2006년도 인권상황실태조사
연구용역보고서

헌법 및 국제인권법의 관점에서 본 개인정보의 취급기준과 그 한계

- 전자정부와 개인정보의 공유·통합의 법적 문제점 -

2006. 12.

국가인권위원회

헌법 및 국제인권법의 관점에서 본 개인정보의 취급기준과 그 한계

- 전자정부와 개인정보의 공유·통합의 법적 문제점 -

2006년도 국가인권위원회 인권상황실태조사
연구용역보고서를 제출합니다

2006. 12.

연구수행기관 전북대학교 산학협력단

연구 책임자 송 기 춘(전북대학교)

연구 보조원 김 영 식(전북대학교 대학원)

김 수 홍(전북대학교 대학원)

이 보고서는 연구용역수행기관의 결과물로서, 국가인권위원회의 입장과 다를 수 있습니다.

< 목 차 >

제1장 서론 ····· 1
1. 연구의 목적과 범위 ····· 1
2. 연구의 방법 ····· 5

제2장 정보인권과 전자정부사업 ····· 7
1. 개인정보보호와 정보인권 ····· 7
2. 정부의 전자정부사업 개요 ····· 12
3. 전자정부의 구현 및 운영원칙 ····· 23
4. 전자정부사업의 일반적인 문제점 ····· 27
5. 소결 ····· 35

제3장 개인정보의 공유·통합의 법적 문제점 ····· 37
1. 개인정보의 공유·통합의 경향 ····· 37
2. 우리나라에서의 개인정보의 공유·통합의 문제사례 ····· 40
3. 외국에서의 정보의 공유·통합 ····· 44
4. 전자정부와 행정정보의 공동이용 ····· 47

제4장 정보인권의 관점에서 본 형사사법정보통합체계의 문제점 ····· 59
1. 미국의 형사사법정보의 공유·통합사업 ····· 59
2. 우리나라 형사사법정보통합체계구축사업의 몇 가지 문제점 ····· 79

제5장 결 론 ····· 90

참고문헌 ····· 96

〈세 부 목 차〉

제1장 서론 ····· 1
1. 연구의 목적과 범위 ····· 1
2. 연구의 방법 ····· 5

제2장 정보인권과 전자정부사업 ····· 7
1. 개인정보보호와 정보인권 ····· 7
가. 정보자기결정권을 보장하기 위한 원칙 ····· 6
나. 개인정보처리의 기본원칙 ····· 8
2. 정부의 전자정부사업 개요 ····· 12
가. 전자정부의 개념 ····· 13
나. 외국의 전자정부사업 ····· 15
(1) 미국 ····· 15
(2) 싱가포르 ····· 15
다. 정부의 전자정부사업의 내용 ····· 20
3. 전자정부의 구현 및 운영원칙 ····· 23
가. 국민편익중심의 원칙 ····· 23
나. 업무혁신 선행의 원칙 ····· 24
다. 전자적 처리의 원칙 ····· 24
라. 행정정보공개의 원칙 ····· 24
마. 행정기관 확인의 원칙 ····· 25
바. 행정정보공동이용의 원칙 ····· 25
사. 개인정보보호의 원칙 ····· 26
아. 소프트웨어 중복개발방지의 원칙 ····· 26
자. 기술개발 및 운영 외주(外注)의 원칙 ····· 26
4. 전자정부사업의 일반적인 문제점 ····· 27

가. 전자정부사업에서 고려하여야 하는 개인정보보호의 기본원칙 · 27
(1) 정보수집 및 활용의 적합성의 문제 ····· 28
(2) 입력정보의 정확성의 문제 ····· 30
(3) 정보처리의 충실성 - 정보의 공유·통합의 문제 ····· 31
(4) 정보관리의 보안성의 문제 ····· 34
5. 소결 ····· 35

제3장 개인정보의 공유·통합의 법적 문제점 ····· 37
1. 개인정보의 공유·통합의 경향 ····· 37
2. 우리나라에서의 개인정보의 공유·통합의 문제사례 ····· 40
가. 교육행정정보시스템(NEIS) ····· 41
나. 전자주민카드사업 ····· 43
3. 외국에서의 정보의 공유·통합 - 미국의 컴퓨터 연결과 관련된 논의 44
4. 전자정부와 행정정보의 공동이용 ····· 47
가. 행정정보의 공동이용의 의의와 필요성 ····· 47
나. 정보공동활용의 구성요소 및 문제점 ····· 48
다. 행정정보 공동이용 추진 ····· 51
라. 행정정보공동이용법안의 문제점 ····· 54
(1) 개인정보보호 ····· 55
(2) 공동이용의 승인주체 ····· 55
(3) 정보주체의 확인 ····· 56
(4) 금지행위 ····· 57

제4장 정보인권의 관점에서 본 형사사법정보통합체계의 문제점 ····· 59
1. 미국의 형사사법정보의 공유·통합사업 ····· 59
가. 사법정보시스템 통합 ····· 61
나. 콜로라도주 형사사법정보통합체계(CICJIS) ····· 60

1) 개요 ····· 60
2) 감사관의 보고(2003년 7월)로 본 문제점 ····· 61
(1) 데이터의 완전성 문제 ····· 61
(2) 시스템의 기능성 문제 ····· 62
(3) 정보의 상위(相違) ····· 62
(4) 시스템 사용교육 필요성 ····· 63
(5) 전자지문채취 ····· 63
3) CICJIS의 미래 ····· 64
다. 형사사법정보통합시스템과 프라이버시권 침해 논의 ····· 64
1) 형사사법정보통합시스템은 프라이버시보호환경을 어떻게 변화시키는가? ····· 65
2) 어떠한 위험을 초래하는가? ····· 68
(1) 누구에게, 어떠한 위험이 있는가? ····· 68
(2) 잘못된 또는 불완전한 정보의 기록으로 인한 위험 ····· 68
(3) 내부자의 불법사용의 문제 ····· 69
(4) 동일성 도용(Identity Theft)의 위험 ····· 70
(5) 청소년기록에 대한 접근의 위험 ····· 70
(6) 폐쇄된 또는 파기된 기록의 위험 ····· 70
3) 정보공유·통합시스템의 운영사례 ····· 71
4) 프라이버시 보호를 위한 정책결정의 고려사항 ····· 74
(1) 정보의 보존과 파기 ····· 74
(2) 정보에 대한 개인의 접근권 ····· 75
(3) 사법정보시스템의 책임성 ····· 75
(4) 통계정보의 이용가능성 ····· 76
(5) 피해자, 증인에 관한 정보의 접근가능성 ····· 76
(6) 가해자와 피해자의 건강정보에 대한 접근가능성 ····· 77
(7) 사회보장번호의 수집, 사용, 배포 ····· 77
5)소결 ····· 77

2. 우리나라 형사사법정보통합체계구축사업의 몇 가지 문제점 ····· 79
가. 사생활의 비밀과 자유 및 정보자기결정권의 침해 ····· 79
1) 사생활의 비밀과 자유 ····· 79
2) 개인정보자기결정권 ····· 83
3) 자기정보통제와 공공기관간의 정보공유 ····· 85
나. 평등권의 침해 문제 ····· 88

제5장 결 론 ····· 90
1. 정보인권의 관점에서 전자정부사업에 대한 치밀한 법적 검토가 필요하다. ····· 90
가. 개인정보 보호의 문제 ····· 90
나. 공공기관간 정보의 공유와 기업과의 공유 문제 ····· 91
2. 행정정보의 공동이용법률안의 내용수정이 필요하다. ····· 91
가. 개인정보의 보호 ····· 91
나. 공동이용의 승인주체 ····· 92
다. 정보주체의 확인 ····· 92
3. 형사사법정보통합체계구축사업은 철저한 법적 검토가 필요하다. ·· 93
가. 사생활의 비밀과 자유 등 기본권을 침해한다. ····· 93
나. 현재 전자문서를 형사재판과정에서 사용하기 어렵다. ····· 94
다. 권력분립주의에 반할 소지가 있다. ····· 94
4. 전자정부사업의 법적 검토 필요성 ····· 94

참고문헌 ····· 96

제 1 장 서 론

1. 연구의 목적과 범위

정보사회에서 정보의 지배 또는 통제는 정보주체에게는 자유의 조건이 되며, 국가 또는 기업에게는 권력과 부의 원천이 된다. 정보주체에게 자기정보통제권[1]이 기본적 인권으로 인정되는 근거는 바로 인간의 삶에서 자기정보의 지배 또는 통제가 가지는 중요성 때문이라 할 수 있다. 반면 국가는 행정업무의 효율성과 행정서비스의 질 제고라는 명분을 내세우면서 업무 관련 정보를 지속적으로 수집·축적하고 있다. 나아가 발전하는 정보기술을 바탕으로 각 부서 단위가 아니라 업무의 내용을 중심으로 각 기관간 중복업무를 간소화하고 필요한 정보를 각 부처간에 공유하는 한편 각 국가기관이 보유하는 정보를 통합 관리하는 전자정부사업[2]을 추진하고 있다. 또한 기업은 인터넷거래 또는 거래흔적('전자지문'[3])을 남기도록 유도하는 방식(예를 들어, 포인트적립을 위한 보너스카드 사용)을 통하여 개인정보를 지속적으로 수집·축적하고 있으며, 이는 모든 영업활동의 기반이자 기초자료로 활용된다. 데이터베이스화된 개인정보가 재산적 가치를 가짐은 말할 나위가 없으며, 소비자들의 인간으로서의 존엄성 자체에 대한 위협이 되기도 한다.[4] "자본주의적 생산양식에서 기업이 소비를 창출

---

1) 헌법재판소의 판례에 의하면 "인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장되는 개인정보 자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리"를 말한다(헌법재판소 2005.07.21, 2003헌마282 결정; 헌재 2005. 5. 26. 99헌마513 결정 등).

