

# 전자정부와 개인정보보호

- 정보사회의 권리장전을 향하여 -

서울대학교 홍준형

## 1. 문제의 제기

전자정부는 무엇보다도 효율성의 약속이다.<sup>1)</sup> 그러나 그 약속은 신뢰의 기반 없이는 통용될 수 없다. 그 신뢰의 기반을 이루는, 최근 전자정부의 급속한 발전에 따라 대두된 가장 현저한 요소가 바로 개인정보 보호의 문제이다. 프라이버시에 대한 법적 보호의 역사는 결코 짧지 않을지라도, 이 문제가 새롭게 조명을 받게 된 것은 정보기술의 비약적 발전, 정보화의 눈부신 진전, 사이버스페이스의 확산으로 집약되는 고도정보사회라는 맥락에서였다.<sup>2)</sup> 특히 인터넷이라는 개방형 네트워크를 통해 개인정보가 자유로이 유통되는 환경에서 전자정부가 성공하려면 국민에게 개인정보가 오·남용되지 아니하고 해킹이나 유출 등의 위협으로부터 안전하다는 신뢰를 줄 수 있어야 한다.<sup>3)</sup> 김대중 정부가 추진했던 11대 전자정부 사업의 핵심을 이루었던 교육행정정보시스템(NEIS) 사태는 이 점을 드러낸 가장 극적인 사례였다.<sup>4)</sup>

반면, 개인정보의 보호는 그것이 과잉되면 전자정부의 기대효과인 효율성을 저해하거나 전자정부의 실현 자체를 방해 또는 좌절시킬 수 있다는 우려의 목소리도 만만치 않다. 이러한 주장의 가장 대표적인 근거는 개인정보를 지나치게 두텁게 보호하면 정보의 공유가 불가능해지거나 곤란해지고 그 결과 정보공유를 통해 정보처리의 효율성을 획기적으로 제고할 수 있다는 전자정부의 핵심적 이점을 살릴 수 없다는 것이다. 즉, 개인정보를 너무 지나치게 보장하면 정보공유에 차질이 생기게 되므로, 정보의 공유를 활성화시키기 위하여 어느 정도 개인정보의 보호라는 가치를 희생시키는 것이 불가피하다는 주장이다.

개인정보의 보호와 정보공유가 서로 상충하거나 길항관계에 있다는 것은 널리 알려진 사실이다. 그러나 문제는 결코 간단치 않다. 어느 정도가 개인정보의 적정한 보호수준이고 어느 정도가 과잉보호의 경계인가? 정보공유를 위해 양보해야 할 그 '어느 정도'는 어느 정도인가? 이 문제를 해결하기 위해서는 먼저 전자정부에 있어 개인정보의 보호가 어떠한 기능적 연관관계를 가지는지를 분명히 해 둘 필요가 있다. 종래 상충·길항관계로만 파악되어 왔던 이 두 가지 요구들이 전자정부의 맥락에서는 오히려 상호보완적 관계에 놓여야 하는 경우도 있을 수 있다. 이러한 견지에서 이 글은 **전자정부라는 정책과제와 개인정보, 특히 정보프라이버시(information privacy)를 핵심으로 하는 개인정보의 보호의 관계를 규명함으로써 향후 전자정부에서의 개인정보 보호를 위한 정책방향 모색을 위한 이론적 근거를 제시해 보고자 한다.**

## 2. 전자정부와 개인정보의 보호

### 2.1 전자정부

전자정부는 오늘날 세계 200여 개 국에 걸쳐 나타나

정보통신정책연구원 등을 참조.

1) OECD, The e-Government Imperative (OECD e-Government Studies: <http://www1.oecd.org/publications/e-book/4203071E.PDF>), 2003a: 11; OECD, Checklist for e-Government Leaders (<http://www.oecd.org/dataoecd/62/58/11923037.pdf>), 2003b: 3.  
2) <http://www1.oecd.org/publications/e-book/9303051E.PDF>, p.12. 이 점은 정보화가 진전되기 훨씬 이전 시기에도 빈번히 지적되고 있었다(Rein Turn & W.H. Ware, Privacy and Security Issues in Information Systems, 1976; Spiros Simitis, Reviewing Privacy in an Information Society, 135 U.Pa. L. Rev., 707(1987) 등).  
3) 한국정보보호진흥원, 2003 개인정보보호백서, 170; 이동훈, 전자정부와 개인정보보호, Information Security Review (한국정보보호진흥원) 제1권 제2호 (2004), 69-83, 75 등.  
4) 이에 관한 최근의 분석으로는 홍성걸, 개인정보 보호와 정책갈등 - NEIS 사례를 중심으로 -, Information Security Review (한국정보보호진흥원) 제1권 제2호 (2004), 27-46; 조화순, (2004) "거버넌스 관점에서 본 NEIS 갈등사례 연구", 「정보화 정책」 2004년 봄호. 한국전산원; 임규철, (2003) "NEIS와 개인정보자기결정권-국가인권위원회의 NEIS 결정을 중심으로", 「인권과정의」, 323호; 황주성·최선희, (2003) "전자정부 사업과 개인정보보호 이슈-NEIS를 중심으로", 「KISDI 이슈리포트」.

는 대단히 보편적인 현상이다.<sup>5)</sup> 그러나 이러한 보편성에도 불구하고 전자정부의 개념은 관점에 따라 다양하게 정의되고 있고,<sup>6)</sup> 그 의미하는 바도 한결같지 아니하다. 전자정부의 가장 일반적·공통적 개념을 정의한 예로는 UN DPADM/UNDESA<sup>7)</sup>와 OECD의 '전자정부 프로젝트'의 경우를 들 수 있다. 전자는 "그 기능수행을 최적화하기 위하여 정보통신 기술을 적용하여 그 내부 및 외부 관계를 변화시키는 정부"로 정의한다.<sup>8)</sup> 후자에 의하면, 전자정부란 "정보통신 기술, 특히 인터넷을 더 나은 정부를 실현하기 위한 수단으로 사용하는 것"을 말한다(OECD, 2003a: 23).<sup>9)</sup>

전자정부 개념과 의미의 다양한 차이는 단순한 의미론적 차원이 아니라 각국 정부가 추구하는 전략상 우선순위의 차이를 반영하는 결과라고 볼 수 있다. 전자정부의 개념정의는 대체로 세 가지 부류로 나뉘는데, 첫째, 전자정부를 인터넷을 통한 정부 서비스의 온라인 제공(internet online service delivery)과 'e-consultation' 같이 그 밖의 인터넷기반 활동으로 정의하는 경우, 둘째, 정부 서비스의 전달과 사무처리에 초점을 맞추면서도 가장 넓은 의미로 파악하여 정부에서 행해지는 정보통신 기술을 활용한 모든 활동으로 전자정부를 정의하는 경우, 셋째, 정보통신 기술을 사용하여 공행정을 변화시키는 역량, 즉 정보통신 기술에 둘러싸여 구축된 새로운 형태의 정부로 정의하는 경우가 그것이다(OECD, 2003a: 23). 이와 같이 상이한 전자정부 개념이 채택되고 있는 것은 각국 정부가 설정한 우선순위가 변화하고 각기 특정 목표들의 달성을 위하여 성과를 내고 있다는 사실과 무관하지 않다. 다시 말하면 각국에서의 전자정부 개념의 차이는 각국이 추진하는 전자정부 정책의 우선순위와 발전수준을 반영한다는 사실이다. 물론 전자정부라는 정책과제 자체가 매우 역동적 특성을

띠고 정책과 개념도 그에 상응하기 마련이므로 이는 극히 자연스런 결과라고 이해될 수 있다. 다만, 각국의 전자정부 추진 전략상 우선순위의 차이를 엿볼 수 있게 해준다는 점에서 전자정부의 개념정의에 주목하는 것은 충분히 의미 있는 일이라고 생각된다.

가령 우리나라의 경우 전자정부에 대한 공식적 정의는 전자정부구현을위한행정업무등의전자화촉진에관한법률(일부개정 2003.5.15 법률 제06871호. 이하 "전자정부법"이라 한다.) 제2조 제1항에 의하여 주어지고 있는데, 이에 따르면 전자정부란 "정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부"를 말한다. 이러한 전자정부법의 개념정의는 정보기술의 활용에 의한 행정사무의 전자화와 이를 통한 행정업무의 효율적 수행에 초점을 맞추고 있다는 점에서, 대체로 위의 두 번째 유형에 속한다고 볼 수 있다. 여기서 법제정 과정에서 전자정부의 정부혁신적 측면이 전적으로 도외시되지는 않았다고 하더라도, 전자정부의 개념에서 정부혁신의 요소는 별로 부각되지 않고 있음을 엿볼 수 있다. 행정혁신, 전자화 대상업무의 처리과정 혁신 등에 대한 행정기관과 공무원의 책무(제4조·제5조), '업무혁신 선행의 원칙'(제7조)에 대한 규정들도 불구하고, 전자정부법의 정책관심이 세 번째 유형에서 두드러지는 정부혁신의 측면보다는 두 번째 유형의 특징, 즉 업무의 전자적 처리를 통한 행정효율화에 치중하고 있다는 것은 부정하기 어렵다. 이 점은 우리나라 전자정부의 기본성격과 전자정부 추진과정에서 대두된 정책적 애로와 시민사회의 도전을 이해하는데 중요한 단서가 될 것이다.

