 정보주체의 분명한 인식 또는 동의하에 수집되어야 함에도 불구하고 주민등록번호는 모든 국민에게 출생신고와 동시에 강제 부여된다. 이렇게 강제 부여된 주민등록번호는 공공부문은 물론 민간부문에서도 목적 범위를 벗으나 광범위하게 수

449) 정연수·김희은, 앞의 주 444, 198면.
450) 이상명, 앞의 주 338, 95면 참조.
451) 한상희 외, 주민등록번호 사용현황 실태조사, 국가인권위원회, 2005, 24면.

집되고 있으므로 개인정보의 수집제한청구권을 침해할 소지가 크다. 또한 현행 주민등록법은 주민등록표의 수록사항을 전산정보 처리조직에 의하여 처리하도록 하고(법 제7조 제1항), 전산처리된 주민등록표 파일 등의 주민등록 전산정보 자료를 다른 공공기관의 어떤 개인정보 파일과도 연계될 수 있는 가능성이 법적으로 열려 있다.[452] 더 나아가 오늘날 전자정부 구축에 따른 행정정보의 공동이용이 본격화된 시점에서 개인정보의 수집은 전자행정의 구현을 위한 핵심요소이고 행정정보 중에 들어있는 개인정보의 공동이용은 피할 수 없는 핵심 수단으로 자리 잡고 있다.

행정정보공동이용을 위한 개인정보를 수집함에 있어서도 자기정보관리통제권을 실현하는 차원에서 수집제한의 원칙, 정보내용의 정확성 원칙, 목적명확성 원칙, 이용제한의 원칙, 안전확보의 원칙, 사전동의의 원칙이 준수되어야 한다.

라. 주민등록번호의 위헌성 여부

1) 법적 근거 및 의회유보의 원칙

우리나라의「주민등록법」은 1962년 제정 당시에 주민등록번호의 부여에 대해 전혀 규정하지 않고, 다만「주민등록법」시행령에서 시장·군수 또는 구청장이 개인별로 고유한 주민등록번호를 부여하도록 규정하고 있었다. 이러한 규정의 체계에 대해서 주민등록번호 부여의 법적 근거가 부족할 뿐만 아니라 위임입법의 한계를 일탈하고 있다는 비판이 제기되었다.

그런데 2001년 개정된「주민등록법」에서는 주민등록번호의 부여에 대해 직접적인 규정을 두게 되었다. 즉 제7조 제3항에서 주민에 대하여 개인별로 고유한 주민등록번호를 부여하도록 하고, 제4항에서 주민등록번호의 부여방법은 대통령으로 정하도록 하였다. 이에 따라 주민등록번호를 부여하고자 하는 때에는 반드시 본적을 확인하여야 한다(시행령 제7조 제2항). 또한 주민등록번호를 부여할 때에는 주민등록번호부여대장에 이를 등재하며(시행령 제7조 제3항), 주민등록번호의 부여는 전산조직을 이용하여 처리할 수 있도록 하고 있다(시행령 제7조 제4항). 그리고 주민등록번

452) 이상명, 앞의 주 338), 98면.

호는 생년월일·성별·지역 등을 표시할 수 있는 13자리의 숫자로 작성하고(시행규칙 제2조), 시·구청장 또는 읍·면장은 주민등록지의 시장·군수 또는 구청장으로부터 해당 주민에게 주민등록번호가 부여되었음을 통보받으면 해당자의 가족관계등록부란에 이를 기록하여야 한다(시행규칙 제5조). 이로써 현재의 주민등록관련법령의 체계는 법률유보의 원칙이나 위임입법의 한계에 관한 문제는 일단 해소되었다[453]고 볼 수 있다.

하지만 법치주의는 헌법의 기본원리 중 하나로, 행정작용은 국회가 제정한 형식적 법률에 그 근거가 있어야 한다는 법률유보의 원칙을 그 핵심적 내용으로 하고 있다. 그러나 법률유보의 원칙에 의하면 행정작용이 단순하게 법률에 근거를 두기만 하면 되는 것이 아니고, 국가공동체와 그 구성원에게 기본적이고도 중요한 의미를 갖는 영역인 국민의 기본권 실현에 관한 영역을 행정부의 처분에 맡기지 말고, 국민의 대표자인 입법자가 스스로 그 본질적 사항에 대해 결정해야 한다는 것을 의미한다. 이러한 원칙을 의회유보의 원칙이라고 한다.[454]

이러한 점에 비추어 볼 때 우리나라의 주민등록번호는 그 자체만으로 다른 보조적 자료가 필요 없이 사람의 내밀한 개인정보인 생년월일과 성별, 출신지역, 등재순위를 드러나도록 되어 있고, 고유 불변이라는 주민등록번호의 특성 때문에 한번 타인에게 노출된 후에도 평생 그대로 노출된 채 살아갈 수밖에 없어 개인의 사생활을 크게 해치고, 종국에는 개인의 인격을 파괴할 수도 있다. 따라서 기본권의 하나인 자기정보관리통제권을 실현하는데 있어 주민등록번호의 부여에 관한 필요한 사항을 현행「주민등록법」제7조 제4항에 직접 규정하지 않고, 이 법 시행령 제7조 제4항과 제5항에 그 사항을 위임하고, 다시 이 법 시행규칙 제2조에 그 사항을 위임하는 방식은 의회유보의 원칙에 위반된다[455]고 할 수 있다. 특히 모든 국민에 대한 개인식별번호 부여 여부는 국회 스스로가 반드시 법률로 정해야 하는 사항인데도 이를 행정부에 위임한다는 것은 위헌이다.[456] 곧

453) 권건보, 앞의 책, 269-270면.
454) 헌법재판소 1999. 5. 27. 선고, 98헌바70 결정, 11-1, 643면.
455) 이희훈, "주민등록번호에 대한 헌법적 고찰 -개인정보자기결정권의 침해를 중심으로-", 토지공법연구 제37집 제1호, 한국토지공법학회, 2007, 389면; 김일환, 앞의 주 233), 324-327면; 이인호, 개인정보감독기구 및 권리구제방안에 관한 연구, 236면; 한상희, 앞의 주 315), 123면.
456) 헌법재판소 1995. 7. 21. 선고, 94헌마125 결정.

헌법우위가 확립된 민주법치국가인 우리나라에서 법률유보란 우선 법률에 유보된 곧 행정의 자율적인 규정에서 벗어나 있는 사항영역과 대상을 뜻한다. 따라서 개인식별번호의 부여와 같은 기본권을 제한하는 국가작용의 법적 근거는 행정부가 제정한 법규명령이 아니라 의회가 제정한 법률이어야 한다.[457] 더욱이 전술한 바와 같이 주민등록번호는 개인의 사생활 및 인권을 침해할 뿐만 아니라 주민등록번호의 도용 등과 같은 많은 문제점과 위험성을 안고 있기 때문에 더욱 법률의 확실한 근거를 요한다고 하겠다.

2) 비례원칙의 충족 여부

「주민등록법」에 의한 주민등록번호제도가 합헌 또는 합법으로 인정되기 위해서는 헌법 제37조의 기본권 제한의 일반원칙에 합치되어야 한다. 특히 문제되는 것은 비례의 원칙에 따라 필요최소한의 조치에 한정되어야 한다.

첫째, 현행「주민등록법」제1조에 의하면 주민등록제도는 주민의 거주관계를 파악하고 상시로 인구의 동태를 명확히 하여 행정사무의 적정하고 간이한 처리를 도모할 목적을 가지고 있다. 행정사무의 적정하고 간이한 처리라는 목적은 오늘날 국방, 치안, 조세, 선거인명부의 작성, 사회복지, 인구센서스 등 국가나 지방자치단체가 수행하는 수많은 책무들에 비추어 볼 때 일단 헌법상 그 정당성이 인정된다고 할 수 있다.

둘째, 주민등록번호에는 거주지와 관련된 표지를 담고 있으나, 그것은 신청 당시의 거주지와 관련된 것이므로 현재의 거주를 파악하는 것과는 관련이 있다고 하기 어렵다. 하지만 인구의 동태를 명확히 하여 행정사무의 적정하고 간이한 처리를 가능하게 하는 측면은 인정될 수 있다. 특히 모든 국민에게 주민등록번호를 부여함으로써 범죄의 예방이나 범인의 검거 등에 있어서 상당한 효과를 거두고 있는 것으로 판단된다. 따라서 주민등록번호의 부여는 주민등록법상의 목적을 달성하기 위한 수단으로서 적합성을 갖추지 못한다고 쉽게 단정하기는 어려울 것이다.[458]

셋째, 프랑스와 달리 우리나라가 위의 첫째 목적을 실현하기 위해 주민

457) 김일환, 앞의 주 233), 326-327면.
458) 권건보, 앞의 책, 270-271면.

등록번호를 강제로 부여하는 것을 설사 인정한다고 하더라도 미국이나 독일 또는 일본처럼 그 번호가 무작위의 일련번호를 부여하여 개인의 내밀한 정보를 타인에게 그대로 드러나지 않도록 하더라도「주민등록법」제1조의 목적을 실현하여 국가안전보장이나 질서유지 또는 공공복리를 실현할 수 있을 것이다. 따라서 주민등록번호 소지자의 내밀한 개인정보를 번호 그 자체로 드러나게 하고, 고유불변한 현행의 주민등록번호는 최소침해의 원칙에 반한다고 할 것이다.

넷째, 현행처럼 주민등록번호 소지자의 의사와 상관없이 자신의 내밀한 개인정보를 외부에 번호 그 자체로 드러나게 하고, 주민등록번호의 변경을 불가능하도록 하는 것에서 도출되는 행정사무의 적정하고 간이한 처리를 통한 국가안전보장이나 질서유지 또는 공공복리의 실현이라는 공익보다 그 피해를 최소화하는 다른 수단을 강구하지 않아 주민등록번호 소지자의 자기정보관리통제권을 심히 침해하여 그 사람의 인격을 파괴하여 잃게 되는 사익의 침해가 더 크다는 점에서 법익의 균형성의 원칙에 반한다고 할 것이다.[459]

이러한 관점에서 보았을 때 주민등록번호에 관한 내용을 법률에 규정한다 할지라도 주민등록법상 규정된 주민의 거주관계 등의 파악이라는 목적의 달성을 위하여 모든 국민에게 일률적이고 강제적으로 주민등록번호를 부여해야 할 필요성을 설명하지 못하고 있다. 결국「주민등록법」은 목적 그 자체에 비추어볼 때 모든 국민에게 출생과 더불어 개인식별번호를 부여하는 것은 위헌이다. 왜냐하면 반드시 모든 국민에게 개인식별번호를 부여해야 할 필요성 자체가 설명되지 않을 뿐만 아니라 설사 이를 인정한다 해도 기본권을 덜 침해하는 다른 수단 등이 있음에도 불구하고 반드시 개인을 식별할 수 있는 방법으로만 번호를 부여하도록 하는 것은 방법의 적절성, 피해의 최소성에 반할[460]뿐만 아니라 추구하는 공익보다 사익의 침해가 더 크다고 하겠다.

마. 주민등록번호제도의 개선방안

앞서 검토한 바와 같이 오늘날 고도화된 정보사회에서 개인정보는 국가

459) 이희훈, 앞의 논문, 390-391면.
460) 김일환, 앞의 주 233), 329-330면.

나 기업 등에 의해 점점 더 많이 수집되고 관리·처분되어, 정보의 주체인 개인은 정보의 객체로 전락되며 자기정보관리통제권을 상실하게 되는 위험한 상황에 처하게 되었다.