2) 전자정부사업에 관해서는 정부혁신지방분권위원회혁신자료실에 게시된 「전자정부 로드맵」(2003) (http://www.innovation.go.kr/policy/view.htm?id=61&page=4&condition=&keyword=&teamcode= 2006. 12. 20. 검색) 참조.

3) 홍성욱, 『파놉티콘-정보사회 정보감옥』, 책세상, 2002.

4) 국가인권위원회, 『금융기관과 인터넷에서의 개인정보 공유현황 실태조사』, 2003, 3면의 각주 8번에서는 "작게는 스팸메일이나 텔레마케팅, 제3자와의 정보 공유 등으로 인한 각종 불안감 및

하고 그로부터 이윤을 추구하기 위한 전략의 하나로 나타나는 소비자 감시(consumer surveillance)의 문제는 국가감시의 문제와 비교도 되지 않을 만큼 엄청난 속도로 그 진행을 가속화하고 있다"[5]고 할 수 있다.

국가감시의 문제가 기업에 의한 소비자 감시에 비하여 점차 비중이 약화된다고는 하지만, 그것은 기업에 의한 감시가 비약적으로 증가해가기 때문에 나타나는 상대적 약화일 뿐, 여전히 증가하고 있다. 과거 수작업에 의하여 처리되던 정보가 정보기기를 통하여 매우 신속하고 정확하게 처리되며, 나아가 각 국가기관과 공공기관의 정보가 공유되고 통합되는 경향이 두드러지게 나타난다. 이는 단순한 정보의 통합이나 공유를 넘어서서 개별적 정보로는 파악하기 불가능 또는 어려웠던 정보를 새롭게 수집할 수 있게 됨을 의미하기 때문에 실제 보다 정교한 개인정보를 보유하게 되는 것이다.[6] 이러한 경향은 국가적 차원에서 진행되는 '전자정부(e-Government)' 사업에 의하여 '합법적'으로 강화되고 있다.

전자정부는 전자정부법 제2조의 정의에 의하면 "정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부"를 말한다. 그 동안 정부기관의 정보에 대해 국민이 접근·이용하고 통제하는 것이 매우 어려웠던 데 비하여 전자정부사업을 통하여 행정기관의 정보가 상당 부분 자발적으로 공개되

정신적 스트레스를 일으키고, 크게는 소비자들의 구매실적에 따라 등급을 재기는 현대판 카스트 제도의 출현이나 정보를 활용한 소비자 심리조작 등의 문제로까지 이어질 수 있다."고 지적한다.

5) 한상희, 「국가감시와 민주주의-공공영역의 창출을 위한 헌법해석」, 프라이버시보호네트워크 제2차 공동토론회 자료집 『개인정보의 국가등록/관리제도의 문제점』, 2001, 18면.

6) 이러한 기관간 정보의 공유 및 통합은 공공기관의개인정보보호에관한법률(이하에서는 "개인정보보호법"이라 한다.) 제10조 제2항은 "보유기관의 장은 제1항의 규정에 불구하고 다음 각호의 1에 해당하는 경우에는 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있다. 다만, 다음 각호의 1에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다. (이하 생략))"고 하고 있으며, 심지어 전자정부구현을위한행정업무등의전자화촉진에관한법률(이하에서는 "전자정부법"이라 한다.) 제21조 제1항은 행정기관은 1. 민원사항의 처리를 위하여 필요한 행정정보 2. 통계정보 문헌정보 등 행정업무의 수행에 참고가 되는 행정정보 3. 공공기관의개인정보보호에관한법률 제10조제2항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보 4. 정보화촉진기본법 제8조의 규정에 의한 정보화추진위원회가 행정기관간 공동이용이 필요하다고 인정하는 행정정보를 공동이용하여야 한다고 규정하고 있다.

고 제공된다는 것은 국민을 위한 행정서비스 실현이나 국민의 알 권리 신장에 의의를 가지는 것이 사실이다. 전자적 방법을 이용한 일처리를 통하여 수작업에 소요되는 인력을 절감하고 행정의 효율성을 높일 수 있다. 행정의 투명성과 효율성을 높이고 국민의 행정에 대한 접근·참여와 이용가능성을 향상시키기 때문에 국민주권을 실현하는 데도 긍정적으로 평가된다.[7)]

그러나 아무리 전자정부사업의 긍정적인 측면을 부각시킨다고 하더라도 앞에서 언급한 것과 같은 정보의 공유와 통합을 통한 국민감시가능성의 증가라는 어두운 면이 간과되어서는 안된다. 전자정부사업은 정부기관간의 정보의 공유와 통합(공동이용)이 필연적으로 수반되며, 나아가 공공기관 및 사적영역의 필요한 정보까지도 통합할 가능성을 열어두고 있다. 전자정부의 핵심적 요소의 하나는 바로 개인정보를 포함한 행정정보의 공동이용이다. 예를 들어, 국세정보서비스는 조세행정에 필요한 개인의 지출정보를 파악하는 게 핵심적 요소가 되므로 국가기관, 지방자치단체 및 공공기관이나 신용카드회사 또는 금융기관이 보유하는 정보와 연계될 것을 예정하고 있다. 이 점은 2006년말 신용카드, 현금영수증, 보험료납부 등 금융정보를 국세청 사이트(국세청 연말정산간소화서비스)[8)]를 통하여 제공받은 것에서도 볼 수 있다.[9)]

기업에 의한 소비자 감시의 문제도 매우 심각한 문제를 야기시키고 있지만, 전자정부사업의 추진에 따른 국가감시의 문제는 이제 정보의 공유와 통합이라는 현상과 함께 보다 심각한 양상을 맞이하고 있다고 생각된다. 정보의 통합·공유를 통하여 기존의 정보와는 다른 정보를 수집하게 되고, 정보의 오류는 그 피해의 규모가 엄청날 수 있기 때문이다. 그렇지만 '전자정부로드맵'에서는 전자정부사업에서 구축되어야 할 법제도의 문제

7) 장용근, 「전자민주주의의 헌법적 연구」, 서울대학교 대학원 박사학위논문, 2004, 229면 참조.

8) http://www.nts.go.kr/call/year_end/index.htm(2006. 12. 20. 검색)

9) 좀 시간이 경과한 자료이긴 하지만, 이인호, 『개인정보보호법제의 현대화방안에 관한 연구』, 국회사무처 법제실, 2005, 1면의 각주 2번에서는 "2000. 8. 30. 현재 중앙행정기관, 지방자치단체, 정부투자기관 등 전체 4,373개의 공공기관이 모두 452종, 8,421개의 개인정보화일을 보유하고 있고, 그 속에 담긴 개인정보의 전체양은 실로 엄청나다."는 점을 지적하고 있다.

를 2007년도까지 마무리하기로 예정하고 있으나 아직까지 개별과제가 내포하고 있는 기본권침해요소에 대한 파악이 제대로 되지 않은 것이 현실이어서 과연 2007년 말까지 전자정부과제 사업 관계법규정비가 마무리될 수 있을지는 심히 의문이다. 한 예로, 전자정부사업의 하나인 형사사법정보통합시스템구축사업의 경우 2006년 9월이 되어서야 그 사업이 가지는 문제점에 대해 헌법적·형사법적 문제점이 공개적으로 지적[10]된 바 있다. 이는 비록 전자정부사업이 상당 부분 진행되었지만 지금이라도 제도가 가지는 인권침해적 요소를 지적하여 시정하도록 하고 시정이 어려울 경우 그 추진을 중지 또는 계획을 대폭 수정하도록 하는 것이 옳다는 점을 상기시켜 준다.

이러한 상황에서 이 연구는 전자정부사업이 가지는 문제점을 기본권 침해적 요소와 관련하여 지적하고자 한다. 민간에 의한 감시문제도 중요한 것이긴 하지만 이 연구에서는 국가에 의한 국민감시의 문제를 최근 추진중인 전자정부사업을 중심으로 하여 고찰하고자 한다. 전자정부사업의 여러 과제 가운데서도 특히 행정정보공동이용사업과 형사사법정보시스템구축 사업을 중심으로 고찰하고자 한다. 연구의 주제를 이와 같이 좁힌 데는 다음과 같은 이유가 있다.

첫째, 국가에 의한 개인정보침해의 문제가 가장 심각하게 일어날 수 있는 사안이 전자정부사업이라는 점이다. 전자정부사업은 정부의 일하는 방식 혁신·정보서비스 혁신·정보자원관리 혁신을 통하여 투명한 행정·효율적인 행정·참여하는 선진행정을 구현함으로써 참여민주주의를 실현하고, 균형발전사회 구축, 동북아시대 구현, 소득 2만 불 시대 달성을 추구한다는 것이며, 서비스 전달의 혁신을 통한 네트워크 정부, 행정의 효율성·투명성 향상을 통한 지식정부, 진정한 국민주권 실현을 통한 참여정부를 전자정부의 비전으로 제시하고 있어 정부의 모든 행정영역에 걸쳐 근본적인 업무처리방식의 변화를 초래할 수 있는 위력을 가지고 있다는 점이다.

둘째, 그 동안 개인정보보호제도 일반에 관한 연구[11]는 상당 부분 진척

10) 김희수, 「형사사법 통합정보체계 문제점」, 국회의원 최규식 주최 정책토론회 자료집 “온 국민을 감시의 그물망에 묶어 두려는가?”(2006. 9. 26.) 발제문 참조.

이 있었으나 전자정부사업[12] 또는 그 세부과제에 대한 치밀한 법적 연구는 아직 제대로 진행되고 있지 않다는 점이다. 개인정보침해의 위험과 그 구제의 문제는 매우 구체적인 사안을 중심으로 파악되고 구제방안이 제시되어야 하므로 현재 가장 중심이 되는 전자정부사업의 세부과제에 나타나는 문제점을 파악하는 것은 그 구제수단과 대안을 마련하는 데 매우 유용할 것이라는 점이다.