## 2.2 개인정보와 프라이버시

전자정부에 있어 개인정보의 보호에 대한 논의는 개인정보의 개념을 정의함으로써 그 본질과 범위를 파악하는데 출발점을 둔다. 개인정보를 보호한다고 하면 과연 무엇을 왜 어디까지 보호하는 것인지를 분명히 해야 하기 때문이다. 그런데 개인정보의 개념 규명을 위해 반드시 짚고 넘어가야 할 문제가 하나 있다. 개인정보 보호에 대한 논의에서 언제나 빠짐없이 등장하는 프라이버시와의 관계를 밝히는 일이다. 사실 그동안 국내 문헌들은 프라이버시를 통해 개인정보 보호 문제에 접근하는 것이 주류적 관점이었다.<sup>10)</sup> 즉, 개인정보 보호의 토대로서 프라이버시권의 기원과 법적 근거 및 성질을 규명하고 정보사회의 진전에 따른 새로운 프라이버시의 침해유형

5) Cathia Gilbert Riley, THE CHANGING ROLE OF THE CITIZEN IN THE E-GOVERNANCE & E-DEMOCRACY EQUATION([http://www.electronicgov.net/pubs/research\\_papers/cath/thesi.pdf](http://www.electronicgov.net/pubs/research_papers/cath/thesi.pdf)), 2003: 37-38.

6) 가령 김성태, 2003: 14-29; 황성돈·경진·김현성·명승환·정충식·황승홍, 2000: 55; 황성돈·황승홍·권기현, 1999: 11~20; 정충식, 1997: 95~116; 한국전산원, (1996), 「전자정부 개념 정립 및 구현 방안에 관한 연구」 등을 참조.

7) Division for Public Administration and Development Management, United Nations Department of Economic and Social Affairs.

8) <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan008633.pdf>.

9) <http://www1.oecd.org/publications/e-book/4203071E.PDF> 또는 <http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf>을 참조.

10) 권현영, 2004. 구체적인 예로는 권영성, 2000: 427-431; 김철수, 2000: 522-524; 정영화, 2001: 50-85; 성낙인, 1999: 21-60 등을 들 수 있다.

을 지적하면서 그 대응책으로 외국의 입법사례들을 참조하여 새로운 프라이버시권의 보호영역을 모색하는 것이 국내 법학계의 일반적 경향이었고(김종철, 2001: 24), “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다”는 표현으로 헌법(제17조)에 정착된 사생활의 비밀과 자유, 그리고 그 비교헌법적 준거개념으로서 프라이버시의 보장이라는 틀 안에서 개인정보자기결정권이나 개인정보통제권을 설명하는 방식이 통용되었다.<sup>11)</sup> 그 결과 단순한 편의상의 필요를 넘어 자칫 개인정보와 프라이버시를 동일시하거나 혼동하는 결과를 낳을 우려가 없지 않았다. 그러나 개인정보와 프라이버시는 나라에 따라 또는 법체계적 전통에 따라 상이한 문제에 대한 접근방식의 차이<sup>12)</sup>를 반영하는 법적 실체로서 개념적으로나 이론적으로 서로 구별되는 개념이라고 보아야 한다. 이들 개념을 간략히 비교해 보면 다음과 같다.

먼저, 개인정보는 일상 언어관용에서는 모든 ‘개인에 관한 정보’를 뜻하지만, 법적 보호대상으로 고려되는 개인정보는 그보다 좁은, ‘개인관련성’과 ‘식별가능성’이란 두 가지 기준에 의해 제한된 법기술적 개념이다. 즉, 개인에 관한 정보일 뿐만 아니라 당해 정보에 의하여 개인을 알아볼 수 있는 가능성이 있어야 개인정보로서 보호의 대상이 될 수 있다. 이러한 개인정보 개념은 다수의 외국 입법례에서 통용되고 있을 뿐만 아니라<sup>13)</sup> 우리나라에서도 실정법에 반영되어 있다. 가령 공공기관의개인정보보호에관한법률은 제2조 제2호에서 개인정보를 “생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)”라고 정의한다. 정보통신망이용촉진및정보보호등에관한법률 역시 부호·문자·음성·음향 및 영상 등 정보의 형태를 예시한 것 외에는 대동소이한 정의규정을 두고 있다(제2조 제1항 제6호).<sup>14)</sup>

반면, 프라이버시 또는 프라이버시권(Right to Privacy)에 대한 만족스러운 정의는, Warren과 Brandeis가 프라이버시권을 제창한지<sup>15)</sup> 한 세기가 넘

은 오늘날까지도 여전히 주어지지 않고 있다.<sup>16)</sup> 미국의 경우 헌법상 프라이버시권은 이를 명시한 조항이 없는, 헌법해석을 통해 인정되는 묵시적 권리(penumbral, implied right)에 해당한다(Ferrera et al., 2004: 258). 하지만, 그 기본권으로서의 대상이나 범위, 효력 등을 분명히 하기 위해서도 이를 정의하는 것이 대단히 중요하다. 그럼에도 불구하고 그 개념정의는 여전히 미해결로 남아 있다. 예컨대 Gomeley(1992: 1339)는 “법적 프라이버시에 대하여 하나의 온갖 사이즈에 다 들어맞는 정의(single one-size-fits-all definitions of privacy)를 내리는 것은 그리 가치 있는 일이 아니라는 사실이 판명되었고”, “법적 프라이버시는 네 다섯의 서로 상이한 종류의 법적 권리들로 이루어져 있기 때문에 이들을 하나로 정의한다는 것은 불가능하다”고 단언하였다. Post(2001: 2087) 역시 “프라이버시가 너무 복잡하고 경쟁적이고 모순적인 차원 속에 얽혀 있으며, 다양하고 특수한 의미로 꼭 차 있어, 이따금 그 개념을 유용하게 파악할 수 있을지 자포자기하게 된다”고 슬회하고 있다. 이처럼 프라이버시 개념의 보편적 정의가 어렵기 때문에 개념보다는 그 가치와 중요성을 강조하는데 논의의 초점을 맞추기도 한다(Solove·Rotenberg, 2003: 27).

원래 프라이버시의 어원은 원래 국가보다는 개인에게 속하는 것을 구별하는 의미였던 분리 또는 박탈이란 뜻을 지닌 라틴어 단어에서 연유한다. 즉 이 개념은 공동체(polis)와 시장(ager)의 적정한 경계에 관한 관념과 연계되어 있고, 개인과 공공, 시장과 국가, 또는 사익과 우월한 공익 사이의 구별에 초점을 맞춰 형성된 개념이다.<sup>17)</sup> 그러나 프라이버시 개념의 성좌는 그렇게 단순하지 않으며, 그 동안 판례와 이론적 논의성과에 비추어, 대체로 다음과 같은 서로 상이한 요소들로 이루어지고 있음을 알 수 있다. 가령 Solove·Rotenberg(2003: 27)는 이들 개념군들을 인격권(right of person-

11) 권현영, 같은곳. 이인호, 2001: 50이하; 김주환, 2001: 45이하; 유황빈, 2001: 61이하; 김기중, 1997 등을 참조.

12) 가령 Bennett, 1992; Reidenberg, 2001 등을 참조.

13) EU 개인정보보호지침, 영국 데이터보호법, 프랑스 국가정보처리자유법, 독일 데이터보호법, 벨기에 개인정보보호법, 스웨덴 데이터보호법 등.

14) 그 밖에 개인정보의 구성요소, 범위의 분류 등에 대하여는 권현영, 2004; 정영화, 2002: 22; 박종찬, 2001: 81-84 등을 참조

15) 미국에서 프라이버시권이라는 법적 개념이 등장한 것은 1880

년 Thomas C. Cooley 판사의 민사상 손해배상법(Laws of Torts 1st ed, 1880, Sec. 29)에서 ‘홀로 있을 권리’(the right to be let alone)라는 의미로 프라이버시권을 주장하고, 1890년 Warren과 Brandeis가 이를 더 상세히 분석한 논문(Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy”, 4 Harv. L. Rev. 193, 195 (1890))에서 ‘프라이버시권은 진보된 문명세계에 살고 있는 개인에게 필수적인 것’이라고 주장한 데서 유래한다. 이에 관하여 상세한 것은 서주실, Warren·Brandeis의 The Right to Privacy, 미국헌법연구 제6호, 미국헌법학회, 1995, 45면 이하를 참조.

16) Solove·Rotenberg, 2003: 27; Solove, 2002; Gomeley, 1992; Gavison, 1980.

17) Jeff Weintraub & Krishan Kumar eds., PUBLIC AND PRIVATE IN THOUGHT AND PRACTICE 1997.

hood), 친밀성의 권리(right of intimacy), 비밀의 권리(right of secrecy), 자신에의 접근 제한의 권리(right of limited access to the self) 및 정보통제권(right of control over information) 등으로 집약하고 있고,<sup>18)</sup> 프라이버시를 개인과 조직의 사적 활동에 관한 프라이버시(territorial privacy), 개인의 신체에 대한 타인의 침해에 관련된 신체 프라이버시(physical privacy), 개인의 정보를 스스로 통제할 수 있을 권리와 관련된 정보 프라이버시(information privacy)로 구분하기도 한다.<sup>19)</sup> 미국 UCLA의 제리 강(Jerry Kang)은 프라이버시 개념을 다음 세 가지 범주로 분류한다.<sup>20)</sup> 첫째, 물리적 공간, 특히 개인의 사적 공간이 원치 않는 대상이나 신호 등에 의한 침해로부터 보호된다는 의미이다. 주거 불가침이나 거주이전의 자유 같은 사생활의 자유가 이 범주에 포함된다. 둘째, 프라이버시는 국가 등 누구의 방해도 받지 아니하고 중요한 결정을 할 수 있는 선택의 능력 또는 권리로도 인식된다. 즉, 결정 또는 선택의 프라이버시("decisional privacy")이다. 이러한 프라이버시의 범주는 공간적 영역이 아니라 외부로부터 간섭을 받지 않는 선택의 자유를 중시한다. 미국 연방대법원이 프라이버시권에서 임신 중절 여부를 선택할 권리를 도출한 1973년의 Roe v. Wade 사건 판결<sup>21)</sup>도 이 범주에 해당한다.<sup>22)</sup> 세 번째 범주는 현대 정보혁명의 결과 대두된 개인정보의 흐름과 관련한 '정보 프라이버시'(Information Privacy)이다. 이로부터 개인정보의 수집·처리·이용 등을 통제할 수 있는 권리로서 개인정보자기통제권 또는 개인정보자기결정권이 도출된다. 정보 프라이버시는 Roe v. Wade 판결에서 쟁점이 되었던 결정 프라이버시와는 구별된다. 후자는 개인이 가령 출산이나 양육 같은 중대한 결정을 내릴 경