그러나 주민등록제도의 긍정적·효율적 측면을 그 누구도 부인할 수는 없을 것이다. 더욱이 주민등록번호의 부여는 오늘날 국방, 치안, 조세, 선거, 사회복지 등 다양한 행정적 수요에 효율적으로 대처하기 위하여 불가피한 측면이 있다고 할 수 있다. 특히 모든 국민에게 개인식별번호를 부여함으로써 범죄의 예방이나 범인의 검거 등에 있어서 상당한 효과를 거두고 있는 점도 과소평가할 수만은 없는 실정이다. 하지만 그렇다고 하더라도 전국민을 대상으로 다량의 개인정보를 내포하는 개인식별번호를 영구적이고 고정불변의 형태로 부여하고 이를 공공부문과 민간부분에 걸쳐 광범한 목적에 활용되도록 하는 현행의 체계는 결코 바람직하다고 할 수 없다.[461]

더욱이 헌법상 보호되어야만 하는 것은 국민의 기본권 행사이지 국가의 기본권 행사는 아니다. 그러므로 국민의 기본권을 제한하려는, 곧 모든 국민에게 개인식별번호를 부여하려는 국가가 왜 이러한 국민의 기본권제한이 필요하며, 국민의 기본권을 가장 적게 제한하면서도 필요한 국가목적을 달성할 수 있는지를 입증해야만 비로소 이러한 기본권제한의 정당성이 확보된다. 결국 개인식별번호의 필요성이나 그 도입 여부는 행정의 효율성이나 편리성 차원이 아니라 헌법 차원에서 과연 허용되는지를 규범적으로 살펴보아야만 한다. 국가가 그 정당성을 입증하지 못하는 한 국민은 당연히 이러한 개인식별번호의 부여를 거부할 권리를 가진다고 할 수 있다.[462]

이러한 차원에서 먼저 주민등록번호의 부여가 과연 필요한지 다른 대안은 전혀 없는지를 고려해 보아야 한다. 앞서 고찰한 바에 의하면 영구불변하고 고정적인 개인식별번호를 부여하는 나라는 우리나라 밖에 없었다. 결국 얼마든지 새로운 형태의 방법이 있다는 것이다.

다음으로 꼭 개인식별번호를 부여해야 한다면「주민등록법」에서 그 정당성을 부여하여야 한다. 그러기 위해서는 현행「주민등록법」제7조 제4항에서 규정하고 있는 조항을 개정하여 법규명령에 위임하는 것이 아니라

461) 권건보, 앞의 책, 273면.
462) 김일환, 앞의 주 233), 331면.

법률에서 직접 규정하여야 한다.

생각건대 장기적으로 볼 때 국가의 행정체계도 무시할 수 없기 때문에 어떠한 형태이든 개인을 식별할 수 있는 번호를 부여하는 것은 바람직하다고 본다. 그러나 방법적으로 각각의 번호체계가 인적 동일성을 가급적 덜 노출시키는 형태여야 할 것이다. 그리고 그러한 조건하에서 부여되는 일련번호라 하더라도 영구적인 것이 아니라 변경의 가능성을 열어두는 것이 바람직하다고 본다. 이러한 점에서 표준통일식별번호나 고유식별번호의 체계가 아니라 분야별 비고정적 일련번호의 체계가 요구된다고 할 수 있다. 예컨대 미국이나 프랑스에서처럼 일련번호를 부여하더라도 그것을 요구할 수 있는 범위를 엄격하게 제한하는 입법적 조치가 필요하다고 본다.

또한 인적 동일성을 확인함에 있어서 일차적으로 주민등록번호 이외의 다른 식별요소를 활용할 것을 의무화하는 것도 필요하다. 예를 들면, 인터넷상에서 주민등록번호를 대체할 수 있는 수단으로 공인인증서, 개인인증키, ID 연계 서비스나 가상주민번호, 실명확인 서비스 등이다. 이는 현재 금융서비스에서는 이미 활용되고 있는데, 이를 다양한 분야에 확대 적용하기 위해서 기술적인 분야만 잘 해결된다면 이 또한 훌륭한 대안이 된다고 할 수 있다.

또한 민간부문의 상업적 거래에 있어서 사업자로 하여금 인터넷 사이트 회원가입에서 주민등록번호 수집 제한을 제도화하는 방안이다. 현재 우리나라의 인터넷 사이트는 대부분 회원가입 시 주민등록번호를 요구하고 있다. 이러한 관행 때문에 주민등록번호 자체가 사생활 침해의 위험성을 내포하고 있음에도 불구하고 어쩔 수 없이 주민등록번호를 내주고 있는 상황이다.

그러나 민간 인터넷 사업자의 경우 주민등록번호를 필수항목으로 수집할 정당한 이유가 없다고 생각되며, 대금의 결제를 위하여 꼭 필요한 경우에도 신용카드나 전자서명 등 공인인증서를 활용하도록 하고 주민등록번호는 요구되지 않도록 해야 할 것이다. 미국을 비롯한 대부분의 해외 무료 인터넷사이트의 경우 타켓 마케팅에 필요한 이름과 아이디, 주소와 연령대, 직업 등 최소한의 정보만을 요구하며 그 정보의 정확성을 의무화하지도 않는다.

이와 더불어 과도한 개인정보 수집범위에 대한 업종별 가이드라인을 설

정하는 방법이다. 산업별·업종별 특성을 반영하여 주민등록번호의 수집에 대한 가이드라인을 제시하여 주민등록번호를 수집할 수 있거나 또는 범위를 미리 고지한다면 최소한 정보통신망 사업자들의 주민등록번호 수집 및 오·남용에 따른 피해는 방지할 수 있을 것으로 본다.[463]

또한 항상 주민등록번호와 같은 선상에서 문제가 제기되는 지문날인제도일 것이다. 이 제도에 대하여 그동안 국내외적으로 많은 논란이 제기되어왔다. 우리의 경우 주민등록발급신청서에 열 손가락의 지문을 날인하도록 하고 있으며, 또 그렇게 하여 만들어진 지문정보를 경찰청장이 보관·전산화하고 이를 범죄수사의 목적에 이용하고 있다. 그런데 이는 개인의 인격적 가치를 위협하는 것일 뿐만 아니라 지나치게 정밀한 개인정보를 수집·관리하는 것이어서 자기정보관리통제권을 과도하게 제한하는 것으로 볼 수 있다.

하지만 현재와 같은 제도들을 당장 변경하는 경우 적잖은 비용이 소요될 수 있고, 이에 따르는 여러 가지 혼란도 초래될 수 있다. 따라서 단기적인 대책으로 주민등록번호의 요구를 최소화하는 방향으로 법제를 정비해나가는 것이 무엇보다도 중요하다.

결국 자기정보관리통제권을 위한 주민등록번호의 대안에 효과적으로 대처하기 위해서는 첨단인증기술의 개발과 더불어 주민등록번호를 대체할 수 있는 법제도적 정비방안이 함께 강구되어야 한다.

463) 정연수·김희은, 앞의 논문, 226면.

제5장 결 론

제1절 요약 및 결론

전자정부는 정보통신기술을 기반으로 하여 정부 행정업무의 투명성·효율성·민주성을 확보하고, 전자적 처리와 유기적 연계로 국민과 기업이 원하는 정보와 서비스를 언제 어디서나 쉽게 접근하고 이용할 수 있도록 하는 것을 목표로 한다. 즉 대국민 서비스의 향상과 국민의 기본적 인권이 보장되고 국민주권주의를 실현하기 위함이다. 또 헌법적으로는 전통적인 대의제원리의 변화에 직면하게 함으로써 직접민주주의 가능성을 제시하고, 실질적인 법치주의 구현에 일익을 담당하게 할 수도 있다. 표현의 자유와 관련하여 알 권리의 실현의 방편으로서의 실현에도 변화를 가져온다. 또한 공공기관은 전자정부사업을 위하여 정보의 수집·관리비용의 절감, 서류작성의 부담 경감, 데이터베이스의 중복개발방지, 복지행정정책에 있어 부당한 급부수령자 색출 등을 위하여 행정정보공동이용은 불가피한 실정이다.

그러나 앞서 고찰한 바와 같이, 전자정부사업에는 긍정적 효과만 있는 것이 아니라 부정적인 역기능도 상당수 존재한다. 그 중에서도 가장 큰 문제가 되는 것은 행정정보를 공동이용함에 있어서 개인정보를 어떻게 보호할 것인가하는 것이다. 개인정보가 데이터베이스화되어 공공기관 상호간 공동이용·처리함에 있어 개인정보보호와 정보자기결정권 및 자기정보관리통제권 등의 문제가 중요한 문제로 부각된다. 만약 행정정보공동이용의 장점(경제성·투명성·효율성·편리성·신속성 등)만 생각하여 개인정보공동이용에 일정한 제약을 가하지 않는다면, 개인정보가 행정정보의 공동이용이라는 장점에만 명분을 내세워 무분별하게 공유·처리될 것이다. 만약 그렇게 된다면 개인정보보호를 목적으로 제정된 개인정보보호법 및 개별법에 있는 개인정보보호 관련규정들은 개인정보보호법 내지 개인정보보호를 위한 규정이 아닌 개인정보이용법 내지는 개인정보이용규정으로 전락할 가능성이 있다. 이는 곧 헌법상 인정되는 자기정보관리통제권의 침해와 상실로 이어질 것이다.

이러한 배경하에서 본 연구는 전자정부 구축에 따른 행정정보공동이용

에 있어서 개인정보의 수집·공개·남용·유출 및 도용으로 인한 문제점 및 개인식별번호로 인한 기본권 침해의 위험 등을 검토하고, 우리나라 전자정부와 관련된「전자정부법」및 개인정보보호법제에 나타난 자기정보관리통제권 보장과 관련된 문제점을 분석하여 그 해결을 위한 법률적 제도적 개선책과 정책대안을 제시하고자 하였다.

먼저 전자정부 일반론과 전자정부 구축이 개인에게 미치는 영향을 살펴보고, 전자정부의 법제를 비교법적으로 고찰한 후, 전자정부에서의 나타나는 행정정보공동이용에 대한 헌법적 논의를 하였다. 전자정부의 헌법적 과제는 행정정보공동이용에 있어서 국가구성 원리의 근간이 되는 민주주의와 법치주의의 원용 문제와 국민주권주의에 기초한 국민의 알 권리 등 헌법의 기본원리 및 기본권 관계 등의 보장을 요한다. 또한 입헌주의의 헌법정신에 충실한 전자정부의 지속적인 발전은 개인정보의 보호를 전제로 해야 하며, 개인정보의 보호와 전자정부의 필요성을 조화시키기 위해서는 행정정보공동이용에 있어서 개인정보관리체계의 민주화와 개인정보보호방안이 동시에 확보되어야 한다. 또 개인정보의 효율적인 정보보호체계를 마련하기 위해서는 현행 법제의 개선이 불가피하다고 본다. 전자정부에서의 행정정보를 공동이용하는 법규정들은 개인정보에 해당하는 행정정보의 공동이용에도 적용할 수 있는지 계속해서 검토해야 한다. 즉 행정정보 중에서도 개인정보에 해당하는 행정정보가 포함되어 있기 때문이다. 개인정보에 해당하는 행정정보를 공동이용하는 경우는 곧 정보주체의 기본권인 개인정보의 침해로 이어지고 나아가 자기정보관리통제권의 침해로 이어지기 때문이다. 따라서 전자정부 구현 과정에서 필수적으로 나타나는 개인정보공동이용이 그 정당성을 입증해야 하는 기본권 제한임을 인식해야 한다.

그리고 제3장에서는 전자정부 등장에 따른 개인정보 침해 가능성이 증대되고 있으므로 개인정보공동이용을 새로운 기본권 제한으로서 인식한 바탕에서, 개인정보보호에 관한 비교법적 고찰을 통하여 우리에게 주는 시사점을 도출한 후 개인정보보호법제의 개선책을 논하였다.

첫째, 개인정보와 관련된 행정정보공동이용은 기본권을 제한하고 있기 때문에 반드시 근거법률에 의거해야 하고 이때의 법률은 전자정부법이나 행정절차법과 같은 일반조항이 아닌 전자행정을 위한 행정정보공동이용법을 신설하여 그 법률에 근거하여야 한다.

둘째, 근거 법률에는 공동이용의 목적과 대상정보, 개인정보의 수집범위, 이용범위, 수집방법 등이 명확하게 규정되어 있어야 한다.

셋째, 개인정보에 해당하지 않는 행정정보와 개인정보에 해당하는 개인정보를 구분하여 규정하고 개인정보에 해당하는 행정정보를 공동이용함에 있어서는 공동이용의 요건이나 절차, 범위 등이 보다 엄격하게 규정되어야 한다. 또한 공동이용되는 개인정보 중 정치적·종교적·사상적 신념 등과 같은 민감한 정보는 특별 관리하여 다른 개인정보보호보다 더 많이 보호될 수 있도록 특별히 규율하여야 하며, 수집이나 이용시 반드시 사전동의 절차를 거치도록 하는 명확한 규정이 있어야 한다.