셋째, 전자정부사업에서 추진하는 31개 세부과제를 전부 검토하기에는 시간과 능력이 제한적이라는 점이다. 단기간에 전자정부사업이 내포하는 문제점을 부각시키기 위해서는 제한적인 세부과제 몇 가지를 중심으로 치밀한 분석을 하는 게 가장 경제적이라 생각되므로 이 연구보고서에서는 주로 행정정보공동이용사업과 형사사법정보통합체계구축 사업을 중심으로 연구를 하는 게 바람직할 것이라는 점이다.

이러한 관점을 가지고 제2장에서는 전자정부사업의 개요와 원칙 및 문제점을 살펴보고, 제3장에서는 전자정부사업의 핵심적 요소가 되는 정보의 공유·통합이 가지는 문제점에 대해 분석한다. 이를 바탕으로 제4장에서는 형사사법정보통합시스템구축사업을 집중적으로 분석하며, 아울러 미국에서의 형사사법정보통합작업에 관하여 제도를 소개하고 그 실시과정에서 지적되는 문제점들에 대해 살펴본다. 제5장에서는 이러한 논의를 바탕으로 전자정부사업 추진과정에서 시급히 시정되어야 할 부분과 특히 형사사법정보통합시스템구축사업의 문제점에 대한 구체적 대안을 제시하고자 한다.

2. 연구의 방법

---

11) 대표적인 연구로는 한국법제연구원, 『개인정보보호법제의 정비방안에 관한 연구』, 1997, 이인호, 앞의 연구보고서 등을 들 수 있다.

12) 감사원, 『전자정부 구현사업 추진실태 감사결과』, 2003; 황승흠, 「전자정부의 법과 국가」, 《법과 사회》 제20호, 2001 등.

이 연구는 우리 나라의 전자정부사업 가운데 특히 행정정보공동이용사업 및 형사사법통합정보시스템구축사업에 대한 헌법적·형사법적 문제점을 분석하는 것을 주된 내용으로 하므로 주로 이에 관한 문헌의 분석적 연구를 위주로 하며, 유사한 제도를 이미 실시하고 있는 미국의 몇 개 주에서의 실시 내용과 문제점 등에 관한 문헌을 비교법적으로 분석하여 우리 제도의 고찰에 이용하고자 한다.

제 2 장 정보인권과 전자정부사업

1. 개인정보보호와 정보인권

가. 정보자기결정권을 보장하기 위한 원칙

개인정보보호에 관한 기본원칙의 도출은 정보의 주체인 한 인간이 인격적 가치를 가지는 존재로서 사생활의 비밀과 자유를 가지며, 자기정보에 관한 자기결정권을 가진다는 점에서 출발한다. 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리로서 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리이며, 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보를 그 보호대상으로 한다. 그러나 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다고 해석된다. 그러한 개인정보를 대상으로 한 조사・수집・보관・처리・이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다."[13]

이러한 정보자기결정권을 보장하기 위해서는 다음과 같은 정보수집 및 활용의 적합성, 입력정보의 정확성, 정보처리의 충실성 및 정보관리의 보안성이 확보되어야 한다.[14]

첫째, 정보주체의 동의 없이 정보를 불법적으로 수집하거나, 수집목적이나 취지를 벗어나서 사용되어서는 안된다(적합성, adequacy).

---

13) 헌법재판소 2005.07.21, 2003헌마282 결정; 헌재 2005. 5. 26. 99헌마513 결정 등

14) 조동기, 「정보화사회와 프라이버시」, 한국언론학회·한국사회학회 엮음, 『정보화시대의 미디어와 문화』, 세계사, 1998, 432-436면 참조.

둘째, 수집된 정보가 개인을 정확하게 표현하는 것이어야 한다(정확성, accuracy), 정보사회에서는 인간이 정보를 통하여 전달되고 평가되므로 정보는 한 인간을 정확하게 표창하는 것이어야 한다. 그런 의미에서 시간이 경과하여 이미 낡은 정보는 정확한 정보가 아니다.

셋째, 정보처리가 충실하게 이뤄져야 한다(충실성, integrity). 개개의 정보가 정확하다 해도 그러한 정보의 연결 또는 공유를 통하여 가공된 정보가 정보주체를 정확하게 반영하지 못하는 결과가 발생할 수 있기 때문이다.

넷째, 개인정보가 외부의 침입 또는 내부의 유출 등 위협에 대하여 엄격하게 관리되어야 한다(보안성, security). 수집되어 관리되는 정보는 내부에서의 유출이나 외부의 침입 등에 의해 정당한 정보관리자 이외의 자에게 흘러나갈 가능성이 있으며, 이는 결국 정보의 적합성이 결여된 정보의 유통을 초래하게 되어 정보자기결정권을 침해하는 결과가 되기 때문이다.

나. 개인정보처리의 기본원칙

이러한 정보수집 및 활용의 적합성, 입력정보의 정확성, 정보처리의 충실성 및 정보관리의 보안성을 확보하기 위하여 국제기구와 각국 정부는 다양한 규범을 제정하여 시행하고 있다. 대표적인 예로는 1980년의 OECD 가이드라인(「프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인」[15]), 1980년 유럽평의회의 개인정보보호협약(「개인정보의 자동처리와 관련한 개인의 보호를 위한 유럽이사회 협약」[16]), 1990년 국제연합(UN)의 가이드라인(「컴퓨터화된 개인정보파일의 규율을 위한 가이드라인」[17]), 1995년 유럽연합(EU)의 개인정보보호지침(「개인정보의 처리

15) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

16) Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 18 September 1980

17) Guidelines for the Regulation of Computerized Personal Data Files

및 자유로운 전송에 관한 개인보호 지침」)[18] 등의 국제규범과 각국의 개인정보보호법 및 산업계의 자율규제규범(Code of Practice) 등을 들 수 있다.

OECD 가이드라인(1980년)에서는 국내적 적용의 원칙으로 수집제한의 원칙, 정보정확성의 원칙, 목적구체성의 원칙, 이용제한의 원칙, 안전성확보의 원칙, 공개의 원칙, 개인참여의 원칙, 책임의 원칙 등을 규정하고 있다(제2장). 이 가이드라인의 해당 부분은 다음과 같다.

· 수집제한의 원칙: 개인데이터의 수집에는 제한을 두어야 한다. 어떠한 개인데이터도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다.

· 정보내용정확성의 원칙: 개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다.

· 목적명확화의 원칙: 개인데이터의 수집목적은 늦어도 수집시까지 명확화되어야 한다. 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어야 하고 목적이 변경될 때마다 명확화될 수 있는 것으로 제한되어야 한다.

· 이용제한의 원칙: 개인데이터는 제9조에 의하여 명확화된 목적이외에 목적을 위하여 개시, 이용, 기타 사용에 제공되어서는 안된다. 다만, 다음과 같은 경우에는 그러하지 아니하다.

(a) 데이터주체의 동의가 있는 경우 (b) 법률의 규정에 의한 경우

· 안전확보의 원칙: 개인데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다.

· 공개의 원칙: 개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다.

· 개인참가의 원칙: 개인은 다음 권리를 갖는다. (a) 데이터관리자가 자기에 관한 데이터를 갖고 있는지 여부에 대하여 데이터관리자 또는 기타의

18) 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; 95/46/EC

자로부터 확인을 받을 권리 (b) 개인에 관한 데이터를 다음과 같이 본인에게 통지하도록 하는 권리 (i) 합리적인 기간내에 (ii) 만일 필요하다면 과다하지 않은 비용으로 (iii) 합리적인 방법과 (iv) 알기 쉬운 형태로 (c) 위의 (a) 및 (b)의 요구가 거부당한 경우에는 그 이유를 밝히도록 하고 이와 같은 거부에 대하여 이의를 제기하는 권리 (d) 자기에 관한 데이터에 대하여 이의를 제기하고 그 이의가 인정되지 않을 경우에는 그 데이터를 소각, 수정, 완전화, 보완하게 하는 권리.

· 책임의 원칙: 데이터관리자는 위의 제원칙을 실시하기 위한 조치에 따를 책임이 있다.

한편 Colin Bennett는 다음과 같은 원칙을 제시하고 있다.

개인정보처리기관은 (1) 자신이 보유하고 있는 모든 개인정보에 대해 책임을 져야 한다. (2) 개인정보의 수집시 또는 그 전에 개인정보처리의 목적을 분명히 밝혀야 한다. (3) (특정 상황에서 예외가 있을 수 있지만) 정보주체의 인식과 동의 하에서만 개인정보를 수집하여야 한다. (4) 미리 밝힌 목적에 필요한 한도 내에서만 개인정보를 수집하여야 한다. (5) 정보주체의 동의가 있는 경우를 제외하고, 미리 밝힌 수집목적 이외의 다른 목적으로 개인정보를 이용하거나 제3자에게 제공해서는 안된다. (6) 필요한 기간 동안만 개인정보를 보유하여야 한다. (7) 수집된 개인정보가 정확하고, 완전하며, 최신성을 유지하도록 하여야 한다. (8) 적절한 보안장치에 의해 개인정보의 안전성을 확보하여야 한다. (9) 자신의 정책과 처리관행에 관해 공개해야 하고, 비밀스러운 처리시스템을 운영하는 것은 절대 허용되지 않는다. (10) 정보주체에게는 자신의 정보를 열람하고 또 필요하다면 그것을 수정할 수 있는 기회를 제공해 주어야 한다.[19]

또한 이인호[20]는 12개의 기본원칙을 제시하고 있다. 다음과 같은 내용이다.

---

19) Colin J. Bennett & Rebecca Grant, “Introduction”, in: Visions of Privacy: Policy Choices for the Digital Age (Colin J. Bennett & Rebecca Grant eds., 1999), p. 6. 이인호, 앞의 보고서, 8면에서 재인용.

20) 이인호, 앞의 보고서, 8-12면.

1. 익명거래의 원칙: 정보주체는 정부 또는 기업과 교섭 내지 거래를 할 때 불필요하게 자신의 신원을 밝히지 않고 거래할 수 있어야 한다.