우 '간섭으로부터의 자유'(freedom from interference)에 초점을 맞추는데 반하여 정보 프라이버시는 일상생활에서 생성되는 개인데이터의 이용, 전달 및 처리에 관련된 것이기 때문이다.<sup>23)</sup> 물론 양자가 전혀 무관한 것은 아니다. 공적 부문과 사적 부문의 조직, 단체들이 개인데이터의 이용, 전달 및 처리를 통해 우리의 선택에 영향을 미치기 때문이다(Schwartz, 2004).<sup>24)</sup> 이렇게 볼 때, 프라이버시의 개념을 Warren과 Brandeis의 "홀로 있을 수 있는 권리(the right to be let alone)"에서 웨스틴이 "개인, 단체 또는 기관들의 자신들에 대한 정보를 언제, 어떻게 그리고 어느 정도로 타인에게 유통시킬 것인지를 스스로 결정할 수 있는 권리"라고 요약한 정보프라이버시<sup>25)</sup>로 변모해 왔다기보다는 그 성좌가 정보프라이버시라는 별까지 외연이 확장되어 왔다고 보는 것이 정확하다(김종철, 2001: 29~30). 그리하여 개인정보의 수집·처리가 확산되고 개인정보 자체가 유통의 대상이 되는 정보사회의 환경에 맞게 새로운 기본권으로서 개인정보통제권 또는 개인정보권<sup>26)</sup>을 이론적으로 재구성하여 사용하여야 한다는 견해가 대두되고 있다(김종철, 2001; 김종철, 2004; 한상희·황승흠·권현영, 2002; 권현영, 2004). 즉, 기존의 연구들이 개인정보통제권의 상위개념으로 제시해왔던 프라이버시권은 개인정보의 통제로 그 외연이 확대되어 왔을지라도, 여전히 사생활보호 중심의 측면<sup>27)</sup>

18) 다양한 개념정의의 소개로는 Solove, 2002; CATE, FRED, PRIVACY IN THE INFORMATION AGE 19-23 (1997) 등을 참조.

19) 교영삼, 전자감시사회와 프라이버시, 한울 아카데미, 1998, 31을 참조.

20) Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1202 (1998).

21) 산모의 생명을 구하기 위한 경우가 아니면 임신의 어느 단계에서든 낙태를 할 수 없다고 규정한 Texas낙태법규정을 위헌으로 판결한 사건이다.(Jane Roe et al., appellants v. Henry Wade, 410 U.S. 113, 93 S.Ct. 705 (1973)).

22) '헌법 제10조가 보장하는, 모든 기본권 보장의 기본이념이라고 할 수 있는 인간의 본질이며 고유한 가치인 개인의 인격권과 행복추구권에 개인의 자기운명결정권이 전제되는 것이고 이 자기운명결정권에는 성행위 여부 및 그 상대방을 결정할 수 있는 성적자기결정권이 또한 포함되어 있다'고 판시한 우리나라 헌법재판소의 결정(헌법재판소 1990.9.10 선고, 89헌마82 결정)도 이 범주에 속한다.

23) 개인정보의 재산권화(propertization) 문제에 관해서는 Schwartz, 2004: 2055를 참조.

24) 이 논문에서 Schwartz는 개인정보의 처리와 의사결정간의 연관관계, 즉 개인정보가 개인의 자율성과 민주질서의 유지에 어떠한 영향을 미치는지를 구명하고 있다.

25) ALAN F. WESTIN, PRIVACY AND FREEDOM, Atheneum, 1967: 7. 이것은 규제정책의 맥락에서 가장 널리 채택된 정의라 할 수 있다. 예컨대 미국의 Privacy Working Group, Information Infrastructure Task Force, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information ([http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin\\_final.html](http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html) 1995.6.6 최종수정) 역시 "개인정보-식별가능한 개인 정보-의 취득, 공개 및 이용에 관한 조건을 결정할 수 있는 개인의 권리"라는 유사한 정의를 채택한 바 있다.

26) "자기정보관리통제권 또는 개인정보자기결정권"(권영성, 2001: 427); "개인정보자기결정권"(이인호, 2002); "자기정보에 대한 통제권"(성낙인, 2001: 439); "자기정보통제권"(차명진, 1991); "정보자기결정권"(김일환, 2001); "정보의 자결권"(정태호, 2000); "개인정보통제권 또는 자기정보통제권"(한상희·황승흠·권현영; 2002) "개인정보통제권"(김종철, 2001) 등 다양한 용어가 사용되고 있으나, 정보주체의 개인정보 통제에 관한 권리(control over personal information) 또는 자기결정권(Selbstbestimmungsrecht)을 의미한다는 점에 있어서는 공통적이다.

27) 전통적인 프라이버시권은 사적 영역의 비밀성을 외부적 간섭으

때문에 새로운 개인정보통제권의 본질을 내포하기에는 부적절하며, 그 정당성을 개인의 인격 보호나 자율성 보호라는 사생활 영역의 보장에 한정시킴으로써 일상화된 정보관리에 대한 적극적 통제나 정치 및 경제 권력에 대한 통제권으로서의 정치적, 헌법적 의미를 담보하는데 부족하였다는 것이다. 이처럼 개인정보통제권을 근거지우는 법적 개념이 원래부터 가지던 특수한 의미 때문에 본질을 왜곡시킬 우려가 있다면, 무리하게 기존의 법 개념에 안주하기보다는 이를 탈피하여 새로운 법 개념으로 재구성하는 것이 필요하며(김종철, 2001: 29~30), 개인정보자기결정권이나 개인정보통제권 등의 프라이버시적 관념이 포함된 용어에서 탈피하여 권리의 객체인 개인정보에 대한 권리라는 보다 포괄적인 개념을 정립하는 것이 바람직하다고 한다. 즉, 개인정보권은 개인정보에 대한 권리를 포괄하는 상위개념으로 보아 권리의 객체가 되는 개인정보를 범주화하고 이에 대응하는 권리를 세분화·체계화함으로써 보호와 이용의 조화로운 법률관계를 형성하도록 하는 적극적 효과를 기대할 수 있다고 한다(권헌영, 2004).

이러한 주장들은 경청할 만하다. 앞서 살펴 본 바와 같이 프라이버시와 개인정보 둘 중 어느 하나를 상위개념으로 파악하거나 양자를 동일한 차원에서 상하관계에 있는 것으로 보는 것은 오류이며, 또 하필이면 보편타당하게 정의하기 곤란한 프라이버시의 개념(Solove · Rotenberg, 2003: 27)을 통하여 또는 그것을 근거로 삼아 개인정보에 접근해야 할 까닭도 없다. 나아가 개인정보권 또는 개인정보통제권이란 개념을 정립함으로써 프라이버시의 신세를 지지 아니하고도 정보사회 및 전자정부의 권리장전으로서의 의미를 부여할 수 있는 토대를 구축하는 의미도 있을 것이다. 그러나 많은 부분에서 법리적·실천적 공통분모를 가지는 양자를 전혀 무관한 것으로 절연시키려는 관점은 결코 적절하다고 볼 수 없고, 또한 개인정보권 또는 개인정보통제권이란 새로운 기본권 영역의 개척이 필요하다고 할지라도 이를 헌법상 보장되어 온 프라이버시권을 대체하는 것으로 이해한다면

로부터 보호하려는 개인의 권리로서 인정되기 시작했다는 한계를 가진다고 한다. 일반적으로 소극적 의미의 프라이버시권으로 불리는 이 권리의 논거는 자유로운 삶의 주체로서의 개인의 정체성에 관련되기 때문에 신성한 것으로 인정되어야 하며 따라서 제3자-공공기관을 포함하여-의 침해로부터 절대적으로 보호받아야 한다는 데 있다는 것이다. 그러나 이러한 권리는 다양한 정보의 공유 속에 합리적이고 민주적인 결정에 따라 공동체의 운영이 결정되는 것을 골자로 하는 민주주의 이념에 대한 개념이 될 수 있고, 프라이버시권이 가지는 민주주의 이념과의 대칭성은 이 권리가 원래 평범한 개인의 권리차원보다는 권력자와 자산가 등 유명인이 주장해 왔던 것과 무관하지 않다고 한다(김종철, 2001: 32).

그것은 오류이다. 오히려 개인정보에 대한 권리의 많은 부분이, 특히 정보 프라이버시의 경우, 프라이버시 보호에 의해 지지되거나 중첩적으로 보장되는 관계에 있기 때문에, 프라이버시 보장의 법리는 개인정보 보호에서 필수불가결한 핵심요소를 이루는 것으로 보아야 한다. 오히려 양자가 공통되거나 중첩되는 영역인 정보 프라이버시의 보호에 논의의 초점을 맞추는 것이 합당하다고 볼 수 있다. 우리나라 대법원은 인간으로서의 존엄과 가치, 행복추구권, 국가의 기본권조장의무를 규정한 헌법 제10조와 사생활의 비밀과 자유를 보장한 헌법 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 보장하려는 데에 그 취지가 있는 것으로 해석되는바, 원심이 적법하게 확정한 바와 같이, 피고 산하 국군보안사령부가 군과 관련된 첩보 수집, 특정한 군사법원 관할 범죄의 수사 등 법령에 규정된 직무범위를 벗어나 민간인인 원고들을 대상으로 평소의 동향을 감시·파악할 목적으로 지속적으로 개인의 집회·결사에 관한 활동이나 사생활에 관한 정보를 미행, 망원 활용, 탐문채집 등의 방법으로 비밀리에 수집·관리하였다면, 이는 헌법에 의하여 보장된 원고들의 기본권을 침해한 것으로서 불법행위를 구성한다고 하지 않을 수 없다”고 판시하여 프라이버시권의 정보통제권으로서의 측면을 확인한 바 있는데,28) 프라이버시권으로부터 또는 그와 더불어 정보통제권을 도출했다고 하여 맞할 바는 없을 것이다.