넷째, 개인정보공동이용을 허용하는 기관의 범위를 명확하게 설정할 필요가 있다. 왜냐하면 그 기관이 특정된 목적의식이 없이 개인정보의 보유나 통제의 목적으로 개인정보를 보유해서는 안된다. 따라서 개인정보공동이용의 요건을 엄격하게 설정하고 그 대상기관을 확대하는 경우 개인정보의 보호를 위한 실효적인 관리와 규제가 미치는 영역인가를 반드시 고려해야 한다.

다섯째, 개인정보공동이용이 제한되는 경우와 허용되는 경우를 구분하고, 허용하는 경우에 전자적 조회로 공동이용이 가능한 경우와 개인정보의 송신이 필요한 경우를 구분한 후 전자는 전자조회의 방식으로 공동이용을 허락하되, 송신을 하더라도 그 송신방법을 법률에서 명확히 하여야 한다. 그리고 전달 과정에서 발생할 수 있는 개인정보의 유출을 방지할 수 있는 대책을 강구하여야 한다.

여섯째, 공동이용되는 개인정보의 오류로 인하여 정보주체에게 피해가 발생하지 않도록 개인정보의 최신성과 정확성을 확보하여 개인 데이터의 질을 향상시키고, 합리적인 방안을 강구하여 유통되는 개인정보의 유효기간을 설정할 필요가 있다. 사용이 종료된 개인정보는 정보주체에게 통보와 아울러 즉각 폐기하여야 한다. 그리고 개인정보의 포괄적 노출과 유출 등의 부작용을 최소화하기 위하여 수집·보관의 책임주체가 명확하게 규정되어 책임소재를 분명히 할 수 있어야 한다.

일곱째, 개인정보를 공동이용하기 위해서는 개인정보의 사용계획을 사전에 충분히 수립하고, 목적구속의 원칙에 반하지 않는 범위 안에서 구체화하여 명확하게 규정하여야 한다.

여덟째, 정보주체에게 자기정보관리통제권의 차원에서 또한 정보주체에

게는 어떠한 수단을 통해 어떠한 목적으로 자신의 정보가 제공 또는 이용되는지에 대하여도 설명의무와 알 수 있는 권리가 인정되어야 한다. 이것은 개인정보공동이용으로 인한 권리침해의 위험을 방지하기 위해 단순한 열람권만이 아닌 어떤 목적으로 자신에 관한 정보를 제공하였는지, 또 누구에게 어떻게 전달하였는지에 관한 설명을 들을 권리가 인정되어야 한다. 따라서 법률상 예외적으로 목적 외의 공동이용이나 타기관에 제공이 허용되는 경우라고 하여도 적어도 정보주체에게 그 제공에 관련된 사항을 통지하도록 하고, 정보주체의 이해를 얻지 못한 경우에 대해서는 불복절차도 함께 안내해야 한다.

아홉째, 개인정보를 공동이용하기 위하여 반드시 국제규범을 충족할 수 있는 독립된 개인정보감독기구의 설치가 필요하다.

열째, 현재 미국에서 실행되고 있는 개인정보공동이용을 위한 제도적 장치이자 사전적 권리구제절차로서 개인정보사전영향평가제도의 도입을 고려할 필요가 있다. 이 제도는 개인정보공동이용으로 발생될 문제점을 미리 예방하는 차원에서 국가의 예산절감에도 많은 도움이 있으리라 예상된다.

제4장에서는 전자정부에서의 개인정보보호 문제를 자기 자신에 관한 정보를 스스로 관리·통제할 수 있는 개인의 법적 능력에 주목하여 개인정보보호의 문제를 고찰하였다. 이 분석에서는 개인정보관리통제권을 확보하기 위한 개인정보보호법제의 정비와 개인식별번호제도의 개선방안을 논하였다. 여기에서는 개인정보보호의 문제를 헌법상 자기정보관리통제권의 보장이라는 측면에서 접근할 필요가 있음을 밝히고, 이 권리를 자신에 관한 정보의 흐름을 자율적으로 컨트롤 할 수 있는 기본권으로 정의하였다.

우리 헌법은 자기정보관리통제권에 대한 명문의 규정을 두고 있지 않아 자기정보관리통제권에 대한 헌법적 근거 조항이 무엇인가에 대해 학설과 판례가 심하게 대립되어 있다. 자기정보관리통제권의 헌법적 근거에 대하여 헌법 제10조의 인간의 존엄과 가치조항에서 구하는 입장, 헌법 제17조와 제16조(주거의 자유)와 제18조(통신비밀의 자유)에서 구하는 입장, 헌법 제10조와 제16조·제17조·제18조에서 구하는 입장, 헌법 제10조와 제17조에서 구하는 입장 등이 있다. 생각건대, 우리 헌법이 미국이나 독일과 달리 제10조와 제17조를 별도로 규정한 헌법정신의 살려 조화로운 해석을 하기 위해서는 제10조의 인간의 존엄과 가치 및 행복추구권에 근거를 두

고 있는 일반적 인격권과 제17조의 사생활의 비밀과 자유조항에서 자기정보관리통제권의 근거를 찾는 것이 현실적으로 타당하리라고 본다.

개인정보의 보호에 있어서는 무엇보다도 정보주체에 의한 자기정보의 관리 및 그 정보에 대한 사전통제가 가장 중요하다고 할 것이다. 수집자로서의 정부와 보호자로서의 정부 사이의 태생적 갈등은 자기정보관리통제권을 보장하기 위한 국가 입법 활동에 대한 신뢰를 의심하게 되므로 정보주체의 자기정보관리통제권을 보다 강화할 필요가 있다.

자기정보관리통제권은 개인의 의사소통능력을 보장함을 목적으로 하고 이는 민주사회에 있어서 필수요건이라 할 것이다. 그러나 자기정보관리통제권도 무제한으로 보장되는 것은 아니며 헌법 제37조 제2항의 규정에 따라 일정한 제한이 따르게 된다. 이러한 자기정보관리통제권은 법률적 근거에 의하여 제한할 수 있다. 개인의 기본권인 자기정보관리통제권을 제한하기 위해서 법률은 규범명확성의 원칙에 따라 자신에 관한 정보가 어떤 구체적인 목적들을 위하여 필요한지를 정보주체가 명확하게 인식할 수 있도록 규정되어야 하고, 비례의 원칙 내지 과잉금지원칙은 개인정보보호에서는 특히 목적구속의 원칙, 수집제한의 원칙, 정확성·안전성의 원칙, 정보분리의 원칙, 시스템공개의 원칙 등으로 나타난다.

앞서 고찰한 바와 같이 우리나라는 개인정보보호를 위한 일반법 또는 기본법이 제정되어 있지 않다. 또한 공공부문의 개인정보보호의 일반법이라 할 수 있는「공공기관의 개인정보보호에 관한 법률」은 전산으로 처리되지 않은 개인정보는 그 보호대상에서 제외하고 있고 목적 외 이용 및 제공에 대한 예외가 너무 광범위하게 규정되어 있다. 그리고 민간부문에서는 개별법에 의한 규제와 자율규제를 병행하고 있으나,「정보통신망 이용촉진 및 정보보호등에 관한 법률」역시 전산으로 처리된 개인정보만을 보호대상으로 삼고 있어 수기로 처리된 정보는 보호대상에서 제외하고 있다. 더 나아가 공공부문이나 민간부문에 의한 무차별적인 개인정보의 수집·저장, 효율적인 통제방안 결여, 국민의 낮은 개인정보보호의식 등으로 인해 개인정보보호법들이 많이 제정되어 있음에도 불구하고 개인정보의 보호는 만족할 만한 수준에 이르지 못하고 있다.

그리고 우리나라의 개인정보보호법제는 외국의 법제와 비교해 볼 때, 개인정보보호에 관한 종합 일반법의 불비, 개인정보보호전담기구 미비 등 아직도 미흡한 점이 많이 있다. 따라서 인터넷 강국 내지 세계적 수준의

지식정보화사회의 달성을 목표로 하고 있는 우리나라는 그 규격에 충족하는 개인정보보호법제를 구비하여 개인의 사생활보호와 자기정보관리통제권을 확보하는데 만전을 기함으로써 인권보장이라는 법적 과제와 정보사회에서 정보공유 및 커뮤니케이션 보장에서 적절한 조화와 균형을 찾아야 할 것이다.

이를 위하여 첫째, 개인정보보호에 관한 종합적인 기본법을 제정하여야 한다. 이 법에서는 특히 정보조사나 수집의 단계에서부터 개인정보를 보호하도록 하여야 하고, 수집이 불가피한 경우는 반드시 정보주체인 당사자의 사전동의를 구하는 절차가 마련되어야 한다.

둘째, 우리나라에서도 국제기구 및 외국의 사례를 참조하여 국제규범에 충족하는 독립된 권한을 가진 개인정보보호전담기구를 설립해야 한다. 이 기구는 개인정보처리가 합법적으로 이루어지고 있는지를 감독하고 개인정보에 관한 분쟁이 발생한 경우 이를 신속하게 조정·해결함으로써 정보주체의 권익을 보호할 수 있도록 한다.

셋째, 프라이버시 내지 개인정보는 한 번 침해되고 나면 거의 원상회복이 불가능한데다 그 회복에 있어서도 많은 비용이 소요되는 점을 감안하여 우리나라에서도 미국에서와 같이 프라이버시 영향평가제도를 도입함으로써 개인정보 침해 가능성을 가급적 줄여 나가야 한다.

넷째, 그 무엇보다도 중요한 것은 국민 개개인에게 부여하는 주민등록번호제도이다. 강제로 개인에게 부여하는 개인식별번호로서 우리나라에서는 그 사람 개인을 몰라도 주민등록번호만 알면 그 개인의 신상에 대하여 뿐만 아니라 그 개인의 공적생활 및 사적생활의 모든 분야에 대하여 상세히 알 수 있어 개인정보보호의 측면에서 부정적인 측면이 너무 많다. 따라서 강제 부여되고, 영구불변한 주민등록번호부여 제도는 위헌적인 소지가 많은 만큼 하루 빨리 폐지 내지는 개선하는 것이 시급하다.

다섯째, 개인정보보호를 위한 국민의 법의식을 앙양하는 것이다. 우리나라는 아직 국가나 기업 및 국민의 개인정보보호 의식이 희박할 뿐 아니라 개인정보보호를 위한 법제도 및 기술이 제대로 확립되지 못해 개인정보보호 문화가 확립되어 있지 않은 실정이다. 아무리 훌륭한 개인정보보호 법제를 구비하고 있다고 하더라도 정부나 기업 및 국민들의 개인정보보호에 대한 법의식이 뒷받침되어 있지 않으면 그 실효성을 확보하기 쉽지 않을 것이다. 따라서 국가는 개인정보보호 관련 법률의 정비와 아울러 개인정

보보호를 위한 적극적인 교육과 홍보활동을 전개해 나가야 할 것이다. 그리고 국민 개개인인 정보주체도 자신의 정보가 어떻게 오·남용되고 있는가에 대하여 늘 관심을 가지고 자신에게 주어진 권리행사와 권리보호에 적극적인 자세를 취해야 한다.

마지막으로 전자정부 구축에 따른 행정정보공동이용에 있어서 개인정보의 침해 내지는 남용이 심각하므로 시급히 대책을 수립하여 전자행정의 활성화와 개인정보보호를 동시에 만족시킬 수 있는 법률을 제정해야 한다.

제2절 「(가칭)행정정보공동이용에 관한 법률(안)」 제안

이 연구는「전자정부법」,「행정정보공동이용법(안)」,「전자정부법개정안」등의 문제점을 고찰하고, 이에 대한 이론과 외국의 법제 분석을 바탕으로, 전자정부의 행정정보공동이용에 있어서 자기정보관리통제권을 확보할 수 있도록 다음과 같은「(가칭)행정정보공동이용에 관한 법률(안)」이 제정되어야 한다고 제안한다. 이 법안은 2006년 11월 14일 정부가 제출한「행정정보공동이용법안」을 그대로 활용하면서 행정정보공동이용에 있어서 개인정보보호 및 자기정보관리통제권의 보호에 관한 내용을 반영한 것이다.[464]

「(가칭)행정정보공동이용에 관한 법률(안)」

제1장 총칙

제1조(목적) 이 법은 행정정보의 공동이용을 위한 기본원칙, 절차, 추진체계와 일반 행정정보 및 개인정보의 보호 등에 관하여 필요한 사항을 규정함으로써 민원사항의 신청에 따른 국민의 불편을 없애고 행정업무의 효율을 증대함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

464) 법안 중 밑줄 친 부분은 정부안에 대하여 수정한 부분이다.