2. 합법성의 원칙: 개인정보처리시스템은 법률의 의사에 따라 합법적으로 구축되어야 한다.

3. 분리처리의 원칙: 특정 목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 통합되지 않고 분리된 상태로 유지되어야 한다.

4. 시스템공개의 원칙: 개인정보처리시스템의 설치 여부, 설치목적, 정보처리방식, 처리정보의 항목, 시스템운영책임자, 처리시스템에 의한 자동결정이 이루어지는지 여부 등이 일반에게 투명하게 공개되어야 한다.

5. 수집제한의 원칙: 개인정보의 수집은 (i) 정당한 수집목적 하에 (ii) 필요한 범위 내에서 (iii) 공정하고 합리적인 방식으로 (iv) 정보주체의 분명한 인식 또는 동의 하에 수집되어야 한다.

6. 목적구속의 원칙: 개인정보를 수집하는 목적은 (i) 수집 당시에 명확히 특정되어 있어야 하고(목적의 특정성), (ii) 그 후의 이용은 이 특정된 수집목적과 일치하여야 한다(목적일치성).

7. 제공제한의 원칙: 수집기관 외부의 제3자에게 개인정보를 제공하는 것은 정보주체의 사전 동의 또는 분명한 인식 하에 이루어져야 한다.

8. 정보정확성의 원칙: 개인정보는 정확성·최신성·적실성을 항상 유지하여야 하며, 처리과정에서 부당하게 변경·훼손되어서는 아니 된다.

9. 참여의 원칙: 정보주체는 자신에 관한 정보의 소재를 확인할 권리를 가지며, 필요한 경우에는 자신에 관한 정보의 내용을 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 열람할 권리를 가진다. 정보주체는 정확성·시의성·적실성을 상실한 자기정보를 수정·보완·삭제를 요구할 권리를 가진다. 이들 권리가 거부되는 경우 효과적인 구제수단을 보장받아야 한다.

10. 보안의 원칙: 개인정보는 적절한 보안장치를 통해 내부자 및 외부자에 의한 불법적인 접근·사용·훼손·변조·공개 등의 위험으로부터 보호되어야 한다.

11. 책임의 원칙: 개인정보의 관리주체를 명확히 설정하고, 관리주체에게는 상술한 원칙들이 지켜지도록 필요한 조치를 취해야 할 책임이 부여되어야 한다.

12. 감독의 원칙: 개인정보처리원칙의 이행 여부를 감시·감독할 수 있는 전문적이고 독립적인 감독체계가 마련되어야 한다.

위에서 언급한 여러 원칙은 내용은 다르게 구성되어 있으나 실제 앞의 정보수집 및 활용의 적합성, 입력정보의 정확성, 정보처리의 충실성 및 정보관리의 보안성이라는 원칙을 달성하기 위한 것임에는 차이가 없다고 생각된다.

이를 재구성해 보면 다음과 같이 정리할 수 있다.

(1) 정보수집 및 활용의 적합성: 익명거래, 수집제한, 합법성, 목적구체성(구속성), 제공제한의 원칙
(2) 입력정보의 정확성: 정보정확성, 개인참여, 열람 및 정정, 최신성 유지 등 원칙,
(3) 정보처리의 충실성: 시스템공개, 분리처리, 비밀처리금지 원칙
(4) 정보관리의 보안성: 안전성 확보(보안), 책임, 감독의 원칙

이러한 정보에 관한 기본원칙은 아래의 전자정부사업에 관한 전반적인 검토에 유용한 기준이 된다고 생각된다.

2. 정부의 전자정부사업 개요

전자정부는 국민을 정부의 고객으로 생각하고 고도화된 정부의 서비스를 제공하기 위한 방편으로 인식되며, 일단 “정보기술을 이용하여 정부의 행정조직, 업무, 시스템을 효율적으로 개혁하여 정부의 행정능률을 최고로 하며 국민에 대한 정부의 각종 정보 및 행정서비스가 언제 어디서나 어떤 방법으로든 국민에게 효과적으로 제공될 수 있도록 하는 정부”[21]라고 정의할 수 있다.

21) 한국전산원, 『전자정부 개념 정립 및 구현 방안에 관한 연구』, 1996, ix면 참조.

영국은 1999년 3월 토니 블레어 수상이 전자정부계획을 발표하였으며, 2006년 6월 미국의 빌 클린턴 대통령은 연방정부와 관련된 모든 정보가 통일된 웹사이트를 통하여 국민에게 전달될 것이라는 전자정부계획안을 발표하여 추진하고 있다.[22] 싱가포르에서는 1999년 전자민원실인 전자시민센터(ecitizen center)가 신설되어 활동하고 있다.[23] 싱가포르의 전자시민센터는 정부의 기관별 구성이 아니라 대국민서비스에 초점을 맞춰 국민생활중심으로 구성되어 있다[24]는 점에서 그 의의가 평가되고 있다.[25] 이러한 전자정부사업은 우리 나라의 경우에도 예외가 아니다. 2003년 8월 정부혁신지방분권위원회는 참여정부의 전자정부로드맵을 작성하였다.[26]

가. 전자정부의 개념

앞에서 잠시 언급하였지만 전자정부법에서는 전자정부를 “정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다”고 정의하고 있다. 달리 살펴보면, 전자정부란 수단 또는 활용양태에 초점을 맞춰 정의할 경우 “대부분의 업무를 컴퓨터, 인터넷, 데이터베이스. 네트워크 등 각종 정보통신기 과 정보통신기기를 사용하여 처리하는 정부” 또는 “전자문서, 전자서명, 전자결재. 원격영상회의. 사이버정부기관. 단일한 종합전자민원실, 디지털화된 지식정보를 기반으로 하여 대부분의 업무가 종이문서와 사람들 사이의 직접적인 접촉 없이 각종 정보통신기기를 매개로 하여

22) 미국의 전자정부사업에 관해서는 한국전산원, 『미국의 전자정부를 향한 도정』, 1997; 임지봉, 『미국의 전자정부법제』, 한국법제연구원, 2001 등 참조.

23) Holmes, Douglas, *eGOv, eBusiness strategies for Government*, London: Nicholas Brealey Publishing, 2001. 24면.

24) 경건, 「전자정부구현을 위한 법제 동향과 과제」, 2000.10.24. 한국법제연구원 워크샵발제문, 50-51면.

25) 전자민주주의의 실현과 관련한 세계각국의 전자정부사업에 관해서는 G7 GOL 운영위원회 지음, 원성묵·김장묵 옮김, 『세계의 전자정부와 전자민주주의』, 커뮤니케이션북스, 1999.

26) 「전자정부로드맵」은 정부혁신지방분권위원회 인터넷사이트(http://www.innovation.go.kr)에서 검색(2006. 12. 24.)

처리되고 하루 24시간 중단 없이 가동되는 정부"라 정의할 수도 있다.[27]

그러나 이러한 개념정의에는 단순히 행정정보처리의 수단이나 양태만이 나타나 있을 뿐 국민주권주의에 바탕을 둔 '정부'로서의 성격은 잘 나타나지 않는다. 정보통신기술과 기기가 '누구에 의해서', '누구를 위해서' 그리고 '무엇을 위해' 정비되고 사용되는지에 대한 근본적인 고려가 담겨 있지 않다는 점이다. 물론 전자정부사업의 구체적인 내용에서 행정의 효율성을 추구하면서 아울러 행정의 민주성도 강화하려 하고 있는 점에서 보면 분명 전자정부사업에 국민주권주의의 관점이 담겨 있음은 부인할 수 없으나, 일차적으로 전자정부의 개념정의에도 이러한 고려가 담기지 않으면 안된다는 점이다.

전자정부사업을 추진하는 입장에서는 이것이 당연히 국민의 이익을 위한 것이라고 주장하지만, 자칫 국가 또는 자본가계급, 기득권층처럼 사회 내 특정집단의 이익을 증진하는 것으로 전락할 가능성도 존재한다. 엄청난 예산을 들여 추진하는 사업이고 그 개발 및 운영은 '외주의 원칙'(전자정부법 제14조)을 취하고 있으므로 사업주체인 기업의 이익을 위하여 구상되고 추진되다가 국민에게 별 이익을 주지 못한 채 흐지부지 표류할 가능성도 존재한다는 것이다. 제1차적 이익이 정부 내부에 근무하는 사람 내지는 상층조직과 조직상층부에 있는 사람들에게 귀속되어 국가 내지 정부 자체의 내부적 업무처리의 효율성을 증진시킬 뿐 국민에게는 별 이익을 주지 못하는 경우도 있을 수 있다. 또한 국가 내지 정부의 입장에서 투명성이 제고된 정부, 즉 정부가 국민들에 관한 정보를 잘 파악하거나 국민들의 생활을 잘 감시할 수 있는 정부를 만들거나 정부 내에서의 투명성 역시 상부기관 이나 상급자가 하부기관 또는 하급자에 관한 정보를 잘 파악할 수 있게 되는 정도에 그치는 경우도 있을 수 있다. 이러한 경우는 모두 정보기술과 기기를 이용한 전자정부이면서도 정부구성의 헌법적 기초인 국민주권주의에 전혀 부합하지 못하는 결과를 낳고 만다.

---

27) 경건, 「전자정부구현을 위한 법제 동향과 과제」, 한국법제연구원 워크샵 발제문(2000. 10.24.), 52-53면. 장용근, 『전자민주주의의 헌법적 연구』, 서울대학교 법학박사학위논문, 2004, 229면에서 재인용.