반면, 프라이버시를 개인정보통제권으로 개념화하는 것은 개인이 어떤 유형의 정보에 대해 통제권을 가지는지를 분명히 정의하지 못하기 때문에 너무 모호하고 개인정보에 대한 정의는 때로 너무 넓거나 때로 너무 협소하다고 비판하는 Solove(2003: 1115)의 지적도 간과할 수 없다. 그는 개인정보통제권이라고 할 때, 통제의 개념도 이를 일종의 소유권으로 정의하는 등 불분명한 부분이 많고, 정보통제의 개념도 하고 프라이버시를 정보에 국한시키거나 프라이버시의 영역에서 결정의 자유를 배제하여 너무 배타적으로 개인의 선택에 초점을 맞추고 있다고 비판하고 있다(Solove, 같은 곳). 이는 결과적으로 프라이버시를 개인정보통제권으로 개념화하는 것이 이론적으로 적지 않은 취약점을 가진다는 사실을 드러내는 것이기 때문에 ‘프라이버시 대신 개인정보통제권이나 개인정보권’을 기본권으로 정립하는 경우에도 마찬가지로 문제점을 안게 되는 것이다. 요컨대, 다음의

28) 대법원 1998. 7. 24. 선고 96다42789 판결【순해배상(기)】(공1998.9.1.(65).2200).

도식에서 보는 바와 같이, 프라이버시의 성과에는 개인 정보로 커버되지 않는 부분이 있는 반면, 프라이버시와 직접 또는 간접적으로 연관되지 않는 개인정보 영역과 개인정보에 대한 정보주체 등의 권리도 성립할 수 있는 것이다. 후자의 법적 보호문제 역시 정보프라이버시 보호 문제와 더불어 정보사회와 전자정부의 법정책적 맥락에서 검토되어야 할 것임은 물론이다.

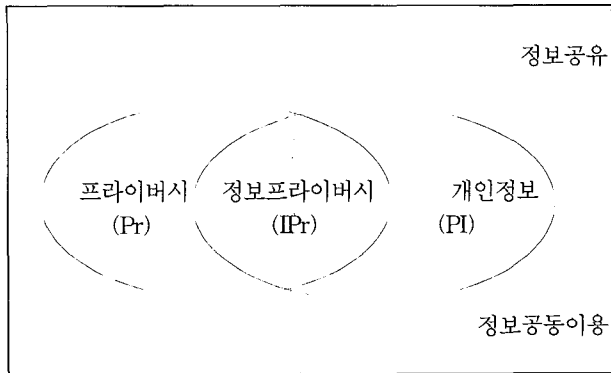


그림 1 프라이버시·개인정보·정보공유 등의 관계

## 2.3 전자정부와 개인정보 보호의 관계

### 2.3.1 개설

일반적으로 전자정부와 개인정보 보호와의 관계를 설명해 주는 이론이나 이론적 모형은 존재하지 않는다. 그러나 개인정보 보호의 문제가 그것을 포함한 정보보호, 즉 정보의 안전(information security)과 더불어 신뢰성이란 변수를 구성하며 온라인 환경에서의 신뢰를 구축함에 있어 프라이버시·개인정보의 보호가 매우 중요하다는데 대해서는 폭넓은 공감대가 형성되어 있다(OECD, 2003c: 7).<sup>29)</sup> 프라이버시는 신뢰의 전제조건(precondition for trust)이며 신뢰는 다시 프라이버시에 영향을 미친다(Samarajiv, 1998: 2). 이 점은 전자정부와 개인정보 보호에 대해서도 마찬가지로 적용된다.<sup>30)</sup> 앞서 지적하였듯이 국민에게 개인정보가 오·남용되지 아니하고 해킹이나 유출 등의 위협으로부터 안전하다는 신뢰를 줄 수 있느냐 하는 것이 전자정부의 성

공을 좌우하는 관건이 되기 때문이다. 개인정보의 충분한 보호가 전자정부의 성과를 좌우하는 핵심적 성공요인의 하나라는 것, 그리고 전자정부 활성화의 선결조건을 이룬다는 것은 널리 공유되고 있는 생각이다(김성태, 2003: 29; OECD, 2003a: 48, 51; 이민영·주지홍, 2003).

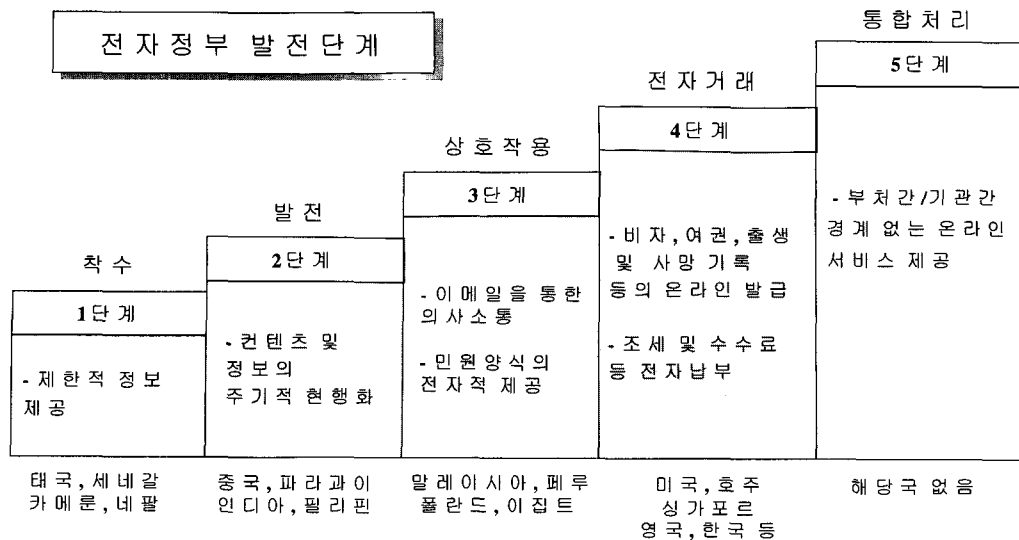
그런 의미에서 매년 세계 각국의 정부 웹사이트들을 대상으로 거기서 제공되는 온라인 서비스에 초점을 맞춰 전자정부를 비교·평가해 오고 있는 미국 브라운대 토브맨공공정책연구소(Taubman Center for Public Policy)가 전자정부 평가항목으로 정보보안과 함께 프라이버시 보호를 포함시키면서, “보통 시민들이 그들의 온라인 정보와 서비스 활동이 안전하다고(safe and secure) 느끼지 못한다면, 전자정부는 그리 빨리 성장하지 않을 것”이라고 지적한 바 있는데, 그 평가 방법론, 조사범위나 평가결과의 시사점에 관한 한 논란의 여지가 있을지라도, 적절한 것이었다.<sup>31)</sup> OECD 역시 성공적 전자정부를 위한 지도원리(Guiding Principles for Successful E-Government)에서 전자정부의 성공요인의 하나인 고객지향성(Customer Focus)의 항목에 프라이버시를 포함시키고, 전자정부와 관련하여 개인의 프라이버시를 보호하기 위한 메커니즘이 마련되어 있는지 여부, 그리고 프라이버시 보호를 위한 광범위한 기준들이 공공기관들 사이의 정보의 공유를 그 남용방지와 함께 허용하고 있는지 여부를 척도로 제시한 바 있다.<sup>32)</sup>

29) 일례로 1997년 11월 19일부터 21일까지 핀란드 Turku에서 개최된 OECE 회의(“Dismantling the Barriers to Global Electronic Commerce”)에서 프라이버시 보호가 소비자 신뢰(consumer trust)의 핵심 요소이자 전자상거래 발전을 위한 필수불가결의 조건(sine qua non condition)임을 확인한 바 있다.

30) Global Internet Policy Initiative, Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners - Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online, 2003 (<http://www.internetpolicy.net/practices/030501pia.pdf>).

31) 평가결과 한국은 전세계 198개국중 30.5점을 받아 32위를 차지했는데, 'Privacy'와 'Security' 항목에서 각각 14점과 7점을 받았다. 상위권에 든 국가 대부분이 그 항목에서 80-90점을 받은 것을 감안할 때, 그것이 평가결과 전체에 매우 중대한 영향을 미쳤을 것으로 추정된다. 43.8점을 받아 2위를 한 싱가포르는 97점과 93점, 3위(41.9) 미국은 82점과 67점, 4위(40.3) 캐나다는 90점과 23점, 7위(36.7) 호주는 97점과 23점을 받았고, 44.3점을 받아 1위를 한 대만도 50점과 54점을 받았다. 특히 중국이 6위(37.3)를 차지하며 이 항목에서 각각 35점, 35점을 받은 것은 괄목할 만한 사실이다(<http://www.insidepolitics.org/egovt/04int.pdf>; <http://www.insidepolitics.org/Press Release/04int.html>). 평가자에 따르면, 프라이버시 정책의 경우 공시된 프라이버시 정책이 방문자 정보에 대한 상업적 마케팅을 금지하고 있는지 여부, 쿠키나 방문자들의 개인적 프로필의 이용, 방문자의 사전 동의 없이 개인정보를 공개하는지 여부, 또는 법집행기관에게 방문자 정보를 공개하는지 여부 등을 세부평가항목으로 삼아 조사했는데, 조사결과, 방문자 프라이버시의 보호가 매우 취약하다는 사실을 확인했다고 한다. 기행 조사대상 정부 웹사이트 가운데 방문자 정보의 상업적 마케팅 금지는 10%, 쿠키 금지는 6%, 개인정보의 공유 금지는 10%, 법집행기관과의 정보공유를 금지하는 경우는 8%에 불과했다(West, 2004: 6-7; <http://www.insidepolitics.org/egovt/04int.pdf>).