1. “행정정보”라 함은 행정기관과 공공기관이 직무상 작성·취득하여 유지·관리하는 부호, 문자, 음성, 음향 및 영상 등의 전자적 자료를 말한다.
2. “공동이용”이라 함은 행정정보의 전부나 일부를 이 법이 정한 절차에 따라 보유기관이 전자적 체계를 통하여 연계함으로써 이용기관이 조회하거나 전송받는 것을 말한다.
3. “행정기관”이라 함은 중앙행정기관과 그 소속기관, 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 지방자치단체를 말한다.
4. “공공기관”이라 함은 다음 각 목의 어느 하나에 해당하는 기관을 말한다.
 가. 「정부투자기관관리기본법」에 따른 정부투자기관
 나. 「지방공기업법」에 따른 지방공사와 지방공단
 다. 특별법에 따라 설립된 특수법인
 라. 그 밖에 대통령령이 정하는 법인·기관 및 단체
5. “금융기관”이라 함은 다음 각 목의 어느 하나에 해당하는 기관을 말한다.
 가. 「은행법」 제8조 제1항에 따라 은행업의 인가를 받은 자
 나. 「한국산업은행법」에 따른 한국산업은행
 다. 「중소기업은행법」에 따른 중소기업은행
 라. 「한국수출입은행법」에 따른 한국수출입은행
 마. 「농업협동조합법」에 따른 농업협동조합과 그 중앙회
 바. 「수산업협동조합법」에 따른 수산업협동조합과 그 중앙회
 사. 그 밖에 법률에 따라 금융업무를 행하는 기관으로서 대통령령이 정하는 기관
6. “보유기관”이라 함은 제6조에 따른 행정정보를 보유하는 행정기관이나 공공기관으로서 행정정보를 직무상 작성·취득하여 유지·관리하는 기관을 말한다.
7. “이용기관”이라 함은 다음 각 목의 어느 하나에 해당하는 기관 중 제9조제1항에 따라 행정안전부장관의 승인을 받아 행정정보를 조회하거나 전송받는 기관을 말한다.
 가. 행정기관

나. 공공기관
다. 금융기관
라. 그 밖에 민원사항의 처리를 소관 사무로 하는 기관으로서 대통령령이 정하는 기관

8. “정보주체”라 함은 행정정보에 의하여 식별되는 자로서 그 정보의 주체가 되는 자를 말한다.
9. “표준화”라 함은 행정정보의 수집·보존·전송 및 기타 공동이용을 위하여 필요한 표준 규격을 제정·관리하는 것을 말한다.

제3조(적용범위) 행정정보의 공동이용에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법이 정하는 바에 따른다.

제4조(적정이용의 원칙) 행정정보의 공동이용은 이용목적에 부합하도록 필요한 범위에서 정해진 절차에 따라 정당하게 이루어져야 한다.

제5조(상호협조의 원칙) 보유기관과 이용기관은 해당 사무를 원활하게 처리하기 위하여 상호협조하여 행정정보를 공동이용하여야 한다.

제2장 공동이용의 내용 및 절차

제6조(공동이용 행정정보) ① 행정기관과 공공기관이 정보주체가 동의한 행정정보를 이 법이 정하는 절차에 따라 공동이용할 수 있는 행정정보는 다음 각 호와 같다.

1. 별표에 규정된 행정정보
2. 제1호 외의 행정정보로서 민원사항과 행정업무를 효율적으로 처리하기 위하여 공동이용할 필요성이 특히 높다고 인정되어 다른 법률에서 정하는 행정정보

② 행정기관과 공공기관은 정보주체가 동의한 행정정보를 이 법이 정하는 절차에 따라 공동이용할 수 있다. 이용대상은 제1항에 따른 행정정보의 범위에서 국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙이나 대통령령으로 정한다.

③ 행정기관은 제1항의 행정정보 외에 국가정책의 수립과 행정업무를 수행하기 위한 주요 판단자료로서 특정 개인을 식별할 수 없는 형태로 가공된 행정정보(이하 “정책정보”라 한다)를 공동이용할 수 있다.

제7조(공동이용의 신청) ① 제2조 제7호 각 목의 어느 하나에 속하는 기

관 중 행정정보를 공동이용 하고자 하는 기관은 공동이용의 목적, 공동이용 대상 행정정보와 그 보유기관을 특정하여 행정안전부장관에게 공동이용을 신청하여야 한다.

② 공동이용의 신청절차는 대통령령으로 정한다.

제8조(공동이용의 승인) ① 행정안전부장관은 제7조 제1항에 따른 공동이용의 신청을 받은 경우에는 대통령령이 정하는 바에 따라 공동이용의 목적, 공동이용 대상 행정정보와 그 범위, 그 밖에 공동이용의 조건을 정하여 이를 승인할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 공동이용을 승인하여서는 아니된다.

1. 공동이용을 신청한 행정정보가 공동이용기관 고유의 직무수행에 필요하다고 인정되지 아니하는 경우
2. 신청기관 및 그 소속직원이 제23조·제24조 및 제26조에 따른 의무를 이행하지 못할 상당한 이유가 있다고 인정되는 경우
3. 신청기관의 담당사무의 성질 또는 처리업무의 분량 등에 비추어 공동이용이 비효율적이라고 인정되는 경우
4. 공동이용을 신청한 행정정보가 다른 법률 또는 법률이 위임한 명령(국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙·대통령령·총리령·부령 및 조례·규칙에 한한다)에서 비밀 또는 비공개 사항으로 규정된 경우
5. 공동이용을 신청한 행정정보가 국가안전보장, 국방, 통일, 외교관계 등에 관한 사항으로서 공동이용할 경우에는 국가의 중대한 이익을 매우 크게 해칠 우려가 있다고 인정되는 경우
6. 그 밖에 이 법에 따른 공동이용의 목적이나 행정정보의 안전성과 신뢰성을 해칠 우려가 있다고 인정되는 경우로서 대통령령이 정하는 경우

② 행정안전부장관은 제1항에 따른 공동이용을 승인하는 경우에는 보유기관과 미리 협의한 후 제15조에 따른 행정정보공동이용위원회의 심의를 거쳐야 한다. 이 경우 보유기관은 특별한 사유가 없으면 협의에 응하는 등 공동이용에 적극 협조하여야 한다.

제9조(심사·승인 등의 의제) ① 신청기관이 제8조제1항에 따라 공동이용의 승인을 받은 경우에 다음 각 호의 어느 하나에 해당하는 사항이 포함되어 있는 때에는 그 행정정보는 다음 각 호에 해당하는 규정에 따라

신청기관에게 제공할 수 있는 행정정보로 본다.

1. 「국세기본법」 제81조의8 제1항 각 호 외의 부분 단서
2. 「관세법」 제116조 제1항 각 호 외의 부분 단서
3. 「지방세법」 제69조 제1항의 각 호 외의 부분 단서

② 신청기관이 제8조 제1항에 따라 공동이용의 승인을 받은 경우에 다음 각 호의 어느 하나에 해당하는 사항이 포함되어 있는 때에는 그 행정정보에 대하여 다음 각 호의 어느 하나에 따른 심사·승인 등을 받은 것으로 본다.

1. 「부동산등기법」 제177조의5 제3항에 따른 등기전산정보자료의 이용·활용에 관한 심사·승인 및 협의
2. 「호적법」 제124조의6 제1항에 따른 호적전산정보자료의 이용·활용에 관한 심사·승인 및 협의
3. 「주민등록법」 제18조의2 제1항에 따른 주민등록전산정보자료의 이용·활용에 관한 심사 및 승인
4. 「지적법」 제15조 제1항에 따른 지적전산자료의 이용·활용에 관한 심사 및 승인
5. 「자동차관리법」 제69조제2항에 따른 자동차전산자료의 이용에 관한 심의 및 승인
6. 「건축법」 제25조의4 제2항에 따른 건축전산자료의 이용에 관한 심사 및 승인
7. 「상업등기법」 제16조 제2항에 따른 등기전산정보자료의 이용에 관한 심사 및 승인

제10조(공동이용 승인의 철회 및 중단) ① 행정안전부장관은 이용기관 또는 그 소속직원이 다음 각 호의 어느 하나에 해당하는 경우에는 제15조에 따른 행정정보공동이용위원회의 심의를 거쳐 해당 이용기관에 대한 공동이용의 승인을 철회할 수 있다.

1. 제23조·제24조 및 제26조에 따른 의무를 위반한 경우
2. 공동이용을 신청한 후에 제8조 제1항 각 호의 어느 하나에 해당하는 사유가 발생한 경우
3. 제8조 제1항 각 호 외의 부분에 따라 정한 공동이용의 조건을 위반한 경우
4. 그 밖에 제1호 내지 제3호에 준하는 사유로 행정정보의 공동이용을

금지하여야 할 불가피한 사유가 있는 경우

② 행정안전부장관은 제1항에 불구하고 제1항 각 호에 해당하는 사유가 일시적으로 발생하였다고 인정되는 경우에는 제15조에 따른 행정정보 공동이용위원회의 심의를 거쳐 그 발생 원인이 해소될 때까지 해당 이용기관의 공동이용을 중단시킬 수 있다.

③ 행정안전부장관은 제1항이나 제2항에 따라 공동이용의 승인을 철회하거나 공동이용을 중단시키고자 하는 경우에는 해당 이용기관의 의견을 들어야 한다.

④ 보유기관은 소관 행정정보를 공동이용하는 이용기관이나 그 소속직원이 제1항 각 호의 어느 하나에 해당하는 경우에는 해당 이용기관의 공동이용을 중단시키거나 공동이용의 승인을 철회하여 줄 것을 행정안전부장관에게 요청할 수 있다.

⑤ 행정안전부장관은 제1항이나 제2항에 따라 공동이용의 승인을 철회하거나 공동이용을 중단시킨 경우에는 그 사유를 명시하여 해당 이용기관과 보유기관에게 통지하여야 한다.

⑥ 이용기관은 제1항이나 제2항에 따라 공동이용의 승인이 철회되거나 공동이용이 중단된 때에 이미 전송받은 자료가 있는 경우에는 해당 행정정보를 즉시 파기하고 행정안전부장관에게 그 사실을 통보하여야 한다.

제11조(공동이용의 사전동의) ① 이용기관이 행정정보를 공동이용하는 경우에는 정보주체가 다음 각 호의 사항을 알 수 있도록 하여 정보주체의 사전동의를 받아야 한다.

1. 공동이용의 목적
2. 공동이용 대상 행정정보
3. 공동이용의 범위
4. 공동이용 이용기관의 명칭

② 제1항에 불구하고 이용기관이 다음 각 호의 어느 하나에 해당하는 경우로서 이용기관은 그 행정정보를 공동이용한 후에 국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙이나 대통령령이 정하는 바에 따라 제1항 각 호의 사항을 정보주체가 알 수 있도록 하여야 한다.

1. 정보주체의 생명 또는 신체의 보호를 위하여 긴급하게 공동이용할

필요가 있는 경우

2. 기타 제1호에 준하는 경우로서 법령에서 정하는 업무를 수행하기 위하여 필요한 경우로서 정보주체의 사전동의를 받는 것이 그 업무의 성질에 비추어 현저히 부적합하다고 인정되는 경우

③ 제2항에 따라 정보주체의 사전동의 없이 공동이용할 수 있는 소관업무와 행정정보의 구체적인 범위는 국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙이나 대통령령으로 정한다.

제12조(공동이용) ① 이용기관은 특별한 사유가 있는 경우를 제외하고는 자료를 조회하는 방식으로 행정정보를 공동이용 하여야 한다.

② 이용기관은 정보주체에게 제16조에 따른 행정정보공동이용센터(이하 "행정정보공동이용센터"라 한다)가 구축·운영하는 전자적 체계(이하 "행정정보공동이용체계"라 한다)를 통하여 전자적으로 확인할 수 있는 자료를 제출하도록 요구하여서는 아니된다.