결국 전자정부는 국민주권주의의 이념을 충실하게 반영하는 것이어야 한다. 기존의 행정업무처리방식이나 내용과는 다른 일처리방식을 통하여 행정의 효율성과 민주성을 달성하는 것이어야 한다. 일반시민의 입장에서 투명성이 제고된 정부, 즉 정부가 지니고 있는 보다 많은 정보들이 보다 편리하게 일반시민에게 공개되고 정부 내 업무처리과정이 사전적·사후적으로 시민들에게 투명한 상황에 있는 정부를 만드는 것이어야 하며, 나아가 정부에 대한 국민의 지배력 또는 통제력의 강화. 사회내 불평등의 해소, 국민의 기본권 증진 그리고 국민의 정치적 의사가 보다 국정의사결정과정에 반영될 수 있는 정부를 만드는 것이어야 한다.[28)]

이러한 관점에서 전자정부는 “정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부”이면서도 그것이 국민의 이익을 지향하고 국민의 정부에 대한 통제와 참여를 보다 강화하고 국민의 기본적 인권의 신장에 기여하는 정부를 말한다고 정의할 수 있다.[29)]

나. 외국의 전자정부사업

(1) 미국

1993년 미국 국가성과평가위원회(NPR)의 부속보고서인 ‘정보기술을 통한 리엔지니어링’에는 전자정부는 전자은행서비스(Electronic Banking)에서 대두된 개념을 확장한 것으로서 ATM과 플라스틱카드, 전국적 네트워크가 은행업무를 편리하게 해주었듯이 전자정부도 정부와 국민간의 의사소통을 신속, 용이하게 할 것이며 전자은행서비스에서와 마찬가지로 프라이버시 및 보안문제가 중요하게 다루어져야 한다고 서술되어 있다. 이처럼 미국에서 전자정부의 개념은 전자은행서비스개념에서 출발하여 이후 정부가 정부의 고객인 국민들에게 보다 편리한 정부서비스를 제공해야 한

28) 장용근, 앞의 글, 230면도 같은 취지.

29) 김성태, 『전자정부론 -이론과 전략-』, 법문사, 2004, 14면 이하에서는 전자정부의 개념을 기술결정론적 관점, 사회결정론적 관점, 경제발전의 수단적 관점 등에서 다양하게 정의하고 있다.

다는 차원에서 전자정부의 개념으로 발전한 것으로 보인다. 미국의 전자정부는 1993년 클린턴 행정부 시절, 정보기술을 활용한 전자정부의 구현을 통해 기존의 사람과 종이문서 위주의 업무처리방식 대신 정보기술을 업무보조 및 대체수단으로 적극 활용하여 정부 내부적으로는 업무의 효율성을 높이고, 국민의 입장에서는 정부의 의사결정에서부터 그 집행에 이르기까지 보다 용이하게 참여할 수 있게 함으로써 정부의 모습 자체를 근본적으로 바꾸고자 하였다. 그러나, 초창기 전자정부는 업무의 효율성 향상을 주된 목적으로 공공부문의 정보자원관리 차원에서 관리예산처(OMB)와 각 연방정부간의 자율과 통제의 틀을 마련하는 데 초점을 맞추었기 때문에 그 동안 정보자원관리 관련 다양한 법제가 정비되고 정보화책임관협의회 등 기본적인 추진체계가 갖춰져 있었음에도 불구하고 전자정부의 성과에 대한 정확한 측정이나 평가는 물론 기관간 중복투자의 문제도 해결하지 못하는 불합리한 결과가 발생하였다. 심지어 2000년 6월에 개통된 정부 포털 사이트 ‘firstgov.gov’ 조차도 연방기관간 상호연계 및 운용성 미흡으로 별다른 성과를 거두지는 못하는 상태가 지속되었다.

특히 2001년 출범한 부시 행정부는 'A Blueprint for New Beginnings' 제하의 2002년도 예산안을 통해 '능동적인 작은 정부(active and limited government)'를 구현하기 위한 국민중심의 정부, 결과중심의 정부, 시장중심의 정부를 표방하는 전자정부를 보다 적극적으로 추진하겠다는 의지를 표명하기에 이르렀다. 2001년의 부시 대통령의 정부개혁안(President's Management Agenda)의 하나로 본격적인 전자정부가 추진되었는데, 국민의 정부서비스에 대한 접근, 정부기관과의 상호교류의 편의성 강화, 정부의 능률성과 효과성의 강화, 정부의 대국민 대응능력 개선 등의 목표를 제시하였다. 그리고 2002년에는 전자정부를 지향한 포괄적 입법으로 전자정부법이 제정되었다. 이 법은 연방정부가 인터넷을 비롯한 정보기술을 최대한 활용하여 정부의 효율성을 높이고, 전자정보를 보호하며, 행정서비스를 요구하거나 받을 때 국민에 대한 편리성 제공을 주목적으로 하고 있다. 또한 이 법은 동시에 정보공유와 보안, 프라이버

시 보호를 추구하고 있다.[30]

이와 관련 2001년 8월 발표된 보고서에서는 고객지향적인 전자정부의 구현을 연방차원에서 지속적으로 추진하기 위해서는 관리예산처(OMB)가 정보기술투자를 기획의 관점에서 보다 효율적으로 운영할 필요가 있으며 이를 위해 대통령실에 특별전담반을 설치할 것이라고 발표하였다.

이처럼 부시 행정부는 클린턴 행정부에서 시작된 전자정부를 보다 적극적으로 추진하겠다는 의지를 분명히 하였고, 이는 전자정부법의 제정, 관리예산처 내에 전자정부의 전담기관인 전자정부국의 설치, 정보화책임관 협의회의 역할강화, 전자정부기금의 설치 등을 통해 가시화되었다.

지난 2002년 2월에는 대통령의 전자정부 구현의지가 담긴 5대 정부개혁안을 구체화하기 위하여 범정부차원의 전자정부사업과 구현전략을 제시함으로써 전자정부 추진에 대한 확고한 의지를 다시금 표명하게 된다.[31]

전자정부 관련 법제[32]로는 1974년 프라이버시법에서 그 법적 토대가 되는 맹아가 발견된다고 하며, 정부문서감축법(Government Paperwork Elimination Act, 1980, 1986, 1995, 1998 등), 1993년 정부업무수행결과법(Government Performance Results Act, Public Law 103-62), 1996년 정보기술관리개혁법, 1996년 전자정보자유법, 2000년 연방전자서명법 등이 있다.

---

30) 미국의 전자정부법의 입법배경 및 주요내용에 관하여는 권태웅, 「미국의 전자정부법제와 추진전략」, 《법제》 통권 제554호, 법제처, 2004. 24면 이하 참조.

31) 한국전산원, 「미국 전자정부법 분석 및 시사점」, 2003. 7. 9. (「미국의 전자정부구현동향」, KAIST 테크노경영대학원의 자료실 검색자료에서 재인용)

32) 제사한 내용은 임지봉, 『미국의 전자정부법제』, 한국법제연구원, 2001을 참조.

영역	개요	사업 (Administration's 24 E-Gov Initiatives)
개인에 대한 서비스 (G2C : Service to individuals)	국민이 용이하게 정부서비스를 이용할 수 있도록 one-stop-shops를 구성	- Recreation One-stop - Eligibility Assistance Online - Online Access for Loans - USA Services - EZ Tax Filing
기업에 대한 서비스 (G2B : Service to businesses)	인터넷을 활용한 통합적 보고로 기업의 부담 최소화	- Online Rule making Management - Expanding Electronic Tax Products for Business - Federal Asset Sales - International Trade Process Streamling - One-Stop Business Compliance Information - Consolidated Health Informatics
정부간 관계 (G2G : Intergovernmental affairs)	연방정부에 대한 지방정부의 보고의무 간소화 및 연방정부 지원 산업에 대한 정확한 성과측정	- Geospatial Information One-stop - e-Grant - Disaster Assistance and Crisis Response - Wireless Public SAFECOM - e-Vital
내부적 효율성과 효과성 (IEE: Internal efficiency and effectiveness)	모범사례의 활용으로 연방정부의 행정성과 제고 및 비용 절감	- e-Training - Recruitment One-stop - Enterprise HR Integrations - e-payroll - e-Travel - Integrated Acquisition Environment - Electronic Records Management
정보화 기반		- e-Authentication

(2) 싱가포르

싱가포르 정부는 2000년 6월, Infocomm 21의 일환으로 디지털 경제에 더 나은 서비스 제공을 위한 전자정부 실현이란 비전을 제시한 15억 싱가포르 달러 규모의 전자정부추진 3개년 계획을 발표. 이어 이를 실천하기 위한 전자정부 전략 프레임워크가 마련하였다. 이 프레임워크는 정부대국민(G2C), 정부대기업(G2B), 정부대공무원(G2E)의 세 그룹에 초점을 둔 것이다. 또한 정부기관들이 G2C, G2B관련 전자정부 프로젝트를 수립하거나

제공할 때 반드시 대상 그룹의 수요 충족을 최우선 과제로 두어 국민 및 기업 대상 대민서비스에 대한 지속적 재고와 업무방식의 리엔지니어링, 서비스 제공에 있어서 부처간 협력을 요구하였다.

정부대국민(G2C)의 대표적 프로젝트는 'e-Citizen Centre'이며 1998년에 시범적으로 도입되어 1999년 공식 개통된 이 서비스는 단일 창구를 통한 종합적인 행정 서비스 제공 및 보편적인 서비스 확보에 목표를 두고 있다. 이 서비스는 모든 정부기관들에서 얻어진 통합된 정보와 서비스를 제공하는 원스톱 논스톱 사이버센터로 540여 가지의 전자정부 서비스가 기업, 고용, 가족, 건강, 주택, 교통, 여행 등 14개의 삶의 여정에 따라 분류되어 일반 국민이 찾기 쉽게 구성되어 있다고 평가된다.