32) OECD, 2003a: 19. Elizabeth Muller, From e-Government



(자료 : UN, Benchmarking e-Government, 2002.6)

그림 1 전자정부 발전단계

### 2.3.2 전자정부의 발전과 개인정보 보호 문제의 대두

아래 도식은 세계 각국의 전자정부 발전수준을 측정하기 위한 범주들을 도식화한 것이다(UN/ASPAs global survey). 2002년에 실시된 이 조사에서 한국은 영국, 호주, 싱가포르 등과 함께 4단계인 전자거래 단계(Transactional Web Presence)에 도달한 나라로 평가되었다.<sup>33)</sup> 그런데 전자정부와 개인정보 보호의 관계에 관한 흥미로운 사실은 전자정부에 있어 개인정보 보호 문제는 전자정부가 어느 정도 성숙단계에 접근해야 비로소 대두된다는 것이다.

전자거래 단계에서는 운전면허증 갱신, 출생신고 등 각종민원이 온라인으로 완전하고 신뢰성 있게 처리되며, 정부 웹사이트를 통해 이용자들의 특수한 수요나 선호에 따른 개인화 서비스가 가능해지게 되는 단계이다. 그 경우 이용자가 민감한 개인정보를 온라인으로 제출하는 일이 빈번히 일어나므로 정보보호, 프라이버시, 인증 등의

문제들이 부각될 수밖에 없다. 특히 5단계, 즉 통합처리 단계로 나아가려면, 정부 웹사이트에 대한 국민의 신뢰를 구축하고, 시민들의 선호와 요구에 따른 맞춤형 웹사이트를 구성하는 것이 필요한데, 그 경우 프라이버시, 개인정보의 보호에 대한 신뢰를 이끌어 내는 것이 필수적이다. 나아가 급속히 발전하는 유비컴 환경에서 개인정보 보호의 문제는 더욱 긴박한 과제로 대두된다. 보이지 않는 컴퓨팅으로 별도의 명령행위 없이 언제 어디서나 개인의 행적을 집약적·전자적 기록으로 남기거나, 전자적인 측면에서 원하기만 하면 개인을 완전히 발가벗길 수 있게 된다는 점에서 위험요인이 현저히 커지고, 그만큼 'u-전자정부'에 있어 개인 정보·프라이버시의 한계와 보호 문제가 긴절한 현안과제로 대두될 수밖에 없기 때문이다.<sup>34)</sup>

### 2.3.3 전자정부와 개인정보 보호: 전자정부의 신뢰성 함수

전자정부와 개인정보 보호의 관계는 무엇보다도 전자정부의 신뢰성 함수에 의해 좌우된다. 신뢰성 함수는 후자가 전자에 대한 불신을 증대시켜 저해하는 방향으로 작용하는 부(負)의 함수, 즉 불신의 함수와, 후자가 전자의 신뢰성을 증진시켜 그 추진을 용이하게 만드는 정(正)의 함수, 즉 신뢰의 함수, 두 가지 측면에서 구체화된다. 이 두 가지 함수관계는 전자정부 추진에 있어 개인정보 보호가 가지는 이중적 의미를 집약적으로 보여준다. 이들 함수관계를 그 주요변수들을 중심으로 간략히 살펴보기로 한다.

to e-Governance: The OECD Experience E-Government Project OECD SitExpo 2004 (<http://unpan1.un.org/intradoc/groups/public/documents/CAFRAD/UNPAN015841.pps>) 는 그 밖에 온라인상담(Online consultation), 국제협력이란 요소를 제시하고, 프라이버시 문제를 책임(Responsibility)의 요소로 다루면서 책임소재를 명확하게 하기 위한 업무분장의 유무, 전자정부의 수요, 비용, 편익 및 기대효과를 조사·평가하기 위한 제도적 틀의 유무와 함께 전자정부와 관련하여 개인의 프라이버시를 보호하기 위한 메커니즘이 마련되어 있는지 여부, 그리고 프라이버시보호를 위한 광범위한 기준들이 공공기관들 사이의 정보의 공유를 그 남용 방지와 함께 허용하고 있는지 여부를 성공요인으로 내세우고 있다.

33) 미국은 1993년부터 정보제공 단계, 1998년부터 전자거래 단계를 거쳐, 2001년부터는 서서히 통합·변혁의 단계로 나아가고 있는 것으로 평가된다.

34) 정준현, '유비쿼터스컴퓨팅과 프라이버시보호', 제2회 개인정보 보호심포지움, 2003. 12. 142.

가. 불신의 함수

1) 정보위험(privacy risk or information peril: pr)의 증대

비약적인 기술발전 및 그에 따른 정보 집적과 연동으로 인한 정보위험이 커질수록 전자정부에 대한 불신도 증가하기 마련이다. 정부는 시민들 개개인에 대한 데이터의 프라이버시를 보호할 수 있는 정책과 기술적 해결책들을 계속 개발해야 하며, 이 문제는 제대로 처리되지 못할 경우 다른 어느 것보다도 심각하게 전자정부에 대한 지지를 손상시킬 가능성이 크다고 지적된다(GOV/PUMA, 2002: 3).

로텐버그(Rotenberg, 1998: 3)에 따르면, 기술이 프라이버시를 위협한다(Technology Threatens Privacy). 그는 현대에 이르기까지 기술을 프라이버시 문제의 주요 원천으로 보는 경향이 있었지만, 기술과 감시의 관계가 그리 간단한 것은 아니며, 본래 사생활 침해의 우려가 생기게 된 것은 기술 자체가 아니라 감시(surveillance)를 증폭하고, 일상화·정교화하는 기술의 능력 때문에 생긴 것이라고 한다(Rotenberg, 1998: 4). 일례로 증폭(amplification) 기술은 당초의 조사목적에 의해 정당화 될 수 있는 이상의 정보 수집을 가능하게 해 주는데, 가령 파파라치(papparazzi)의 렌즈는 명사들의 사적 순간을 포착하거나, 범죄자들을 감시하기 위해 설치된 감청 장치가 무고한 사람들의 대화를 기록할 수도 있고, 열추적 장치는 아래층의 마리나나 흡입기 뿐만 아니라 위층에서 두 사람이 사랑을 나누는 것까지 탐지해 낼 수 있는 것이다. 그렇지만, 기술은 반드시 프라이버시에 대한 위협만은 아니며 그 보호수단을 제공하는 경우도 많다(Solove·Rotenberg, 2003: 47ff.; Marx, 1999: 7). 이른바 'PET'(Privacy Enhancing Technology), 즉 암호화(Encryption), 익명화 기술(Anonymizing Technologies) 등이 그러한 예이다. 가령 익명화 기술은 스팸메일을 막을 수 없게 만들기도 하지만, 웹사이트 방문자에 대한 추적 가능성을 차단함으로써 이용자의 프라이버시를 보호해줄 수 있는 것이다. 감시 기술이 사생활을 침해하는 것은 사실이지만, 유익하게 적용되는 경우도 많다는 것도 명백하다. 행위보다 기술을 통제하면 불가피하게 다른 경우라면 허용될 수도 있었을 행위들을 범죄화하는 위험을 초래한다. 그러므로 프라이버시 보호를 위한 입법에 대한 가장 기본적인 교훈은 기술 자체가 아니라 그것에 의하여 기도된 행위에 초점을 맞춰야 한다는 것이다(Rotenberg, 1998: 4).

2) 감수성·안전성 우려(sensitivity and concern: sc)

사람들의 정보 감수성(information sensitivity)이나 전자정부 시스템에 대한 안전성 우려(safety and

security concerns)가 커질수록 전자정부에 대한 불신도 커지는 경향이 있다. 전자정부에 대한 대부분의 조사 연구들은 이구동성으로 프라이버시와 정보안전이 온라인에 접속하는 사람들의 주된 관심사라는 점을 지적하고 있다. 이러한 관심은 단순히 온라인 쇼핑이나 전자상거래 참여에만 관련된 것이 아니라 시민들이 정부 사이트들을 이용하는 방식에 관한 것이기도 하다(Riley, 2003: 36). NEIS 사례에서 보는 바와 같이 정보처리 기술과 능력이 현저히 향상된 오늘날의 컴퓨팅환경에서는 정보 시스템에 집적된 정보의 종류, 민감성 또는 포괄성만으로도 정보 안전성에 대한 우려를 불러일으킬 수 있다. 또한 전자정부의 어느 한 하위 시스템에서 개인정보가 유출되는 사고가 일어나거나 보안상의 취약점이 드러날 경우 그 우려는 훨씬 심각한 양상으로 증폭되며 이러한 사회적, 집단적 학습과정을 통해 정보 감수성도 경우에 따라서는 전자정부 사업 추진의 효율성을 저해할 수준까지 고조될 수 있다.

3) 정보화·정보사회에 대한 의식적인 저항(resistance to information society: ris)

정보화, 자동화, 정보기술, 정보사회 등에 대한 반감, 기술 결정론적 사고에 대한 의식적인 저항도 전자정부에 대한 신뢰를 저하시키는 요인으로 작용할 수 있다. 급속한 정보화가 수반할 가능성이 높은 정보격차(digital divide) 등 정보화 역기능 사례들이 전자정부에 대한 반감을 촉발하여 프라이버시·개인정보의 침해 우려를 강화시킬 수 있다.

4) 권력에의 불신·반감(mistrust and antipathy toward government authority: dag)

정부가 프라이버시를 위협한다. 프라이버시나 개인정보에 대한 가장 심각한 위협은 대부분 정부로부터 온다(Rotenberg, 1998: 4). 사람들은 특히 정부기관이나 공권력에게 민감한 개인정보의 제공을 꺼리는 경향을 보인다. 일례로 2002년 5월 발표된 네덜란드의 Van Dusseldorp and Partners의 조사결과에 따르면 유럽 27개국의 시민들은 정부기관에게 온라인상 신용카드나 은행업무내역 같은 정보의 제공을 꺼리는 일반적인 경향을 보이는 것으로 나타났다.<sup>35)</sup> 아울러 과거 권위주의적 개발독재의 경험을 통해 대중의 의식 속에 고착되고 일상화된 권력에 대한 불신과 두려움이 전자정부에 대한 경계와 불신으로 이어지는 경우도 적지 않다. 더욱이 문화적 전통과 정치사회적 여건에 따라 상이하게 나타나는 사회적 자본으로서의 신뢰여건의 차이 때문에 전자정부에 대한 신뢰가 영향을 받을 가능성도 상존한다.