③ 보유기관은 행정정보처리의 정확성·최신성 및 안전성이 유지되도록 노력하여야 하며, 행정안전부장관이 요청하는 행정정보를 공동이용하기 위하여 필요한 조치를 취하여야 한다.

④ 이용기관은 제7조 내지 제11조에 따른 절차에 의하지 아니하고 공동이용 행정정보를 다른 기관에게 다시 제공하여서는 아니된다.

제13조(정책정보의 공동이용) ①행정기관은 국가정책의 수립과 행정업무의 수행을 위하여 필요한 경우에는 행정안전부장관에게 정책정보의 생성·제공을 요청할 수 있다.

② 행정안전부장관은 제1항에 따라 정책정보의 생성·제공을 요청받은 때에는 관련 행정정보 보유기관과의 협의한 후 제15조에 따른 행정정보공동이용위원회의 심의를 거쳐 이에 응할 수 있다.

③ 행정안전부장관은 정책정보를 생성·제공하기 위하여 필요한 경우에는 보유기관에 해당 행정정보의 제공을 요청할 수 있다. 이 경우 보유기관은 그 행정정보를 특정 개인을 식별할 수 없는 형태 등으로 가공하여 행정안전부장관에게 제공하여야 한다.

제3장 공동이용의 추진체계

제14조(공동이용기본계획의 수립) ①국가는 행정정보의 공동이용을 촉진

하기 위하여 3년의 기간을 단위로 하는 행정정보공동이용기본계획(이하 “기본계획”이라 한다)을 수립하여야 한다.

② 기본계획은 행정안전부장관이 관계행정기관의 부문계획을 종합하여 수립하고, 제15조에 따른 행정정보공동이용위원회(이하 “행정정보공동이용위원회”라 한다)의 심의를 거쳐 확정한다.

③ 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 행정정보공동이용의 기본 방향에 관한 사항
2. 행정정보의 구축 및 표준화 방안에 관한 사항
3. 행정정보의 현황, 수요와 공급 및 그 대책에 관한 사항
4. 행정정보공동이용의 실태조사 및 보안대책의 수립에 관한 사항
5. 행정정보공동이용 관련 교육에 관한 사항
6. 정책정보의 가공·활용에 관한 사항
7. 그 밖에 행정정보공동이용의 추진 및 확대를 위하여 필요한 사항

④ 행정안전부장관은 제2항에 따라 수립된 기본계획을 「정보화촉진기본법」 제5조제2항에 따른 관계중앙행정기관별 부문계획에 포함시켜야 한다.

⑤ 관계중앙행정기관의 장과 지방자치단체의 장은 소관 주요정책을 수립하고 집행하는 경우에는 기본계획에 포함되어 있는 사항을 우선적으로 고려하여야 한다.

제15조(행정정보공동이용위원회) ① 행정정보의 공동이용에 관한 주요정책을 수립하고 중요사항을 심의하기 위하여 대통령 소속하에 행정정보공동이용위원회를 둔다.

② 행정정보공동이용위원회는 다음 각 호의 사항을 심의한다.

1. 기본계획에 관한 사항
2. 공동이용 행정정보 및 이용기관의 추가·변경에 관한 사항
3. 제8조 및 제10조에 따른 공동이용의 승인·철회 및 중단 등에 관한 주요 사항
4. 행정정보공동이용의 정보 보호 및 보안 대책에 관한 사항
5. 행정정보공동이용의 제도 개선에 관한 사항
6. 정책정보의 이용에 관한 사항
7. 그 밖에 행정정보공동이용의 촉진 및 관련 정책에 관한 사항

③ 행정정보공동이용위원회의 위원장은 국무총리와 행정정보의 공동이용에 관한 학식과 경험이 풍부한 자 중에서 대통령이 위촉하는 자가 공

동으로 된다.

④ 위원장은 각자 위원회를 대표하며, 위원회의 업무를 통할한다.

⑤ 행정정보공동이용위원회는 위원장 2인을 포함한 20인 이내의 위원으로 구성한다.

⑥ 행정정보공동이용위원회의 위원은 다음 각 호의 자가 된다.

1. 국회사무총장
2. 법원행정처장
3. 관계 중앙행정기관의 장 중에서 국무총리인 위원장이 임명하는 자
4. 행정정보의 공동이용에 관하여 학식과 경험이 풍부한 자 중에서 국무총리인 위원장이 다른 위원장과 협의하여 위촉하는 자

⑦ 위원 중 공무원이 아닌 위원의 임기는 3년으로 하되, 연임할 수 있다.

⑧ 행정정보공동이용위원회를 효율적으로 운영하기 위하여 실무위원회와 간사 1인을 두되, 간사는 행정안전부장관이 된다.

⑨ 행정정보공동이용위원회의 운영과 실무위원회의 구성·운영, 그 밖에 행정정보공동이용위원회에 관하여 필요한 사항은 대통령령으로 정한다.

제16조(행정정보공동이용센터) ① 정부는 행정정보의 공동이용에 필요한 시책을 효율적으로 추진하기 위하여 「전자정부법」 제22조 제4항에 따른 행정정보공동이용센터로 하여금 다음 각 호의 업무를 처리하게 할 수 있다.

1. 행정정보공동이용에 필요한 안정적인 공동이용체계의 구축·관리
2. 보유기관이 보유하고 있는 행정정보의 조사 및 그 목록의 작성·배포
3. 이용기관이 공동이용을 필요로 하는 행정정보에 대한 수요 조사
4. 공동이용의 촉진을 위한 행정정보와 사무처리절차 등의 표준화
5. 이용기관이 공동이용한 행정정보의 유지·관리
6. 공동이용의 신청과 승인 등 행정안전부장관의 행정사무의 처리
7. 공동이용의 목적 및 이용기관의 보안수준 등을 고려한 접근 권한의 등록 및 관리
8. 공동이용 기록의 유지·관리와 보유기관·이용기관에 대한 실태조사 및 보안 점검
9. 정책정보의 생성·제공

10. 보유기관과 이용기관에 대한 행정정보공동이용 관련 사항의 교육
11. 다른 법률에 따라 행정기관·공공기관 또는 금융기관 사이에 행하여지는 행정정보의 제공·이용의 연계·중계
12. 그 밖에 이 법 또는 다른 법령에서 행정정보공동이용센터의 업무로 정하거나 행정정보공동이용센터에 위탁한 업무

② 제1항에 따른 업무의 처리에 관하여 필요한 사항은 대통령령으로 정한다.

제4장 행정정보의 보호

제17조(공동이용 기록의 공개) 행정안전부장관은 대통령령이 정하는 바에 따라 이용기관이 공동이용한 행정정보의 명칭, 공동이용 횟수 및 공동이용한 시간 등의 기록을 유지·관리하고 이를 공개하여야 한다.

제18조(공동이용 행정정보의 열람) ① 행정안전부장관은 제16조 제1항 제5호에 따라 행정정보공동이용센터가 유지·관리하는 행정정보 중 해당 이용기관이 공동이용한 행정정보를 대통령령이 정하는 바에 따라 그 이용기관이 그 필요에 따라 열람하거나 사본·복제물의 제공(이하 "열람 등"이라 한다)을 받을 수 있도록 하여야 한다. 이 경우 행정안전부장관은 열람 등의 목적과 정당한 접근권한의 유무 등을 확인하여야 한다.

② 정보주체는 행정안전부장관·행정정보공동이용센터·이용기관에게 공동이용한 행정정보 중 본인에 관한 행정정보의 열람 등을 신청할 수 있다.

③ 행정안전부장관·행정정보공동이용센터·이용기관은 제2항에 따른 정보주체의 신청이 있는 때에는 특별한 사유가 없는 한 신청한 날부터 15일 이내에 제1항에 따른 절차를 거쳐 그 정보주체에게 신청한 행정정보에 대한 열람 등을 할 수 있도록 하여야 한다.

④ 제2항 및 제3항에 따른 열람 등에 관한 절차 등에 관하여 필요한 사항은 국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙이나 대통령령으로 정한다.

제19조 (처리정보의 정정 및 삭제 등) ① 제18조에 따라 본인의 처리정보를 열람한 정보주체는 행정안전부장관·행정정보공동이용센터·이용기관의 장에게 문서로 당해 처리정보의 정정 또는 삭제를 청구할 수 있

다. 다만, 다른 법률에 당해 처리정보가 수집대상으로 명시되어 있는 경우에는 그 삭제를 청구할 수 없다.

② 행정안전부장관·행정정보공동이용센터·이용기관의 장은 제1항의 규정에 의한 정정 또는 삭제청구를 받은 때에는 처리정보의 내용의 정정 또는 삭제에 관하여 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다.

③ 행정안전부장관·행정정보공동이용센터·이용기관의 장은 제2항의 규정에 의한 조사를 함에 있어 필요한 때에는 당해 청구인으로 하여금 정정 또는 삭제청구사항의 확인에 필요한 증빙자료를 제출하게 할 수 있다.

제20조 (불복청구) ① 제18조 제1항 및 제19조 제1항에 따른 청구에 대하여 행정안전부장관·행정정보공동이용센터·이용기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 「행정심판법」으로 정하는 바에 따라 행정심판을 청구하거나 「행정소송법」으로 정하는 바에 따라 행정소송을 제기할 수 있다.

제21조(공동이용에 따른 보안관리) ① 행정안전부장관은 행정정보를 공동이용함에 있어서 이용기관에 대하여 다음 각 호의 사항이 포함된 보안에 관한 규정을 대통령령이 정하는 바에 따라 제정·시행하는 등 보안관리에 필요한 대책을 마련하여야 한다.

1. 공동이용 행정정보의 암호화에 관한 사항
2. 제2항에 따른 행정정보공동이용에 필요한 시설과 전자적 체계의 설치·운용 기준, 필요한 보안기술 및 보안관리 인력의 배치 기준에 관한 사항
3. 제4항에 따른 준수사항에 관한 규정에 포함되는 사항
4. 기타 공동이용 행정정보의 안전성과 신뢰성 유지에 필요한 사항

② 이용기관은 행정정보공동이용에 필요한 시설과 전자적 체계를 설치·운용함에 있어서 위조·변경·훼손의 방지에 필요한 보안기술을 적용하여야 한다.

③ 이용기관은 행정정보를 공동이용함에 있어서 공동이용 행정정보의 안전성, 신뢰성 및 보안관리의 총괄책임이 있는 자(이하 “보안관리책임자”라 한다), 그 이용기관의 분장업무 수행을 위하여 설치된 조직에 따

른 보안관리의 책임이 있는 자(이하 “분임보안관리책임자”라 한다)와 보안업무담당자를 지정·운영하여야 한다.

④ 이용기관은 제3항에 따른 보안관리책임자, 분임보안관리책임자 및 보안담당자의 준수사항에 관한 규정을 정하여 이를 행정안전부장관에게 통보하여야 한다. 통보한 내용을 변경하는 때에도 또한 같다.

제22조(접근권한의 등록) ① 이용기관은 다음 각 호에 해당하는 사항을 대통령령이 정하는 바에 따라 행정안전부장관에게 등록하여야 한다. 이미 등록한 사항을 변경하고자 하는 때에도 또한 같다.

1. 이용기관의 장
2. 그 이용기관의 소속 업무 담당자에게 행정정보에 접근할 수 있는 권한을 부여할 권한이 있는 자
3. 공동이용을 통하여 처리하는 소관업무와 그 업무에 접근할 권한을 가진 자

② 제1항에 따라 등록한 자가 행정정보를 공동이용할 때에는 「전자정부법」 제2조제6호에 따른 행정전자서명 또는 「전자서명법」 제2조제3호에 따른 공인전자서명을 사용하여야 한다.

제23조(행정정보공동이용체계의 보호) 누구든지 행정정보공동이용체계를 위법한 방법으로 위조·변경·훼손하거나 이용하여서는 아니된다.

제24조(비밀누설 등의 금지) 행정정보를 공동이용하는 사무에 종사하거나 종사하였던 자는 업무상 알게 된 비밀을 누설하거나 목적 외의 용도로 사용하여서는 아니된다.