정부대기업(G2B) 대표적 프로젝트인 GeBiz(www.gebiz.gov.sg)는 정부 및 기업간 입찰 및 조달의 전 과정을 전자적으로 수행할 수 있도록 하는 웹기반 end-to-end 조달 시스템이다. 2000년 12월에 개통된 이 시스템은 국내 기업에게는 정부와 전자적으로 거래할 수 있는 기회를 제공하면서 해외 기업들에게도 싱가포르 정부의 조달 기회에 쉽게 접근할 수 있도록 하고, 정부에게는 조달의 모든 활동을 온라인으로 추진할 수 있는 기회를 제공하고 있다. 이 시스템이 개통된 이래로, GeBiz를 통해 수행된 전자거래 규모는 8,000만 달러 이상에 이르고 있다 한다. 또 2001년 12월에 개통한 eBizCore 서비스는 기업들이 사업등록을 하기 위해 직접 해당 관청을 방문하지 않더라도 전자적으로 처리가 가능하도록 하고 있다.

정부대공무원(G2E) 프로젝트는 공무원의 ICT 활용능력 강화에 초점을 두고 있으며, 이에 따라 모든 공무원에게 전자정부에서 창출될 수 있는 여러 기회들을 개발하고 활용할 수 있는 능력을 제고시키기 위해 필요한 기술을 교육하는 Infocomm Education(IE) 프로그램을 실시하고 있다. 또한 2001년 2월부터 공공부문 CIO간에 정보와 경험을 공유할 수 있는 장을 마련해 주는 'Distinguished CIO Speaker Series'프로그램을 시작했고, 2001년 7월, 공공부문의 지식관리를 촉진시키기 위한 500만 싱가포르 달러 규모의 지식관리시범프로그램(Knowledge Management Experimentation

Programme)에 착수하여 지금까지 7개 기관이 이 프로그램에 참여하고 있다.

그 뿐만 아니라 전 정부부처를 연계시킴으로써 정부서비스 및 국민과의 커뮤니케이션을 활성화시키기 위해 정부이메일시스템, 공공부문 스마트카드, 범정부 인트라넷 등을 구축하는 노력들이 추진되어, 현재 3만1,000명이 사용하고 있는 정부이메일시스템에서 한 달에 1,200만여 건의 정부내부 이메일이 처리되고 있고, 연간 500만 건의 정부 및 국민간 이메일 교환이 이루어지고 있다. 한편, 향후에는 공무원을 대상으로 한 G2E 포털을 구축할 예정이며, G2E 포털은 정부 인트라넷의 한계를 벗어나 광범위한 정부자원의 범정부적 공유와 서비스에 더욱 쉬운 접근을 제공함으로써 공무원간 연계를 강화시키는 효과를 얻을 수 있을 것으로 기대되고 있다. 이와 함께 정부가 인력자원관리정책을 빠르고 효과적으로 추진할 수 있도록 People Matter Management System(PM2S)를 구축 중인데, 이 시스템은 각 부처별 특정 인력수요에도 대응하면서 정부 전분야의 운영 효율성을 개선시킴으로써 규모의 경제를 달성하는 데 목표를 두고 있다.

이처럼 싱가포르 정부는 국가정보화 전략의 맥락에서 정부의 생산성과 효율성을 제고하여 대국민 서비스를 향상시키기 위해 공공부문의 정보화 추진에 주력한 결과 컨설팅 기업 액센츄어(Accenture)가 전 세계 국가들의 전자정부 성숙도를 조사한 보고서에서 2001년과 2002년 연속 캐나다에 이어 세계 2위를 기록하는 등 현재 싱가포르는 전자적 행정서비스 제공에 있어서 세계 최고의 선도적인 국가로 평가받고 있다고 한다.[33]

다. 정부의 전자정부사업의 내용[34]

2003년 8월 정부혁신지방분권위원회가 작성한 참여정부의 전자정부로드맵에 의하면, 이 사업은 정부의 일하는 방식 혁신·정보서비스 혁신·정보

33) 「외국의 정보화」, 『국가정보화백서 2002』, 2002. 6

34) 구체적 내용은 앞의 「전자정부 로드맵」 참조.

자원관리 혁신을 통하여 투명한 행정·효율적인 행정·참여하는 선진행정을 구현함으로써 참여민주주의를 실현하고, 균형발전사회구축, 동북아시대 구현, 소득 2만불 시대 달성을 추구한다는 것이며, 서비스 전달의 혁신을 통한 네트워크 정부, 행정의 효율성·투명성 향상을 통한 지식정부, 진정한 국민주권 실현을 통한 참여정부를 전자정부의 비전으로 제시하고 있다.

구체적으로 대부분의 민원 및 기업관련 업무를 관청방문 없이 처리할 수 있게 함으로써 행정서비스 수준을 획기적으로 제고하고 기원지원경쟁력도 10위권으로 제고하고(대민서비스), 모든 행정업무의 전자화 및 정보공유를 확대하고 정보자원을 통합 관리하여 실시간행정이 가능하게 함으로써 효율성을 극대화하며(행정효율성), 행정정보의 능동적·개방적 제공(정부투명성)으로 정책참여를 활성화하고 개인정보에 대한 자기통제권을 강화하여 행정의 민주성 제고한다(행정민주성)는 것 등을 내용으로 하고 있다.

대민서비스제고를 위해 단일창구를 통한 기업지원서비스 제공, 분야별 통합서비스(물류, 조세, 외국기업 등), 전자정부 해외진출지원이 추진되며, 인터넷 민원서비스, 국가안전관리종합서비스, 건축·토지·등기 연계화, 종합국세서비스, 국가복지종합정보서비스, 식·의약품종합정보서비스, 고용·취업종합정보서비스, 행정심판인터넷서비스 등이 추진된다. 행정효율성 향상을 위해서는 기관공통 업무처리는 전면적 전자화 및 연계하고, 문서대장은 종이를 없애고(종이 없는 행정구현) 전자대장으로 일원화하며, 부처간 행정정보는 전면적 공유화하고, 정보자원관리는 통합 및 연계된다. 정보자원의 통합·표준화를 통하여 범정부 통합전산환경을 구축하고 전자정부 통신망을 고도화한다고 한다. 행정민주성을 제고하기 위하여 국민의 전자적 참여를 여론조사 수준에서 정책참여 및 협의 수준(전자주민투표제, 전자투표 시범실시 및 확대 구상)으로 격상시키며, 행정정보를 능동적·개방적으로 제공하고 프라이버시 침해에 대비하여 개인정보통제권을 강화하려 하고 있다. 정책정보 공유를 확대함으로써 국정과제 실시간관리시스템을 구축하고 범정부지식관리시스템(KMS)을 구축·연계하여 KMS를 통한 범정

부 정책정보공유를 의무화하는 것을 추구하고 있다. 행정정보 공유도 확대되어 2005년까지 모든 공공기관이 공유하고 2006-7년까지는 모든 금융기관도 이를 공유하는 것을 목표로 설정하고 있다. 전자정부구현 및 안전성 관련 법제정비를 위해서 2005년까지 공공개인정보보호 제도 및 체계를 개선하고 2007년까지는 관계법규 정비를 완료하겠다고 한다. 이를 위하여 제정·시행되고 있는 전자정부구현을위한행정업무등의전자화촉진에관한법률(일부개정 2006. 10. 4. 법률 제8031호)이 제정되어 시행되고 있다.

구체적인 과제로는 위원회핵심관리과제 13건과 위원회중점관리과제 18건으로 전체 31개의 과제를 갖고 있다. 위원회 핵심관리과제는 다음과 같다.

1. 문서처리 전과정 전자화
2. 전자지방정부 구현
3. 행정정보 공유 확대
4. 정부기능연계모델(BRM) 개발
5. 인터넷 민원서비스 고도화
6. 기업지원 단일창구서비스
7. 온라인 국민참여 확대
8. 범정부 통합전산환경 구축
9. 전자정부통신망 고도화
10. 범정부 정보기술 아키텍처(ITA) 적용
11. 정보보호체계 구축
12. 정보화 인력 및 운영조직 강화·정비
13. 전자정부 구현 및 안전성 관련 법제정비

한편 위원회 중점관리과제는 다음과 같다.

1. 국가 및 지방재정 종합정보화
2. 전자감사체계 구축
3. 전자국회 구현

4. 통합형사사법체계구축
5. 인사행정종합정보화
6. 외교통상정보화
7. 국정과제 실시간 관리
8. 국가안전관리종합서비스
9. 건축·토지·등기 연계 및 고도화
10. 종합 국세서비스고도화
11. 국가복지종합정보서비스
12. 식·의약품 종합정보서비스
13. 고용·취업 종합정보서비스
14. 행정심판인터넷서비스
15. 국가물류종합정보서비스
16. 전자무역서비스
17. 외국인종합정보서비스
18. 전자정부 해외진출지원

이러한 전자정부사업은 앞에서 제시한 바와 같이 행정의 투명성과 효율성을 높이고 국민의 행정에 대한 접근·참여와 이용가능성을 향상시키기 때문에 국민주권을 실현하는 데도 긍정적으로 평가된다.

3. 전자정부의 구현 및 운영원칙

전자정부법 제2장에서는 전자정부의 구현 및 운영의 원칙을 다음과 같이 규정하고 있다.

가. 국민편익중심의 원칙(제6조)

“행정기관의 업무처리과정은 당해 업무를 처리하는데 있어서 민원인이 부담하여야 하는 시간과 노력이 최소화되도록 설계되어야 한다.” 전자정부의 목표 가운데 하나가 업무처리의 전자화를 통하여 국민의 이익을 증

가시킨다는 것이며, 이 점을 명문화하고 있다.

나. 업무혁신 선행의 원칙(제7조)

“행정기관은 업무를 전자화하고자 하는 경우에는 미리 당해 업무 및 이와 관련된 업무의 처리과정 전반을 전자적 처리에 적합하도록 혁신하여야 한다.” 전자정부를 만드는 것이 단순히 업무의 전자화만이 아니라 이를 통하여 행정의 효율성을 달성하고자 하는 취지가 반영되어 있다.