35) <http://www.europemedia.net/newsletter.asp> Europemedia (2002.4.14. 기준). Riley, 2003a: 35.



나. 신뢰의 함수

- 1) 효과적이고 수긍할 만한 안전성 실증(effective and convincing demonstration of safety and security: ed)

Fountain(2002: 21-22)에 따르면, 시민들은 전자정부와의 관계에서 신뢰와 책임성을 위한 두 가지 조건을 요구하는데, 그 첫째는, 정부의 공정성과 보편성에 신뢰를 가질 수 있어야 한다는 것이고, 둘째는 정부로부터 확실하고 안전한 정보 및 서비스를 제공받음으로써 그들의 신뢰를 계속 유지시켜 줄 수 있는 시스템들을 원한다는 것이다. 이 중 후자에 대한 요구는 효과적이고 수긍할 만한 방법으로 안전성을 실증해 보일 때 비로소 신뢰의 형성으로 이어진다.

- 2) 불신요인의 회피(avoidance of mistrust factors: amf)

교육, 홍보, 공개토론 등을 통한 정보화·전자정부에 대한 저항, 정보사회에 대한 반감·적대감의 회피 또는 완화, 정보화·전자정부의 부작용, 비용 증가 등과 같은 정보불신 요인들의 예방 또는 해소시키기 위한 작업들도 전자정부에 대한 신뢰를 제고시키는 방향으로 작용할 수 있다. 그러나 그 신뢰는 단순한 홍보의 강화보다는 실제로 전자정부의 부작용이나 문제점을 적기에 해결하는 실천적 활동을 통해 더 효과적으로 제고될 수 있을 것이다. 반면 시민들이 정보기술이 프라이버시에 대해 가지는 함의를 제대로 이해할 수 있도록 함으로써 객관적인 가치중립을 견지하는 것이 중요하다. Gary Marx(1999: 6)는 이와 관련하여 다음과 같이 기술하고 있다: “기술을 탈신비화하고 시민들이 그 기술이 가지고 있지 못한 힘에 의존하지 않도록 하는 것이 …… 중요하다. 정보기술의 위력이 과대평가 될 때 ‘감시의 신화’(myth of surveillance)’에 무시무시한 위험이 존재한다. 다른 한편, 기술이 권위들의 주장보다 덜 강력하다는 사실이 드러날 때 정당성은 쇠퇴한다. …… 기술의 잠재력과 한계를 이해해야만 한다.”

- 3) 자유와 권리의 보장(guarantee of freedom and right: gfr)

전자정부의 안전성 확보를 위한 자유와 권리를 실효적으로 보장하는 것도 전자정부에 대한 신뢰를 제고시켜 주는 요인이 될 것이다. 시민들은 자신들의 프라이버시나 개인정보를 지킬 수 있는 효과적인 법적 수단이 권리의 형태로 보장되어 있을 때 비로소 안심하고 전자정부와 거래를 하기 시작한다.

- 4) 혁신 효과(innovation effect: if)

전자정부는 시민들에게 앞에서 지적하였듯이 무엇보다

다도 효율성 제고와 서비스 개선의 약속으로 다가온다. 전자정부를 통한 행정 서비스의 편익이 증진되고, 업무 재설계 및 혁신의 성과가 가시화될 경우 전자정부에 대한 신뢰도 상승하게 된다.

다. 전자정부의 신뢰성 함수

이제까지의 논의를 간략한 논리적 수식으로 요약하면 다음과 같다:

- 전자정부에 대한 불신(mistrust)은  $f(\text{pr} \cdot \text{sc} \cdot \text{ris} \cdot \text{s} \cdot \text{dag} \cdot \dots \cdot \dots)$ 로 표시된다.
- 전자정부에 대한 신뢰(trust)는  $f(\text{ed} \cdot \text{amf} \cdot \text{gfr} \cdot \text{if} \cdot \dots \cdot \dots)$ 로 표시된다.
- 따라서 전자정부의 성공요인의 하나인 신뢰성은  $f(\text{trust} - \text{mistrust})$ 로 표시된다.

2.4 전자정부의 권리장전으로서 개인정보 보호

과거 프라이버시의 외연이 확장되는 과정에서 대두된 개인정보의 보호 문제는 전자정부가 급속히 발전하고 정보통신환경이 유비쿼터스컴퓨팅 단계로 접어들고 있는 오늘날의 맥락에서 사뭇 새로운 의미를 부여받게 되었다. 정보화의 시대를 1990년대 이전까지의 정보화 이전 단계, 1990년대의 정보화 초기단계, 2000년대 이후의 유비쿼터스 단계로 구분할 수 있다면, 정보화 이전단계에서의 개인정보 보호 문제는 주로 오프라인에서 국가권력에 의한 사적 영역이나, 자기결정권, 즉 결정의 프라이버시 내지 정보 프라이버시에 이르는 개인정보자기결정권의 침해를 방어하는 차원에서 다루어졌고, 미국의 프라이버시법(1974)이 그 전형적인 범모형을 대표하였다. 그러나 정보화 초기시대에 접어들면서 프라이버시·개인정보 보호의 거점도 오프라인에서 온라인으로 이동하기 시작했고, 정보화가 점점 가속도가 붙기 시작함에 따라 증대된 위험에 상응하여 그 보호의 필요성도 강화되었다. 그러나 이 시기에 있어 프라이버시·개인정보 보호 문제는 주로 정보화의 부작용·역기능을 제어·해소한다는 차원에서 다루어졌기 때문에 정책적 우선순위 면에서 뒤로 밀리는 경우가 많았다. 그러나 정보화가 급속히 진전되고 전자정부의 수준이 고도화되는 유비쿼터스 단계로 접어들면서 프라이버시·개인정보 보호 문제는 정보화 이전단계에서와는 현저히 다른 의미를 부여받게 되었다. 눈부신 정보통신 기술 발전에 따라 공동체 생활의 주요부분이 구조적으로 재편성되고 공공 서비스가 전자적 인터페이스를 통해 제공되는 등 정부와 시민 사회 및 그 구성원 사이의 새로운 교섭방식이 확산되면서 전통적인 공·사의 영역가정이 허물어지기 시작하였고 그 결과 새로운 유비쿼터스 네트워크 환경에서 기존의 자유민주주의 체제와 그 안에서의 개인의 삶이 총체

적 도전을 받게 되었기 때문이다. 이러한 상황에서 개인 정보의 보호는 정보사회·전자정부가 수반하는 시민에 대한 영향과 위협에 대처하기 위하여 시민들에게 보장되어야 할 일종의 권리장전(Bill of Rights)의 의미, 전자정부의 안티테제로서의 의미를 가지게 된 것이다. 그런 뜻에서 정보사회에서 실존인격의 존엄과 자유민주체제의 근간이 총체적으로 훼손될 가능성을 사전에 차단하기 위해 절대적으로 필요한 최소한의 헌법적 보장장치이자 가장 핵심적인 기본권 중의 하나로 개인정보자기결정권을 확립시키고자 하는 이론적 시도도 그런 의미에서 충분한 정당성을 가진다.<sup>36)</sup>

### 3. 결 론

이제까지의 논의결과를 요약하면 다음과 같다.

1. 프라이버시와 개인정보는 개념상으로는 이론상, 그 법적 근거나 범위, 효력 등 여러 가지 측면에서 서로 구별된다.

2. 개인정보의 보호에 있어 보호영역은 프라이버시의 그것을 넘는 반면, 프라이버시의 보호영역 역시 개인정보에 의해 파악되지 않는 여러 부분들을 포함한다. 따라서 프라이버시의 물론 둘 중 어느 하나를 상위개념으로 파악하거나 양자를 동일한 차원에서 상하관계에 있는 것으로 보는 것은 오류이며, 또 하필이면 보편타당하게 정의하기 곤란한 프라이버시의 개념(Solove·Rotenberg, 2003: 27)을 통해 개인정보에 접근해야 할 까닭도 없다. 많은 부분에서 법리적·실천적 공통분모를 가지는 양자를 전혀 무관한 것으로 절연시키려는 관점도 결코 적절하다고는 볼 수 없다.

3. 그러나 개인정보권 또는 개인정보에 대한 통제권이나 자기결정권이란 새로운 기본권 영역의 개척이 필요하다고 할지라도 이를 헌법상 보장되어 온 프라이버시권을 대체하는 것으로 이해한다면 그것은 오류이다. 오히려 프라이버시 보장의 법리는 개인정보 보호에서 필수불가결한 핵심요소를 이루는 것으로 보아야 하며, 프라이버시와 직접 또는 간접적으로 관련이 없는 개인정보 영역에서의 법적 보호문제 역시 정보프라이버시 보호 문제와 더불어 정보사회와 전자정부의 법적정책 맥락에서 검토되어야 할 문제이다.

4. 따라서 전자정부의 신뢰를 구축하기 위한 법적 메커니즘을 수립함에 있어 입법정책의 목표는 프라이버시 보다는 개인정보의 보호를 위한 법제도를 산출하는데 맞추어야 한다. 다만, 정보프라이버시에 대해서는 보다 강화된 법적 보호를 부여하여야 할 것이며, 그 밖의 부분

에 있어서는 개인의 권리보호에 대한 요구와 정보화촉진, 전자정부의 발전, 정보통신산업의 진흥 등 국가적 과제수행의 요구를 비교형량하여 개인정보의 보호와 정보공유 및 공동이용의 측면을 적정한 균형을 유지하는 것이 바람직하다.