제5장 보칙

제25조(수수료) 이용기관은 행정정보공동이용으로 인하여 특별한 이익을 얻는 경우에는 대통령령이 정하는 바에 따라 행정안전부장관에게 수수료를 납부하여야 한다.

제26조(금지행위) 이용기관의 소속 직원은 다음 각 호에 해당하는 행위를 하여서는 아니된다.

1. 행정정보를 제9조 제1항에 따라 승인받은 공동이용의 목적 외의 용도로 사용하는 행위
2. 제8조 제1항에 따른 승인을 받지 아니하고 공동이용하는 행위

3. 제8조 제1항에 따른 승인을 받은 공동이용의 범위를 넘어서 공동이용하는 행위
4. 제10조에 따른 공동이용의 승인철회 또는 중단 후에 공동이용하는 행위
5. 공동이용 행정정보를 행정안전부장관의 승인 없이 다른 기관에게 다시 제공하는 행위
6. 제22조에 따른 접근권한을 등록하지 아니하고 공동이용하는 행위
7. 접근권한을 가지지 아니하고 공동이용하는 행위
8. 공동이용 행정정보를 위법한 방법으로 위조·변경·훼손하는 행위
9. 공동이용 행정정보를 해당 처리업무 단위별로 열람하거나 출력하여 사용하는 외에 다른 컴퓨터나 저장장치 등에 저장하는 행위. 다만, 정책정보를 공동이용 하는 경우를 제외한다.

제27조(공무원의제) 제15조 제2항에 따른 행정정보공동이용위원회의 위원장 및 위원 중 공무원이 아닌 자와 행정정보의 공동이용에 관한 사무에 종사하는 자 중 공무원이 아닌 자는 「형법」 제129조 내지 제132조의 적용에 있어 공무원으로 본다.

제7장 벌칙

제28조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
1. 제11조 제1항을 위반하여 정보주체로부터 사전 동의를 얻지 아니한 자
2. 제23조를 위반하여 행정정보공동이용체계를 위법한 방법으로 위조·변경·훼손하거나 이용한 자
3. 제26조 제1호 내지 제8호 중 어느 하나를 위반하여 금지행위를 한 자

② 다음 각호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
1. 제24조를 위반하여 업무상 비밀을 누설하거나 목적 외의 용도로 사용한 자
2. 제10조 제6항을 위반하여 해당 행정정보를 파기하지 아니한 자
3. 제26조 제9호 본문을 위반하여 다른 컴퓨터나 저장장치 등에 저장한 자

③ 거짓 그 밖의 부정한 방법으로 행정정보를 열람 또는 제공받은 자는

2년 이하의 징역 또는 700만원 이하의 벌금에 처한다.

제29조(과태료) ① 다음 각호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에 처한다.

1. 제10조 제6항을 위반하여 행정안전부장관에게 통보하지 아니한 자
2. 제12조 제1항을 위반하여 행정정보의 공동이용에 있어 특별한 사유없이 자료를 조회하는 방식을 채택하지 아니한 이용기관
3. 제12조 제2항을 위반하여 이용기관은 정보주체에게 제16조에 따른 행정정보공동이용센터가 구축·운영하는 전자적 체계를 통하여 전자적으로 확인할 수 있는 자료를 제출하도록 요구하는 행위
4. 제12조 제3항을 위반하여 행정정보처리의 정확성·최신성 및 안전성이 유지되도록 노력하여야 하며, 행정안전부장관이 요청하는 행정정보를 공동이용하기 위하여 필요한 조치를 취하지 아니한 행위.
5. 제18조 제3항을 위반하여 정보주체의 열람 청구에 따른 필요한 조치를 취하지 아니한 자
6. 제21조 제2항을 위반하여 보안기술을 적용하지 아니한 자
7. 제21조 제3항을 위반하여 보안관리책임자·분임보안관리책임자 및 보안업무담당자를 지정·운영하지 아니한 자
8. 제21조 제4항을 위반하여 준수사항에 관한 규정을 정하지 아니하거나 이를 행정안전부장관에게 통보하지 아니한 자

② 제1항에 따른 과태료는 대통령령이 정하는 바에 따라 행정안전부장관이 부과·징수한다.

③ 제2항에 따른 과태료부과에 불복하는 자는 그 처분의 고지를 받은 날부터 30일 이내에 행정안전부장관에게 이의를 제기할 수 있다.

④ 제2항에 따라 과태료 처분을 받은 자가 제3항에 따라 이의를 제기한 때에는 행정안전부장관은 지체 없이 관할법원에 그 사실을 통보하여야 하며, 그 통보를 받은 관할법원은 「비송사건절차법」에 의한 과태료의 재판을 한다.

⑤ 제3항에 따른 기간 내에 이의를 제기하지 아니하고 과태료를 납부하지 아니한 때에는 국세체납처분의 예에 따라 이를 징수한다.

참고 문헌

1. 국내문헌

1) 단행본

강경근, 헌법, 법문사, 2004.

고영삼, 전자감시사회와 프라이법시, 한울 아카데미, 1998.

국회예산정책처, 전자정부 지원사업 평가, 국회예산정책처, 2009.

권건보, 개인정보보호와 자기정보통제권, 경인문화사, 2006.

권기헌, 전자정부와 행정개혁, 커뮤니케이션북스, 1999.

권영성, 헌법학원론, 법문사, 2009.

금봉수・장우영・조용혁, 전자신분증 추진동향과 시사점, 한국전산원, 2005.

김기중, 국가의 국민관리체계와 인권, 21세기의 인권, 한길사, 2000.

김배원, 정부규제적 통합 개인정보 보호법에 관한 연구, 정보통신부, 2002.

김성태, 전자정부 -이론과 전략, 법문사, 2003.

김연수, 개인정보보호, (주)사이버출판사, 2001.

김철수, 헌법학신론, 박영사, 2005.

김형남 외, 미국법 강의, 세종출판사, 2001.

미래사회연구포럼, 개인의 사생활, 국가적 감시, 그리고 규범, 미래사회연구포럼, 2007.

박윤흔, 최신행정법강의(상), 박영사, 2002.

박균성, 프랑스의 전자정부법제, 한국법제연구원, 2001.

박균성, 프랑스에서의 전자정부구현을 위한 법제 동향, 한국법제연구원, 2001.

박홍윤, 공공기관 개인정보의 공동이용에 있어서 문제점과 정책적 과제,

정보통신부, 2002.

백윤철・이창범・장교식, 개인정보보호법, 한국학술정보, 2008.

성낙인, 헌법학, 법문사, 2009.

성낙인 외, 개인정보보호를 위한 정책방안 연구, 정보통신부, 1999.

이인호, 개인정보자기결정권의 한계와 제한에 관한 연구, 한국정보보호진흥원, 2001.

이인호. “한국의 개인정보보호법제의 문제점과 정비방안 -각국 개인정보보호법 제도의 비교법적 접근-”, 2003년 제2회 개인정보보호 심포지움, 한국정보보호진흥원, 2003.

_____, 개인정보감독기구 및 권리구제방안에 관한 연구, 한국전산원, 2004.

_____, 개인정보보호법제의 현대화방안에 관한 연구, 국회사무처 법제실, 2005.

이창범, 미국, 독일, 일본의 정보보호법 체계에 관한 연구, 한국정보보호진흥원, 2006.

이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003.

임지봉, 미국의 전자정부법제, 한국법제연구원, 2001.

장영수, 헌법학, 홍문사, 2009.

장영아, 호적제도의 개선방안에 관한 연구, 한국여성개발원, 1996.

정보통신부, 전자정부사업이 지방자치단체 국제화사업에 미치는 영향에 관한 분석, 정보통신부, 2002.

정종섭, 헌법학원론, 박영사, 2009.

총무처, 축조해설 개인정보보호법, 총무처, 1994.

한상희 외, 주민등록번호 사용현황 실태조사, 2005년도 인권상황실태조사 연구용역죄종보고서, 국가인권위원회, 2005.

한국전산원, 개인정보보호법제 정비를 위한 기본법 제정방안 연구, 한국전

산원, 2004.

한국전산원, 전자정부시대 개인정보보호법제 정립방안 연구, 한국전산원, 2004.

한국정보사회진흥원, 전자정부법 개정방안 연구, 한국정보사회진흥원, 행정안전부, 2008.

행정안전부, 공공기관 개인정보 보호 이해와 해설, 행정안전부, 2008.

행정자치부, 각국의 신분증제도, 행정자치부, 1998.

_____, 전자정부법의 이해와 해설, 행정자치부, 2007.

_____, 전자정부법의 이해와 해설:「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률」, 행정자치부, 2001.

_____, 2006 전자정부사업 연차보고서, 행정자치부, 2007.

_____, 함께 가는 희망한국 건설을 위한 차세대 전자정부 추진계획, 행정자치부, 2007.

_____, 2007 전자정부법의 이해와 해설, 행정자치부, 2008.

황종성 외, 국외 개인정보보호법제 분석 및 시사점, 한국전산원, 2004.

_____, 전자정부법 개정방안 연구, 한국정보사회진흥원, 2008.

홍성방, 헌법학, 현암사, 2009.

홍정선, 행정법원론(상), 박영사, 2001.

홍준형, 개인정보보호법제 정비를 위한 기본법 제정방안 연구, 한국전산원, 2004.

허 영, 한국헌법론, 박영사, 2005.

2003 전자정부백서, 전자정부특별위원회, 2003.

2003-2007 전자정부사업백서, 행정안전부・한국정보사회진흥원, 2008.

2002 개인정보보호백서, 한국정보보호진흥원, 2002.

2003 개인정보보호백서, 한국정보보호진흥원, 2003.

2009 국가정보보호백서, 행정안전부 외, 2009.

堀部政男, 『プライバシ―と高度情報化社會』, 東京: 岩波文庫, 1988; 신구현 옮김,『프라이버시와 고도정보화사회』, 청림출판, 1995.

A. Giddens, "The Nation-State and Violence". Univ. California Press, 1987; 진덕규(역),『민족국가와 폭력』, 삼지원, 1991.

2) 논문

강경근, “전자정부의 헌법적 과제”, 공법연구 제35권 제1호, 한국공법학회, 2006.

_____, “개인정보침해 국내외 판례조사 및 분석”, 개인정보연구 00-1, 한국정보보호센터, 2000.

강경근, “행정정보의 공동이용과 기본권”, 아·태공법연구 통권 제10호, 아세아·태평양공법학회, 2002.

_____, 행정정보의 공동이용에 따른 법적 과제, 한국법제연구원, 2001.

구재군, “인터넷 이용자의 개인정보 자기결정권”, 정보화정책 제10권 제3호, 2003.

구병문, 프라이버시 영향평가제도의 국내법적 도입방안-공공부문의 중심으로, 제3회 개인정보보호 정책 포럼 자료, 2004.

_____, “프라이버시 영향평가제도 도입의 쟁점과 추진방향”, 서울대학교행정대학원 한국정책지식센터, 2004.

권건보, “자기정보통제권에 관한 연구 -공공부문에서의 개인정보보호를 중심으로-”, 박사학위논문, 서울대학교 대학원, 2004.

_____,“행정정보공동이용과 개인정보보호”, 전자정부법제연구, 제1권 제2호, 행정자치부, 2006.

권헌영, “개인정보보호법 입법을 다시 거론하며”, 토지공법연구 제43집 제3호, 한국토지공법학회, 2009.

_____, “개인정보의 헌법적 수용 -헌법재판소의 결정 분석을 중심으로-”, 토지공법연구 제35집, 한국토지공법학회, 2007.

김민호, “행정정보공동이용의 범위와 한계에 대한 이론적 고찰 및 정책과제”, 토지공법연구 제43집 제1호, 한국토지공법학회, 2009.

김배원, “일본의 개인정보보호법제의 최근 동향「개인정보보호에 관한 법률안」을 중심을 중심으로”, 공법학연구 제3권 제2호, 한국비교공법학회, 2002.

김성태, “개인관련정보에 대한 경찰작용 -독일 주경찰법에서 규율-”, 현대공법학의 과제(최송화교수 화갑기념논문집), 박영사, 2002.

김승환, “정보자기결정권”, 헌법학연구 제3호, 한국헌법학회, 2003.

김용섭, “정보공개와 개인정보보호의 충돌과 조화”, 공법연구 제29집 제3호, 한국공법학회, 2001.