다. 전자적 처리의 원칙(제8조)

“행정기관의 주요 업무는 전자화되어야 하며, 전자적 처리가 가능한 업무는 특별한 사유가 있는 경우를 제외하고는 전자적으로 처리되어야 한다.” 행정의 효율성을 증가시키면서 특히 종이 없는 행정을 구현하기 위하여 특별한 사유가 있는 경우를 제외하고는 전자적으로 문서를 작성하고 업무처리를 하도록 한 것이다. 그러나 법제가 이를 따르지 못할 경우, 가령, 형사사법절차에서는 전자문서가 아직 문서로서 효력을 인정받지 못하는 경우가 많아서 전면적인 실시에는 어려움이 존재할 뿐 아니라 자칫 많은 예산을 투여하여 구축한 시스템이 무용지물이 될 가능성도 존재한다.

라. 행정정보공개의 원칙(제9조)

“행정기관이 보유·관리하는 행정정보로서 국민생활에 이익이 되는 행정정보는 법령의 규정에 의하여 공개가 제한되는 경우를 제외하고는 인터넷을 통하여 적극적으로 공개되어야 한다.” 행정기관 스스로 정보를 적극 공개하도록 하고 있어 정보공개를 위한 별도의 노력을 상당 부분 절감시켜 줌으로써 행정에 대한 접근을 강화하고 민주적 통제를 가능하게 한다. 그러나 국가기관간 정보공유를 원칙으로 하므로 수집 목적 외에 정보가

과도하게 공유될 가능성이 존재하며, 정보에 접근할 수 있는 이용자가 증가함에 따라 공개에 따르는 위험도 그만큼 가중된다고 할 수 있다.

마. 행정기관 확인의 원칙(제10조)

“행정기관은 특별한 사유가 있는 경우를 제외하고는 행정기관간에 전자적으로 확인할 수 있는 사항을 민원인에게 확인하여 제출하도록 요구하여서는 아니된다.” 행정정보의 공유와 통합에 따라 별도의 증명을 위한 서류발급 등 노력을 절감하고자 한 것이다. 그러나 이는 한편으로 국민의 편의를 증진시키지만 이러한 확인을 위하여 정보의 공유를 확대하고 정당화의 근거로 삼을 여지를 열어주는 것이기도 하다.

바. 행정정보공동이용의 원칙(제11조)

“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.” 행정기관이 가지고 있는 정보는 원칙적으로 다른 행정기관과 공유하도록 함으로써 정보를 중복수집하는 데 소요되는 비용과 시간을 절감하여 행정의 효율성을 높이고자 하는 것이다. 그러나 이러한 효과는 일차적이며, 행정기관간 정보의 공유를 통하여 새로운 정보를 쉽게 수집하는 결과가 될 뿐 아니라 정보를 교차하여 점검함으로써 정부기관이 보다 정확한 정보를 보유할 수 있게 된다. 이러한 공동이용의 원칙은 같은 법 제21조에서 구체화되고 있다.

그러나 "행정기관"이라 함은 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관 및 국무총리 소속기관을 포함한다) 및 그 소속기관, 지방자치단체를 말한다(전자정부법 제2조 제2호)고 하므로, 자칫 정보의 공유를 통하여 헌법상 국가기

관구성의 원리인 권력분립원리를 위반할 가능성도 배제하지 못한다. 권력분립의 원리는 국가기관의 분리와 분립이기도 하지만 실질적으로는 정보의 분리를 통하여 보장되는 것이라고 생각되기 때문이다.

사. 개인정보보호의 원칙(제12조)

“행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다.” 앞의 행정정보공동이용의 원칙과 짝을 이뤄 정보의 공동이용에도 불구하고 개인정보가 침해되지 않도록 하는 취지를 선언하고 있으나 같은 법에 이 원칙을 선언하는 규정이 없는 데 반하여 제21조에서는 공동이용의 의무까지 설정한 것을 보면 결국은 공동이용의 원칙에 비중이 실린 것으로 볼 수 있다.[35]

아. 소프트웨어 중복개발방지의 원칙(제13조)

“행정기관은 소프트웨어를 개발하는 경우에는 중복개발이 되지 아니하도록 필요한 조치를 하여야 한다.” 전자정부 추진을 위하여 동 사업 내부에서도 중복되는 업무를 간소화한다는 취지가 반영된 것이다. 즉, 전자정부의 소프트웨어는 중복개발되어 예산을 낭비하거나 행정업무의 비효율을 초래해서는 안된다.

자. 기술개발 및 운영 외주(外注)의 원칙(제14조)

“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 한

35) 이인호, 앞의 보고서, 14면 참조.

다.”

전자정부시스템 구축에 필요한 기술을 정부 스스로 개발하고 운영하는 것은 비용의 지출 측면에서도 비효율적이라고 할 수 있다. 경제적 측면에서 기업에 외주를 주는 것이 타당하다는 판단에 기초한 것이라 생각된다.

그러나 정부기관의 정보가 공유되고 나아가 통합되는 현실에서 정부기관의 구성원이 아닌 자가 기술개발을 넘어서 운영까지 담당하는 것은 보안성에 취약요소가 될 수 있다고 생각된다. 컴퓨터 프로그램상의 보안성은 기술적으로 확보할 수 있다지만 결국 시스템 전체의 보안성을 확보하는 것은 그것을 담당하는 사람이 가지는 윤리에 의존하기 때문에 과연 공유·통합된 정보의 관리를 정부기관의 구성원이 아닌 자에게 맡길 수 있는지 의문이 생기지 않을 수 없다. 비록 그 운영기술자를 관리하는 책임자가 공무원이라 할 수 있지만 기술적 능력에 차이가 있을 경우 적절한 관리에 어려움이 없을 수 없다. 결구 최종적인 감시자를 어떻게 감시할 것인가가 과제로 떠오른다.[36]

4. 전자정부사업의 일반적인 문제점

가. 전자정부사업에서 고려하여야 하는 개인정보보호의 기본원칙

전자정부 구현 및 운영의 원칙으로 전자정부법은 앞에서 살펴본 바와 같이 국민편익중심의 원칙, 업무혁신 선행의 원칙, 전자적 처리의 원칙, 행정정보공개의 원칙, 행정기관 확인의 원칙, 행정정보공동이용의 원칙, 개인정보보호의 원칙, 소프트웨어 중복개발방지의 원칙, 기술개발 및 운영 외주의 원칙을 제시하고 있다. 그러나 국민의 편익증진, 업무혁신, 행정정보공동이용을 내세워 개인정보를 침해할 가능성이 높다고 생각된다.

36) 현재에도 개인정보보호법에 의하면 개인정보를 열람하는 데 제한이 있으나 경찰에 아는 사람이 있을 경우 그리 어렵지 않게 특정인에 관한 정보를 상당 부분 알 수 있는 것을 생각하면, 법제도의 실효성도 상당 부분 의문이 제기될 수 있다.

앞에서 설명한 대로, 정보수집 및 활용의 적합성, 입력정보의 정확성, 정보처리의 충실성, 정보관리의 보안성 등의 관점에서 검토되어야 한다.

(1) 정보수집 및 활용의 적합성의 문제

전자정부사업을 추진한다 해도 개인정보보호에 소홀해서는 안되므로, 앞에서 언급한 바와 같이 정보수집의 목적이 구체적이어야 하고 정보활용도 수집목적에 구속되며, 수집기관 외부의 제3자에게 개인정보를 제공하는 것은 정보주체의 사전동의가 있거나 분명한 인식하에 이뤄져야 한다. 물론 정보주체가 동의하지 않더라도 법적 근거가 명확하다면 정보의 수집과 제공이 가능하다. 그러나 법률에 의하여 수집하는 경우에도 수집제한의 원칙에 따라 그 법적 근거, 수집의 이유, 수집정보의 활용, 정확성·보안성 확보장치 등에 대해 설명하여야 한다.[37] 법률에 의한 정보제공의 경우에도 수집목적구속성의 원칙에 비추어 수집된 정보는 수집한 기관에서 관리하여야 하고 다른 기관에 제공하는 것은 무한정 가능한 것이 아니고 제공의 목적이 정당하고, 필요한 최소한의 범위에 한하여 제공되어야 하며, 제공방식이 합리적이고 정보의 정확성과 보안성을 확보할 수 있는 것이어야 한다. 제공된 정보는 제공의 목적에 한정되어 활용되어야 한다.

이러한 관점에서 전자정부법의 내용을 보자. 제9조에서는 행정정보공개의 원칙을 규정하고 있다. 즉 “행정기관이 보유·관리하는 행정정보로서 국민생활에 이익이 되는 행정정보는 법령의 규정에 의하여 공개가 제한되는 경우를 제외하고는 인터넷을 통하여 적극적으로 공개되어야 한다.”(제8조) 그러나 “국민생활에 이익이 되는 행정정보”가 무엇인지를 명확히 판단하기란 어렵다. 역설적으로 개인정보보호법이 정보비공개 사유를 넓게 정하고 있다는 것 때문에 오히려 전자정부법에 의하여 정보공개로 인한 개인정보의 침해가능성이 낮아진다고 해야 할까? 제12조에서는 개인정보보호의 원칙으로 “행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다.”

37) 이인호, 앞의 보고서, 10면.

고 규정하고 있으나, 이는 선언적인 것에 불과하고 당사자의 의사에 반하는 것이라도 공동이용의 대상이 되는 정보면 공동이용에 지장이 없다.

제11조에서는 행정정보공동이용의 원칙을 규정하고 있다. 이 조항은 뒤에 제21조 및 제22조에 정보공동이용에 관한 내용을 상세하게 규정하고 있는 것으로 보아 전자정부사업에서 매우 중요시되는 부분이라고 판단할 수 있다. 실제 전자정부사업이 정보의 공유·통합에 의한 정보의 정확성 확보 및 행정의 효율성 제고를 추구하는 것이고 보면 행정정보공동이용의 비중을 짐작할 수 있다.