5. 효과적인 개인정보의 보호는 성공적인 전자정부의 요체(lynchpin)이다. 정보통신기술의 비약적 발전, 인터넷의 확산, 그리고 그에 따른 인한 변화로 말미암아 개인정보·프라이버시 침해에 대한 대응책 마련이 불가피하게 되었다. 전례없이 증가된 개인정보와 프라이버시 침해 위험이 자칫 사회적 퇴보를 초래할 우려마저 제기되는 실정이다. 그 결과 강력한 정보권을 법적으로 보장 또는 개선하는 것이 정보사회가 가져오는 진보와 변화에 대처하는 필수불가결한 요소라고 지적되고 있다(Riley, 2003b: 8). 물론 Posner(1995: 531, 536; 1981: 231)가 적절히 지적한 바 있듯이, 프라이버시는 사적으로는 훌륭한 가치일지 모르지만 간혹 사회적으로는 악이 될 수도 있고, 정보의 은폐와 왜곡을 가능케 함으로써 사회적 비용을 초래할 수도 있다. 또 Gary Marx (1999: 6)의 지적처럼 극단적인 프라이버시의 보호가 오히려 유해할 수도 있고, 무제한적인 프라이버시가 무제한적인 선이 되는 경우도 거의 없지만, Alan Westin의 말처럼 프라이버시가 현대국가에서의 자유의 심장부에 위치하고 있다는 것도 부인할 수 없는 사실이다. 즉, 개인정보의 보호는 민주적 가버넌스의 중심 요소이자 인본주의적 가치를 대표한다.<sup>37)</sup> 그런 의미에서 개인정보의 보호와 이를 구현하기 위한 입법적 실천은 유비쿼터스 시대 전자정부의 마그나카르타를 정초하는 의미를 가진다.

### 참고문헌

- [1] 고영삼. (1998). 「전자감시사회와 프라이버시」. 한울;
- [2] 권영성. (2001). 「헌법학원론」. 법문사;
- [3] 권현영. (2004). 전자정부시대 개인정보보호법제의 쟁점, 정보화정책 2004 가을호;
- [4] 김기중. (1997). “전자주민카드와 전자감시사회”, 한국정보법학회 발표자료 (1997.3.17);
- [5] 김동원. (2003). 개인정보수집에서 프라이버시와

37) Paul Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev. 553 (1995); Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707 (1987); Alan Westin, Privacy and Freedom 23-26 (1967) 등을 참조.

36) 이인호, 1999: 62- 67; 김종철, 2001: 23- 44 등.

- 경쟁가치들의 경합과 균형, 정보화정책 제10권 제4호, 2003년 겨울, pp.73~91;
- [6] 김성태. (2003). 「전자정부론 - 이론과 전략」 (법문사);
- [7] 김일환. (2001) “정보자기결정권의 헌법상 근거와 보호에 관한 연구.” 「공법연구」제29집 제3호;
- [8] 김종철. (2004) “전자정부와 개인정보보호의 조화-이념적 측면을 중심으로-.” 「개인정보보호 정책 토론회(2004.4.21) 자료집」. 정부혁신지방분권위원회;
- [9] 김종철. (2001). “헌법적기본권으로서의 개인정보통제권의 재구성을 위한 시론.” 「인터넷법률」제4호. 법무부;
- [10] 김주환. (2001) “디지털시대의 개인정보보호와 시민권.” 「인터넷법률」제4호. 법무부;
- [11] 김철수. (2000) 「헌법학개론」. 박영사;
- [12] 김철완·이민영. (2000). 「인터넷 개인정보보호에 관한 법제도 연구」. 정보통신정책연구원;
- [13] 민주사회를 위한 변호사 모임. (2003). “정보통신관계법”, 「전자정부시대 개인정보보호제도 개선방안 토론회 자료집」. 정부혁신지방분권위원회 (2003. 7.25);
- [14] 박종찬. (2001). “정보화시대의 개인정보 보호방안 연구.” 인터넷법률 제4호. 법무부;
- [15] 성낙인. (1999). “프라이버시와 개인정보보호를 위한 입법정책적 과제.” 「영남법학」 제5권 제1·2호;
- [16] 성낙인. (2001). 「헌법학」. 법문사;
- [17] 손상영 외. (1998). 「정보사회에 대비한 일반법 연구(Ⅱ)」. 정보통신정책연구원;
- [18] 유황빈. (2001). “디지털시대의 개인정보보호 기술.” 인터넷법률 제4호. 법무부;
- [19] 이동훈. (2004). 전자정부와 개인정보보호, Information Security Review(한국정보보호진흥원) 제1권 제2호, 69-83;
- [20] 이민영·주지홍. (2003) “전자정부시대의 개인정보보호” 「KISDI 이슈리포트」. 정보통신정책연구원;
- [21] 이은우. (2004). “개인정보보호법안의 주요골자.” 「개인정보보호법 인권시민사회단체(안) 공청회 자료집」(2004.5.27);
- [22] 이은우. (2003). “정보의 수집과 유통을 통제하기 위한 독립감독기구의 구성, NEIS 이후 전자정부에서의 정보인권 어떻게 지킬 것인가.” 「민주사회를위한변호사모임 토론회 자료집」;
- [23] 이인호. (2004). “프라이버시법제정을위한연석회의 공청회 토론요지.”(www.wv.or.kr (2004. 5.27))
- [24] 이인호. (2003). “전자정부에서 정보프라이버시의 실현과제.” 「정보화사회에서의 인권」. 국가인권위원회 토론회 자료집(2003.8.19);
- [25] 이인호. (2002). “디지털시대의 정보법질서와 정보기본권.” 「디지털시대의 헌법질서」. 정보통신정책연구원 정보사회법제도연구센터·중앙대학교 법학연구소 공동학술세미나 자료집;
- [26] 이인호. (2001). “주민등록번호·지문날인과 개인정보자기결정권.” 「인터넷법률」제8호. 법무부;
- [27] 이인호. (1999). “정보사회와 개인정보자기결정권”, 중앙법학 창간호, 중앙법학회;
- [28] 임규철. (2003). “NEIS와 개인정보자기결정권-국가인권위원회의 NEIS 결정을 중심으로-.” 「인권과정의」. 323호;
- [29] 장여경. (2003). “공포체험, 전자정부에 단지 걸다.” 「월간 네트워크」, 2003년 7월호.(<http://networker.jinbo.net/nw-news/show.php?docnbr=19>);
- [30] 전자정부특별위원회. (2003) 「전자정부백서」;
- [31] 정만희. (2000). 프라이버시권 : 언론보도에 의한 침해와 구제를 중심으로. / 考試界 45권 11호 (525호), 42-54 국가고시학회;
- [32] 정보통신부. (2003). 「전자정부시대 개인정보보호제도 개선방안 토론회 자료집」(정부혁신지방분권위원회 2003.7.25);
- [33] 정부혁신지방분권위원회(전자정부법제정비소위원회). (2004). 1차 - 4차 개인정보보호 정책포럼 자료집(2004.4.21, 5.19, 6.16, 6.24);
- [34] 정부혁신지방분권위원회. (2003). 국무회의 자료, “참여정부의 전자정부 비전과 추진원칙”(2003. 5.6);
- [35] 정부혁신지방분권위원회. (2003). 「전자정부시대 개인정보보호제도 개선방안 토론회 자료집」(2003.7.25);
- [36] 정부혁신지방분권위원회. (2003). “전자정부로드맵.” 「정부혁신지방분권 로드맵」(2003.8.14).
- [37] 정부혁신지방분권위원회. (2003a). 「전자적 민원처리의 촉진을 위한 일괄정비 대상법령」(2003. 10.2)
- [38] 정부혁신지방분권위원회. (2003b). “전자정부 관련 법제정비방안.” 제24회 국정과제회의 자료 (www.innovation.go.kr (2003.10.2)).