김일환, “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 공법연구 제29집 제3호, 공법학연구, 2001.

_____, “정보사회에서 기본권제한개념의 확대필요성에 관한 고찰”, 헌법학연구 제9권 제3호, 2003.

_____, “행정정보의 공동이용으로부터 정보자기결정권의 보호에 관한 헌법상 고찰”, 공법연구 제32집 제4호, 한국공법학회, 2004.

_____, “정보사회에서 개인식별번호의 수집 및 이용에 관한 헌법적 고찰”, 성균관법학 제17권 제1호, 성균관대학교 비교법학연구소, 2005.

_____, “주민등록번호의 위헌성여부에 관한 고찰”, 헌법학연구 제11권 제3호, 한국헌법학회, 2005.

_____, “전자정부구축에 따른 행정정보공동이용의 방식과 유형에 관한 고찰”, 성균관법학 제19권 제1호, 성균관대학교 비교법학연구소, 2007.

_____, “민주, 법치국가의 발전과 사회통합”, 2008 한국공법학회[공동]주최 국제학술대회, 한국법제연구원, 2008.

_____, “전자정부와 개인정보보호”, 공법연구 제37권 제1호, 한국공법학회, 2008.

_____, “현행 개인정보보호 체계의 문제점 및 통합 개인정보보호법 제정 방향”, 국회도서관보 제45권 제9호 (통권 제352호), 국회도서관, 2008.

_____, “개인정보보호법제의 정비방안에 관한 연구”, 한국법제연구원, 1997.

_____, “개인정보공동이용의 통제와 감독에 관한 비교법적 고찰 -미국과 독일의 법제를 중심으로-”, 헌법학연구 제13권 제2호, 한국헌법학회, 2007.

김종철, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 인터넷법률 제4호, 2001.

_____, “전자정부와 개인정보보호의 조화 -이념적 측면을 중심으로-”, 세계헌법연구 제12권 제2호, 국제헌법학회 한국학회, 2006.

김주원, “일본 전자정부 추진동향 및 시사점 : 행정정보화를 넘어 국가경쟁력 강화로”, NIA IT 이슈 & 트렌트 제8호, 한국정보사회진흥원, 2008.

김태현, “개인정보보호제도에 관한 헌법적 고찰”, 박사학위논문, 경희대학교 대학원 2003.

김재광, “일본의 전자정부 구현을 위한 법제 고찰”, 한국법제원, 2001.

류현숙 외, Web 2.0 시대 정부신뢰 제고를 위한 전자정부 추진전략 연구, 한국행정연구원, 2008.

명재진, 국가에 의한 지문강제날인제도의 헌법적 문제점, 공법학연구 제7권 제1호, 한국공법학회, 2006.

박선주, “전자정부 해외 동향 : UN E-Government Survey 2008 결과 분석”, 한국정보사회진흥원, 2008.

박선주・김현정, “전자정부 해외 동향”, 한국정보사회진흥원, 2008.

박현진・박선주, “전자정부 해외 동향 : 주요 선진국가의 전자정부 ‘개인화 서비스’ 현황”, 전자정부 포커스 제3권, 한국정보사회진흥원, 2008.

박문석, “사이버공간에서의 프라이버시권에 관한 비교법적 연구”, 박사학위 논문, 영남대학교 대학원, 2009.

백윤철, “헌법상 개인정보자기결정권에 관한 연구”, 법조 제51권 제58호,

2002.

_____, “헌법상 자기결정권과 개인정보자기결정권”, 헌법학 연구 제9권 제3호, 한국헌법학회, 2003.

_____, “개인정보보호법(안)과 최근 입법동향 및 과제”, 토지공법연구 제43집 제2호, 한국토지공법학회, 2009.

변재옥, “정보사회에 있어서 프라이버시의 권리”, 서울대학교 박사학위 논문, 1979.

심현정, “행정정보공동이용 제도에 대한 이해와 관련 법제의 발전방향”, 법제 통권 제589호, 법제처, 2007.

서진완・장지원, “행정정보의 공동활용제도에 관한 연구”, 한국행정연구원, 1997.

서순복, “신 공공 관리에 관한 보완적 접근 : 정보 기술을 활용한 행정 개혁”, 한국사회와행정연구 10,2(’99.12), 서울행정학회, 1999.

서진완, “행정정보의 공동활용제도에 관한 연구”, 한국행정연구원, 1997.

성낙인, “표현의 자유 -기본권의 개념과 범위에 관한 연구-”, 헌법재판연구 제6권, 1995.

양창진, “전자정부시대 개인정보 관리 제도에 관한 연구 -전자주민증 제도의 도입과 그 정치적 함의를 중심으로-”, 한국학중앙연구원 한국학대학원 박사학위논문, 한국학중앙연구원, 2005.

윤영민, “개인정보와 사생활의 비밀과 자유 보호를 위한 정책 연구”, 한양대학교, 2004.

이규정・구병문, 공공부문 프라이버시 영향평가제도, 한국전산원, 2003.

이민영, “행정정보의 공동이용의 추진 방향과 법적 과제”, 정보통신정책 통권 제389호, 정보통신정책연구원, 2006.

이인호, “개인정보보호를 위한 감독기구의 설립방향”, 국회도서관보 제45권 제9호 (통권 제352호), 국회도서관, 2008.

_____, “주민등록번호·지문날인과 개인정보자기결정권”, 인터넷법률 제8호, 법무부, 2001.

이인호, “개인정보감독기구 및 권리구제방안에 관한 연구”, 한국전산원, 2004.

이상명, “주민등록제도에 대한 헌법적 평가 -주민등록번호와 지문날인을 중심으로-”, 박사학위논문, 한양대학교 대학원, 2007.

_____, “개인정보자기결정권의 헌법적 근거에 관한 고찰”, 공법연구 제36집 제3호, 한국공법학회, 2008.

이자성, “일본의 개인정보보호제도에 관한 고찰 -개인정보보호조례를 중심으로-”, 한국행정학회 2007년도 추계학술대회 발표논문집(下), 한국행정학회, 2007.

_____, “한국 지방정부의 개인정보보호 제도화에 관한 연구 -우리나라・일본・국제기구의 법률을 중심으로-”, 한국지역정보화학회지 제11권 제4호, 한국지역정보학회, 2008.

이희훈, “주민등록번호에 대한 헌법적 고찰 -개인정보자기결정권의 침해를 중심으로-”, 토지공법연구 제37집 제1호, 한국토지공법학회, 2007.

임규철, “정보사회에서의 개인정보자기결정권에 대한 연구 -독일에서의 논의를 중심으로-”, 헌법학연구 제8권 제3호, 한국헌법학회, 2002.

임지봉, “우리 전자정부법제의 현황과 개선방향”, 국제헌법학회 한국학회, 2008.

정영화, “인터넷상 개인정보보호 및 분쟁해결에 관한 연구”, 인터넷법연구 제1호, 한국인터넷법학회, 2002.

_____, “사이버스페이스와 프라이버시권 -현행 개인정보보호법제의 문제점을 중심으로-”, 헌법학연구 제6권 제3호, 한국헌법학회, 2000.

_____, “헌법상 프라이버시에 관한 고찰”, 고시계 제47권 제4호(통권542호), 고시계사, 2002.

장영환・도경화・정원모, 행정정보공동이용 현황 및 과제 ,한국정보사회진흥원, 2006.

정연수・김희은, “주민등록번호 도용의 문제점 및 개선방안”, 인터넷법제연구 제3권 제2호, 한국인터넷법학회, 2004.

정재황, “사이버 공간상의 표현의 자유와 그 규제에 관한 연구, 헌법재판

연구”, 제13권, 2002.

정종길, “정보화 사회에서 프라이버시권의 보호”, 경기법학논총 제4호, 경기대학교 사회과학연구소 법학연구실, 2006.

정준현, “민간 온라인 개인정보보호법제에 대한 검토”, 공법연구 제29집 제3호, 한국공법학회, 2001.

_____, “정보통신망이용촉진및정보보호에관한법률 하위법령의 방향”, 한국정보보호진흥원, 2001.

_____, “개인정보의 보호와 그 활용에 관한 소고”, 토지공법연구 제43집 제2호, 한국토지공법학회, 2009.

정태호, “개인정보자결권의 헌법적 근거 및 구조에 대한 고찰 -동시에 교육행정정보 시스템(NEIS)의 위헌여부의 판단에의 그 응용-”, 헌법논총 제14집, 헌법재판소, 2003.

정연수・김은희, “주민등록번호 도용의 문제점 및 개선방안”, 인터넷법제연구 제3권 제2호, 한국인터넷법학회, 2004.

정필운, “행정정보공동이용법안의 추진배경 및 내용”, 한국정보사회진흥원, 2006

조화순, “정보사회의 국가권력과 개인정보 -한국의 전자주민카드 도입논의를 중심으로-”, 한국정치학회보 제39집 제2호, 한국정치학회, 2005.

최진안, “전자정부구축에 따른 개인정보공동이용의 헌법적 고찰 -형사사법통합정보체계 구축사업을 중심으로-”, 박사학위논문, 성균관대학교 중앙학술정보관, 2009.

한국정보사회진흥원 전자정부기획팀, “전자정부 해외 동향: 영국 정부의 전자정보 동향”, 전자정부포커스, 제5권, 한국정보사회진흥원, 2007.

한겨레21, “악착같아라, 정부의 정보 폭식”, 한겨레21(통권766호), 2009.

한수웅, “헌법상의 인격권”, 헌법논총 13, 헌법재판소, 2002.

한상희, 생체정보의 인권적 특성, “지문 등 생체정보이용, 무엇이 문제인가”, 토론회 자료집, 국가인권위원회, 2004.

황인호, “개인정보보호제도에서의 규제에 관한 연구 -제도의 재구조화를 위한 입법론을 중심으로-”, 공법연구 제30집 제4호, 한국공법학회, 2002.

홍성찬・황인호, “프라이버시권에 있어서의 개인정보보호에 관한 연구”, 사회과학연구 제14권 제1호, 건국대학교 사회정책연구소, 2001.

홍준형, “전자정부와 개인정보보호 -정보사회의 권리장전을 위하여-”, 정보과학회지 제22권 제11호, 학국정보과학회, 2004.

현대호, “행정정보공동이용에 관한 법적 과제”, 한국법제연구원, 2007.

2. 외국 문헌

1) 미 국

Adams, Henry, The Education of Henry Adams : Autobiography, Boston : Houghton Mifflin, (1918).

Beaney, W. M., “The Right to and American Law,” 31 Law and Comtemporary Problems, 253 (1966).

Buckholtz, Thomas J., Information Privacy: Your Key to the Information Age, NJ; Wiley, (1995).

Cate, Fried H., “Privacy,” 77 Yale L. J. 475 (1968).

_____, Privacy in the Information Age, Washington, D. C.:Brookings Institution Press, (1997).

Chlapowski, Francis S., “The Constitutional Protection of Informational Privacy,” 71 Boston University Law Review, 133 (1991).

Clarke, Roger, Privacy and Public Registers, Invited Address to the IIR Conference on Data Protection and Privacy, Boulevard Hotel, Sydney, 12-13, May (1997).

Dixon, Jr., Robert G., “The Griswold Penumbra : Constitutional Charter for an

Expanded Law of Privacy?", 64 Michigan Law Review, 197 (1965).

Froomkin, Michael, "The Death of Privacy," 52 Stanford Law Review, 146(2000).

Flaherty, David H., Protecting Privacy in Surveillance Society, Chapel Hill: The University of North Carolina Press, (1989).

Glancy, Dorothy J., Symposium on Internet Privacy: At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet, 16 Computer & High Tech. L. J., 357 (2000).

Gross, Hyman, "The Concept of Privacy", 42 New York Uni. L. Rev. 34. (1967).

Glenn Chatmas Smith, "We've got your Number!" 37 UCLA L. Rev. 145, (1989).

Hicks, Granville, "The Invasion of Privacy : The Limits of Privacy," American Scholar, Spring (1959).

Hallman, E., "The Personal Identification Number System In Sweden", in OECD, Policy Issues In Data Protection and Privacy, Paris. OECD, (1976).

Ken, Gomeley, "One Hundred Years of Privacy", 154 Wis. L. Rev. 1335 (1992).

Kang, Jerry, "Information Privacy in Cyberspace Transaction", 50 Stanford Law Review, 1193 (1998).

Lyon, David, "British Identity Cards: The Unpalatable Logic of European Membership?", 62 The Political Quarterly, 3 (1991).

Miller, Arthur R., The Assault on Privacy: Computers, Data Banks, and Dossier, Ann Arber: The University of Michigan Press, (1971).

Michael, Jemes, Privacy and Human Right, Hampshire: Dartmouth, (1994).

Minor, William H., "Identity Cards and Databases in Health Care: The Need for Federal Privacy Protection," 28 Columbia Journal of Law and Social Problems, 253 (1995).

Masuda, Yoneji, The Information Society as Post-Industrialized Society, Bethedsda, (1981).

Murphy, Richard S., “Property Rights in Personal Information: An Economic Defense of Privacy,” 84 Georgetown Law Journal, 2381 (1996).

Pember, Don R., Privacy and the Press, Seattle : Univ. of Washington Press, (1972).

Pollak, L., “Thomas I. Emerson, Lawyer and Scholar,” 84 Yale Law Journal, 84 (1975).

Pratt, Walter F., Privacy in Britain, Bucknell Univ. Press, (1979).

Prosser, William L., “Privacy,” 48 Cal. L. Rev. 383 (1960).

Posner, Richard A., "The Right of Privacy," 12 Georgia Law Review, 393 (1978).

Rule, James, Douglas McAdam, Linda Stearms and David Uglow, The Politics of Privacy, A Mentor Book : New American Library, (1980).

Rourke, Francis, Secrecy and Publicity, Baltimore; Johns Hopkins Press, (1966).

Redfern, Philip, “Population Registers : Some Administrative and Statistical Pros and Cons,” 152 Journal of Royal Statistical Society, 1 (1989).

Schlesinger, Arhur M., Schlesinger’s Rise of the City, 1878-1898, New York : Macmillan, (1933).

Schwartz, Paul M., “Privacy and Participation: Personal Information and Public Sector Regulation in the United States,” 80 Iowa Law Review, 553 (1995).

Seipp, David J., The Right to Privacy in American History, Harvard Univ. Program on information Resources Policy, Publication p-78-3, July (1978).

Shattuck, John H. F., Rights of Privacy, New York : National Textbook Co. &American Civil Liberties Union, (1979).

Shils, Edward, “Privacy: Its Constitution and Its Vicissitudes,” 31 Law and

Contemporary Problems, 281 (1966).

Simmel, Arnold, Privacy, Edward Sills(ed.), International Encyclopedia of the Social Sciences. Vol. 12: 480-486, New York: Macmillan and Free Press, (1968).

Solove, Daniel J., “Privacy and Power: Computer Databases and Metaphors for Information Privacy,” 53 Stanford Law Review, 1393 (2001).

_____, "The Digital Person: Technology and Privacy in the Information Age", 121 George Washington University Law School Public Law Research Paper, NYU Press, (2004).

_____, "The Origins and Growth of Information Privacy Law", Fourth Annual Institute on Privacy Law : Protecting your client in a security-conscious world. 748 PLI / Pat 29, (2003).

Solove, Diniel J. and Marc Rotenberg, Information Privacy Law, New York: Aspen Publishers Inc., (2003).

Wacks, Raymond, Personal Information : Privacy and the Law, Oxford: Oxford University Press, (1989).

Warren Samuel D. and Louis D. Brandeis, "The Right to Privacy", 4 Harvard Law Review, 193 (1890).

Westin, Alan F., Privacy and Freedom, New York: Atheneum, (1967).

_____, The Equifax Report on Consumers in the. Information Age. New York: Louis Harris & Associates, (1990).

Whitaker, Reg, The End of Privacy: How Total Surveillance Is Recoming A Reality, The New Press New York, (1999).

2) 독 일

D Haas, Freie Entfaltung der Personlichkeit, DOV, (1954).

Dietwalt Rohlf, Der grundrechtliche Schutz der Privatsphäre, (1980).

Klaus Vogelgesang, Grundrecht auf informationelle Selbstbestimmung? Nomos Verlagsgesellschaft, Baden-Baden (1987).

Friedrich Schoch/Hans-Heinrich Trute, öffentlichßrechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57, (1998).

Gallwas, Hans-Ulrich, "Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit", Neue Juristische Wochenschrift(*NJW*) (1992).

Gerald Spindler/Fritjof Börner(Edit.), "E-Commerce Law in Europe and the USA",. Springer, (2002).

Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in Informationsgesell-schaft - Aufem Wege zu einem neuen Konzept des Datenschutzes -, AöR, 123. Band, Heft 4, (1998).

Hans-Ulrich Gallwas, "Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit", NJW (1992).

Marie-Theres Tinnefeld/Eugen Ehmann, Einführung in das Datenschutzrecht, Oldendourg Verlag, (1992).

Rupert Scholz/Rainer Pitschas, Informationelle Selbstbestimmung und staaltiche Informationsverantwortung Duncker &Humblot, (1984).

Wilhelm Steinmüller, Grundfragen des Datenschutzes: Gutachten im Auftrag des Bundesministeriums des Innern, Deutscher Bundestag -6.Wahlperiode- Drucksache 6/3826 Anlage 1, Juli (1971).

Spiros Simitis, "Von der Amtshilfe zur Informationshilfe", NJW (1986).

Franz-Ludwing Knermeyer, Datenerhebung und Datenverabeitung im Polizeirecht, NVwZ (1988).

Konrad Hesse, Grundzuge des Verfassungerechts der Bundesrepublik Deutschland, 20. Aufl., (1995).

Evangelia Mitrou, Die Entwicklung der indtitutionellen Kontrolle des

Datenschutzes, Nomos, (1993).

3) 일 본

藤野剛土, 個人情報保護, JMAM, 2000.

榎原猛(編), プライバシー權の綜合的研究, 京都: 法律文化史, 1998.

芦部信喜, 廣義のプライバシー權(2)-包括的基本權(1), 法學教室 127號, 1991.

_____, 廣義のプライバシー權(2)-包括的基本權(4), 法學教室 131號, 1991.

佐藤幸治, 日本國憲法と「自己決定權」-その根據と性質をめぐつて, 法學教室 98號 1988.

岡村久道・新保史生, 電子ネットワーク個人情報保護, 経濟産業調査會, 2002.

堀部政男(編), 情報公開制度・個人情報保護制度の回顧と前望, 情報公開·個人情報保護, ジェリスト增刊, 1994.

藤原靜雄, 逐條個人情報保護法, 弘文堂, 2003.

A Study of the Right to the Self-control on Information Management according to constructing the electronic government

Jin Sook Jang

Department of Law, The Graduate School
Pukyong National University

Abstract

This study aims at finding out the possibility of establishing personal information protection and the control of individual information management as a fundamental right by the guarantee of a constitution, embodying contents and restrictions of the guarantee in a systematic aspect of ensuring a fundamental right due to the common utilization of the administration information according to the advent of information society and electronic government. Furthermore, it also reviews specific contents and problems of both a constitutional ground and a judicial system on the basis of this fundamental understanding and tries its improvement. On the basis of the result, the goal of this study is to seek ways of redesign of a legal system and proposal of more desirable legislative directions that each of the two legal values, which could be at variance with each other, 'the common utilization of the administration information' and 'the control over 'self-information management', can play their roles.

In compositions of each chapter, firstly, chapter Ⅱ looks at the impact on individuals caused by electronic government generalities and the establishment of electronic government. Considering the legal system of electronic government in a comparative way and constitutional attitude about the common utilization of the

administration information, it discusses the necessity of the protection of personal information, after deriving problems which appear in the national legal system.

In chapter Ⅲ, as the possibility of an intrusion of individual information increases, it suggests the way of enactment of the law of the protection of personal information after drawing implications through a comparative legal consideration of the protection of personal information on the basis of recognition the common utilization of personal information as a limit of new basic human rights.

In chapter Ⅳ, with the attention of an individual legal ability which can manage and control personal information by oneself, it analyzes the matter of personal information protection in electronic government. The establishment of legal system of personal information protection and improvements of one's personal identification number system have been discussed to secure the right of control on personal information management.

Lastly, in chapter Ⅴ, summarizing the study and drawing an conclusion, it suggests 「(tentatively named)Legislation of the common utilization of the administration information 」.

Personal information protection according to the establishment of electronic government needs to be sought the way of reconciliation on the ground of the legal theory, which is the restriction and limitation of the common utilization of the administration information and the control of self-information management. When the common utilization of the administration information related individuals appears as a restriction, it has an enabling act of it and such common utilization can be justified when it reaches the minimum degrees of necessity. The control of personal information management as a fundamental human rights must be a right which restricts public sector, it can also affect private sector at any forms. Therefore, personal information protection can be seen as a more important in private sector than the one in public sector. In this aspect, it is important to prevent an

intrusion of private personal information in advance, to make a legal system to aid after the intrusion and to do research and development of security system or security program in a technical level. However, this study focuses on the way of legislative protection of personal information protection and the control over self-information management in a normative dimension. Therefore, this study interprets and analyzes current laws and regulations and judicial precedents about personal information protection on the constitutional ground with a normative approach.

First, a systematic design has to be needed in order to secure the safety, transparency and responsibility in a point of view of admitting dispositional characters and the necessity of the use, rather than prohibiting or having a prejudiced view of using personal information so as to protect private information in the environment of electronic government and information society. Through the common utilization of the administration information, it is significant to improve the efficiency of administration, to increase the convenience of people, to reinforce national competitiveness but at the same time, it is also important to minimize side effects called an intrusion of personal information. To make it possible, a standard of personal information, which is the subject of the common utilization of the administration information, should be clearly set up. Among administration information, which is another subject, it should be classified into the one which is related to personal information and the other which is not. So in sharing utilization of administration information, the purpose, range, requirement, procedure and processing method should be strictly provided in the laws. In present, the legal basis of the common utilization of the administration information is conducted on the basis of 「The law of electronic government」, however, it is inadequate to be regarded as a fundamental law for the common utilization of the administration information as it is mixed of abstract regulations and procedural regulations which doesn't have the

characteristic of a fundamental law or a procedure law. Thus, it is urgent to set up a systematical and reasonable law for the common utilization of the administration information.

Next, personal information protected by laws stands for the whole information which can identify specific individuals. In a protection of this kind of personal information, the most important thing is the preliminary control over the information subjects. In this point of view, the matter of personal information protection needs to be approached in a view of the control over self-information management affirmed by laws. This control on self-information management is defined as a fundamental right of being able to manage and control autonomically the flow of one's information. That is, one should administer preliminarily the information of oneself and prevent the misuse and abuse of one's information beforehand, which the information subject has to be able to control over cutting, revising and eliminating those wrong parts.

「The law of personal information protection by public organization s」 in public sector, 「The law of encouragement of using information network」 in private sector and the regulations of personal information protection which is prevalent in each law, all of these will reflect an international regulation about personal information protection and be modified in a direction of granting a right of information agents and legislate an integrated fundamental law for the protection of personal information. In a specific way, we need to stipulate a procedure of fair and lawful collection, refrain integrated managements of personal information if possible and enact a law of separating personal information according to each organization and keeping it in each institution. Personal information which has no purpose to use any more has to be specified in the law in accordance with the principle of the elimination in advance and the principle of the anonymity which can identify each person. Although the common utilization and offers of other organizations are exceptionally permitted, it is urged to

inform the person in question relevant facts and to enact a law of the limit of providing computer matching. An independent personal information protective organization needs to be established, which makes it possible that information subjects can be able to request anonymity and deletion of one's own information along with guaranteeing the right to listen to an explanation about information processing situations. It also should perform the outside control for the restraint of abusing personal information with a proper control over the power of each organization expanded by computerization. In the operating electronic government, we should prevent the problem of an intrusion of personal information beforehand with the system of preparatory impact assessment and seek a way of satisfying the effectiveness of national budget reductions.

Also, the law of resident registration number, which makes it possible to use one's personal identification number in all fields and has rarely been seen in any part of the world in a public sector or private sector in the national level, has to reconsider. Above all, the way of the minimum of requesting resident registration number and the application of it in stages have to be led and redesign a law in accordance with them.