- [39] 정영화. (2004). "개인정보침해에 대한 사전·사후적 구제제도," 정부혁신지방분권위원회(전자정부법제정비소위원회), 3차 개인정보보호 정책 포럼, 2004. 6. 16.;
- [40] 정영화. (2002) "인터넷상 개인정보보호 및 분쟁 해결에 관한 연구." 「인터넷법연구」 제1호. 한국인터넷법학회;
- [41] 정영화. (2001) "사이버스페이스와 프라이버시권-현행 개인정보보호법제의 문제점을 중심으로-." 「헌법학연구」 제6권 제3호;
- [42] 정재훈. (1998). 민간부문에서의 정보프라이버시 보호. / 정보법학, 창간호 2호 (98.12) 123-170 한국정보법학회;
- [43] 정충식. (1997). 「전자정부론」 (녹두).
- [44] 정찬모 외. (1999). 「정보사회에 대비한 일반법 연구(Ⅲ)」. 정보통신정책연구원;
- [45] 정찬모. (1997). "개인정보보호에 관한 국제적 입법동향 및 우리의 대응." 「정보사회연구」. 1997 가을호. 정보통신정책연구원;
- [46] 정태호. (2000). "현행 인구주택총조사의 위헌성-독일의 인구조사판결(BVerfGE 65,1)의 법리분석과 우리의 관련법제에 대한 반성-." 「법률행정논총」 제20집. 전남대학교 법률행정연구소;
- [47] 조화순. (2004). "거버넌스 관점에서 본 NEIS 갈등사례 연구." 「정보화정책」 2004년 봄. 한국전산원;
- [48] 차맹진. (1991). 「프라이버시보호와 자기정보통제권」. 인하대 박사학위논문;
- [49] 참여연대. (2003.7.25). 「전자정부시대 개인정보보호제도 개선방안 토론회 자료집」. 정부혁신지방분권위원회;
- [50] 프라이버시법제정을위한연석회의. (2004). 「개인정보보호법 인권시민사회단체(안) 공청회 자료집」 (2004.5.27);
- [51] 한상희. (2002). "정보화와 헌법." 「디지털시대의 헌법질서」. 공동학술세미나 자료집. 정보통신정책연구원 · 중앙대학교 법학연구소;
- [52] 한응길 인격권의 보호 : 프라이버시권과 관련하여. / 東亞法學 26호 (99.12) 27-71 1999 동아대학교 출판부;
- [53] 한위수 프라이버시 침해 관련 국내 판결의 동향 . / 言論仲裁 19권 2호 (통권71호 99.06. 여름) (99.06) 47-61 1999 언론중재위원회
- [54] 행정자치부. (2003). "공공기관의 개인정보보호 법개정안 토론자료." 「전자정부시대 개인정보보호 제도 개선방안 토론회 자료집」. 정부혁신지방분권위원회(2003.7.25);
- [55] 홍성걸, 개인정보보호와 정책갈등 - NEIS 사례를 중심으로 -, Information Security Review(한국정보보호진흥원) 제1권 제2호, 27-46;
- [56] 황주성 · 최선희. (2003). "전자정부 사업과 개인정보보호 이슈-NEIS를 중심으로." 「KISDI 이슈리포트」. 정보통신정책연구원;
- [57] 홍준형. (1998). 「전자정부의 전개와 행정법의 과제」, 『민주헌정과 국가정보화』 헌법제정 50주년 기념 학술대회 자료집, 주최: 한국공법학회, 1998. 6. 26;
- [58] 황성돈 · 경건 · 김현성 · 명승환 · 정충식 · 황승흠. (2000). 「전자정부 법제화의 기본논리와 법안」, (한국의국어대학교 · 행정자치부);
- [59] 황성돈 · 정충식. (2002). 「전자정부의 이해」. 다산출판사;
- [60] 황성돈 · 황승흠 · 권기현. (1999). 「21세기 전자정부 구현을 위한 주요 입법과제와 추진방안」, (국가과학기술자문회의);
- [61] 황승흠. (2000). 「인터넷과 전자정부: 전자정부법 논의를 중심으로」, 『국제법무연구』 제5호, 경희대학교 국제법무대학원;
- [62] 황인호. (2001). 「개인정보보호제도에서의 규제에 관한 연구」. 건국대학교 박사학위논문.
- [63] 황주성 · 최선희. (2003) "전자정부 사업과 개인정보보호 이슈-NEIS를 중심으로." 「KISDI 이슈리포트」. 정보통신정책연구원;
- [64] 황주성 · 권현영 · 전수아 · 최선희. (1997). 「전자정부구현을 위한 관계법령 정비」정보통신정책연구원;
- [65] Bennett, Colin J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press;
- [66] Cate, Fred. (1997). Privacy in the Information Age;
- [67] Davies, Simon. (1998). The New Frontiers of Privacy ([http://www.unesco.org/web-world/infoethics\\_2/eng/papers/paper\\_12.rtf](http://www.unesco.org/web-world/infoethics_2/eng/papers/paper_12.rtf));
- [68] EU. Directive 95/46/EC. "Directive of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data";

- [69] Ferrera, Lichtenstein, Reder, Bird, Schiano. (2004). *Cyberlaw: Text and Cases*, Second Edition, Thompson;
- [70] Fountain, Jane E. (2002). *Developing a Basic Research Program for Digital Government: Information, Organizations and Governance* (Report of a national workshop held in May 2002: <http://verdi.unisg.ch/org/idt/ceegov.nsf/>);
- [71] Gavison, Ruth. (1980). *Privacy and the Limits of Law*, 89 *Yale L.J.* 421;
- [72] Gomeley, Ken. (1992). *One Hundred Years of Privacy*, 1992 *Wis.L.Rev.* 1335;
- [73] GOV/PUMA. (2002). *OECD E-Government Project Key Issues and Findings* (26th Session of the Public Management Committee Paris, 30-31 October 2002: [http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/\\$FILE/egov\\_key\\_issues\\_findings.pdf](http://webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/$FILE/egov_key_issues_findings.pdf));
- [74] Kang, Jerry. (1998). *Information Privacy in Cyberspace Transactions*, 50 *Stan. L. Rev.* 1193;
- [75] Kuhlen, Rainer. (1998). *Trust a Principle for Ethics and Economics in the Global Information Society*, Vortrag auf dem zweiten UNESCO-Kongreß über Informationsethik, Monte Carlo, 1.-3. Oktober 1998 [http://www.unesco.org/webworld/infoethics/papers/paper\\_29.rtf](http://www.unesco.org/webworld/infoethics/papers/paper_29.rtf);
- [76] Lessig, Lawrence. (1996). *Reading Constitution in Cyberspace*, 45 *Emory L.J.* 869;
- [77] Marx, Gary T. (1999). *Privacy and Technology* (<http://web.mit.edu/gtmarx/www/privantt.html>);
- [78] OECD. (2003a). *The e-Government Imperative* (OECD e-Government Studies: <http://www1.oecd.org/publications/e-book/4203071E.PDF>);
- [79] OECD. (2003b). *Checklist for e-Government Leaders* (<http://www.oecd.org/dataoecd/62/58/11923037.pdf>);
- [80] OECD. (2003c). *Privacy Online - OECD Guidance on Policy and Practice* (<http://www1.oecd.org/publications/e-book/9303051E.PDF>);
- [81] Posner, Richard A. (1995). *Overcoming Law*;
- [82] Posner, Richard A. (1981). *The Economics of Justice*;
- [83] Post, Robert C. (2001). *Three Concepts of Privacy*, 89 *Geo.L.J.* 2087;
- [84] Reidenberg, Joel R. (2001). *Privacy Protection and the Interdependence of Law, Technology and Self-Regulation* ([http://www.paris-conference-2001.org/eng/contribution/reidenberg\\_contrib.pdf](http://www.paris-conference-2001.org/eng/contribution/reidenberg_contrib.pdf));
- [85] Riley, Thomas B. (2003a). *Security vs. Privacy: Striking the Balance - A Comparative Analysis of Canada, the United Kingdom and the United States* ([http://www.electronicgov.net/pubs/research\\_papers/slp/Sec&PrivPaper03n03.doc](http://www.electronicgov.net/pubs/research_papers/slp/Sec&PrivPaper03n03.doc));
- [86] Riley, Thomas B. (2003b). *The Information Society: The Role of Information in the Emerging Global E-Government, E-Governance and E-Democracy Environments* ([http://www.electronicgov.net/pubs/research\\_papers/tracking03/IntlTrackingReporttApr03no3.pdf](http://www.electronicgov.net/pubs/research_papers/tracking03/IntlTrackingReporttApr03no3.pdf));
- [87] Rotenberg, Marc. (2001). *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, *Stan. Tech. L. Rev.* 1 ([http://stlr.stanford.edu/STLR/Articles/01\\_STLR\\_1](http://stlr.stanford.edu/STLR/Articles/01_STLR_1));
- [88] Rotenberg, Marc. (2000). *Protecting Human Dignity in the Digital Age* ([http://webworld.unesco.org/infoethics2000/documents/study\\_rotenberg.rtf](http://webworld.unesco.org/infoethics2000/documents/study_rotenberg.rtf));
- [89] Rotenberg, Marc. (1998). *Preserving Privacy in the Information Society* ([http://www.unesco.org/webworldinfoethics\\_2/eng/papers/paper\\_10.rtf](http://www.unesco.org/webworldinfoethics_2/eng/papers/paper_10.rtf));
- [90] Samarajiv, Rohan. (1998). *Trust and Privacy in Cyberspace: A View from an Asian Vantage Point* ([http://www.unesco.org/webworld/infoethics\\_2/eng/papers/paper\\_11.rtf](http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_11.rtf));
- [91] Schwartz, Paul M. (2004). *Property, pri-*

- vacy, and personal data. 117 Harv. L. Rev. 2055-2128;
- [92] Sinrod, Eric J. and Jolish, Barak D. (1999). The Emerging Law of Privacy and Speech in Cyberspace, STAN. TECH. L. REV. 1 ([http://stlr.stanford.edu/STLR/Articles/99\\_STLR\\_1/](http://stlr.stanford.edu/STLR/Articles/99_STLR_1/));
- [93] Solove, Daniel J. (2003). "The origins and growth of information privacy law" Fourth Annual Institute on Privacy Law 2003: Protecting your client in a security-conscious world. 748PLI/Pat 29;
- [94] Solove, Daniel J. (2003). Conceptualizing Privacy ([http://law.shu.edu/faculty/full-time\\_faculty/soloveda/concept\\_privacy.pdf](http://law.shu.edu/faculty/full-time_faculty/soloveda/concept_privacy.pdf));
- [95] Solove · Rotenberg. (2003). Information Privacy Law. Aspen Publishers. New York;
- [96] UN. (2002). "Benchmarking E-government: A Global Perspective - Assessing the Progress of the UN Members States";
- [97] Walker, David B. (1999). Privacy in the Digital Age: Encryption Policy A Call for Congressional Action, STAN. TECH. L. REV. 3 ([http://stlr.stanford.edu/STLR/Articles/99\\_STLR\\_3/](http://stlr.stanford.edu/STLR/Articles/99_STLR_3/));
- [98] Walker, Kent. (2000). Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange ([http://stlr.stanford.edu/stlr/articles/00\\_stlr\\_2/](http://stlr.stanford.edu/stlr/articles/00_stlr_2/));
- [99] West, Darrell M. (2004). Global E-Government(<http://www.insidepolitics.org/egovt04int.pdf>)

홍준형



1979 서울대학교 법과대학 법학사  
 1982 서울대학교 대학원 법학석사  
 1986 서울대학교 대학원 박사과정 수료  
 1988~1991 독일 Göttingen대학교 법학박사(Dr.iur.)  
 1985~1995 아주대학교 사회과학대학 법학과 교수  
 1995~현재 서울대학교 행정대학원 교수  
 1999~현재 국무총리행정심판위원회 위원(1999년~현재)

2001~2003 독일 베를린 자유대학 초빙교수  
 2003~현재 정부혁신·지방분권위원회 전자정부전문위원회 위원  
 2004~현재 정보통신부 정보통신정책심의위원회 위원  
 E-mail : joonh@snu.ac.kr

• HCI 2005 •

- 일 자 : 2005년 1월 31일~2월 3일
- 장 소 : 대구 전시컨벤션센터
- 주 최 : 인간과컴퓨터상호작용연구회
- 상세안내 : <http://www.hcikorea.org/hci2005>