전자정부법에 의하면 민원사항의 처리를 위하여 필요한 행정정보, 통계정보·문헌정보 등 행정업무의 수행에 참고가 되는 행정정보, 공공기관의 개인정보보호에관한법률 제10조제2항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보와 정보화촉진기본법 제8조의 규정에 의한 정보화추진위원회가 행정기관간 공동이용이 필요하다고 인정하는 행정정보는 공동이용하여야 한다.(제21조 제1항) 그러나 국가의 안전보장과 관련된 행정정보와 비밀 또는 이에 준하는 행정정보는 이를 공동이용의 대상이 되는 정보에서 제외할 수 있다(같은 조 제2항). 이 조문을 보면 개인정보침해의 가능성을 쉽게 판단할 수 없다. 그러나 이 조항에서 언급하는 개인정보보호법 제10조 제2항을 보면 “1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, 2. 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우, 3. 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, 4. 통계작성 및 학술연구등의 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 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, 6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우, 7. 법원의 재판업무수행을 위하여 필요한 경우, 8. 기타 대통령령이 정하는 특별한 사유가 있는 경우”에 보유기관의 장은 당해 개인정보화일의 보유

목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있으며, 다만, 다음 각호의 1에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다고 하고 있어, “소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우(제1호)”. “범죄의 수사와 공소의 제기 및 유지에 필요한 경우(제6호)”, “법원의 재판업무수행을 위하여 필요한 경우(제7호)” 등은 남용의 가능성이 있은 부분이다. 소관업무를 수행하기 위하여 당해정보를 이용할 상당한 이유가 있는지 여부, 범죄의 수사와 공소의 제기 및 유지에 필요한 정보인지 여부는 정보를 공동이용하고자 하는 기관이 적당한 이유를 제시하여 요구하면 전자정부법상 공동이용의 원칙과 의무에 비추어 보아 매우 긍정적인 방향으로 결론 날 가능성이 높다고 생각된다. 더구나 범죄의 수사를 위해 필요한 경우까지 행정정보공동이용을 관철할 경우는 검찰이나 경찰에 의하여 제한없이 정보가 사용될 가능성도 배제하지 못한다.

이런 점에서 보면 행정정보공동이용의 원칙과 이에 대한 의무규정은 행정기관이 수집한 정보의 수집목적을 벗어난 사용을 금지하고 있는 제12조와 저촉되고 공동이용을 원하는 정부기관의 의도에 따라 수집제한 또는 수집제한의 원칙에 반할 여지가 많다고 생각된다.

(2) 입력정보의 정확성의 문제

전자정부법에는 입력정보의 정확성을 확보하기 위하여 정보공동이용시 국회규칙이나 대통령령이 정하는 방법으로 송신하여야 하며, 행정정보의 제공기관은 행정정보의 정확성을 유지하여야 한다는 규정을 두고 있다(제21조 제3항, 제4항).

그러나 전자적 방법에 의한 정보의 입력은 항상 입력오류의 위험을 안고 있으며, 문제는 그 정도를 얼마나 낮추느냐에 있다고 할 수 있다. 2003년 현재 정보입력의 오류로 인하여 43,300건의 미상전과(누적수치)가 발생하였다(연간 평균 2,000건).[38] 1996년에 발생한 고교 생활기록부

전산화자료의 입력오류사건도 대표적이다. 당시 교육부가 입시사정자료용으로 각 대학에 제공한 고교 3학년생 생활기록부 전산화 자료에 수험생의 내신석차, 주민등록번호, 재적학생수 등 일부 내용이 잘못 입력된 것으로 밝혀졌는데, 이러한 오류가 발견된 학교는 전체 1,889개 고교 중 0.4%인 70여개 학교에 달하였다. 이는 수기작업이든 전자적 작업이든 정도의 차이일 뿐이지 전자적 방법이라도 정보입력의 오류를 완전히 발생하지 않도록 하기란 어렵다고 생각된다. 다만, 정보의 공동이용을 통하여 각 기관이 가진 정보를 교차적으로 점검함으로써 정보의 정확성을 확보할 가능성은 높아진다고 할 수 있다.

(3) 정보처리의 충실성 - 정보의 공유·통합의 문제

정보처리의 충실성을 위해서는 시스템공개, 분리처리, 비밀처리금지 원칙 등이 언급된다.

우선 정보를 처리하는 시스템 자체의 존재나 저리방식 및 처리내용 등을 비밀로 하는 것은 수집한 정보가 수집목적 외의 다른 용도로 사용되고 가공되는지를 전혀 알거나 통제할 수 없게 한다는 점에서 시스템의 존재와 처리내용과 방식 등은 공개되어야 한다.

또한 시스템의 처리방식 등이 공개되는 한편으로 시스템에 의해 처리되는 정보는 당초의 수집목적에 구속되어 분리처리되어야 한다.[39] 왜냐하면 다른 정보와 교차대조하거나 다양한 정보를 바탕으로 정보를 가공·생산하는 것은 수집목적과 다른 새로운 정보의 수집과 전혀 다르기 않기 때문이다. 과거 상당한 노력을 기울이지 않으면 얻을 수 없었던 여러 정보를 전자적 방법으로 클릭 한 번에 한 자리에 집합시키고 이를 바탕으로 새로운 고급정보를 취득하는 것은 정보주체의 총체적인 모습을 매우 손쉽게 드러내 줄 수 있기 때문이다. 정보기관의 용어로 말하자면 '첩보(intelligence)'가 손쉽게 '정보(information)'으로 변하게 되는 것이다. 또

38) 형사사법통합정보체계추진단, 『형사사법 통합정보체계 구축사업 - 추진경과 및 사업내용』, 2006. 9. 26., 3면 참조.

39) 이인호, 앞의 보고서, 9면.

한 파편적인 정보의 부정확성의 피해보다 점차 총체적이고 잘 가공되어 저오학성이 있다고 하는 정보의 오류로 인한 피해가 그 규모가 매우 크기 때문이다. 결국 총체적인 인격의 전무를 드러내는 정보의 경우 그 정보 자체에 의해 한 인간의 인격이 평가되고 타인과 교류하게 되므로 근본적인 인격권의 문제상황을 야기시킬 위험이 있다는 점에서 전자정부법의 행정기관간 정보공동이용의 원칙에도 불구하고 각 행정기관이 수집한 정보는 분리처리의 원칙을 바탕으로 하여야 한다고 생각된다.

그러나 분리처리의 원칙을 바탕으로 행정기관간 행정정보의 공동이용의 원칙을 정하고, 더 나아가서는 공동이용의 의무를 부과하는 것은 단순한 정보공동이용을 넘어서서 자신이 가지고 있는 정보와 연계시키게 됨으로써 정도가 문제겠지만 필연적으로 정보의 결합 및 새로운 정보의 가공·생산을 초래할 위험이 존재한다. 특히 정보공동이용이 남용될 위험이 있으면 있을수록 업무상 불필요한 정보를 집적하여 새로운 정보를 가공할 가능성이 증가한다고 할 수 있다.

미국에서 복지혜택을 사기적 방법으로 받는 자들을 색출하기 위하여 전자적 방법으로 처리된 복지수혜자명부와 임금소득자명부를 대조하는 것[40]이나, 우리 나라의 경우에 세금정산용 서류를 허위로 제출한 경우를 색출하기 위하여 병원·약국, 금융회사·신용카드회사 등의 정보망과 연계하는 것은 정보공유를 통하여 예산의 절감과 행정의 효율성을 높이는 예로서 평가된다. 엄청난 인력을 동원해야만 가능했던 일이 단기간 안에 끝날 수 있고 부당한 지출을 막을 수 있어 예산을 절감하게 된다.

그러나 이러한 긍정적인 부분만 나타나는 것은 아니다. 아무리 개인정보보호의 원칙을 내세운다고 해도 본래 수집한 행정기관 외의 기관이 행정정보를 공유한다는 것은, 그것의 처리가 전자적 방법으로 쉽게 되므로 파편적인 정보가 개인의 사생활의 전체 모습 또는 상당부분의 모습을 보여주게 되어 사생활의 비밀과 자유를 침해할 가능성을 높이게 된다. 특정한 목적을 위해 수집된 정보가 정보주체의 통제를 받을 기회를 상실한 채

40) 이에 관해서는 변재옥, 「입법소개: 1988년 컴퓨터연결 및 프라이버시보호법」, 《미국헌법연구》 재1권, 1990, 5면 이하 참조.

유통되는 것은 개인정보자기결정권에 상당한 위협이 된다. 또한 정보라는 게 단 하나의 내용만 가진 것이 아니라 여러 가지 내용과 사람이 관련되어 있는 복합적 존재라는 점에서 정보의 공동이용은 그것이 아무리 합법적인 것이라고 하더라도 필연적으로 사생활의 비밀과 자유를 침해할 가능성을 수반하는 것이다. 예를 들어, 사건의 수사를 위한 과거 기록을 공동이용하는 경우 그 사건의 피의자뿐 아니라 피해자, 증인 및 참고인 등 사건에 관련되는 수많은 사람들의 정보도 함께 다른 기관이 이용하게 되는 것이다. 전체의 내용을 알 수 있어야 필요한 정보를 끌어낼 수 있는 것이므로 피의자에 한정해서 정보를 제공하는 것도 어려움이 있음을 생각하면 정보공유가 가지는 문제점을 쉽게 알 수 있다. 전자정부법시행령에서도 이러한 침해가능성을 엿볼 수 있다. 시행령 제22조(행정정보의 제공 요청)에서는 행정기관의 장은 필요한 최소한의 범위에 한정하여(제2항) 그 소관업무를 수행함에 있어서 다른 행정기관이 보유·관리하는 행정정보를 이용할 필요가 있는 경우에는 그 보유기관에 대하여 이용목적을 밝혀 당해 행정정보의 제공을 요청할 수 있다(제1항)고 규정하고 있으나, 제23조(행정정보의 제공)에서는 이를 제공하는 행정기관의 심사의 여지를 매우 좁게 하고 있다. 즉 “제22조의 규정에 의하여 행정정보의 제공요청을 받은 행정기관의 장은 정당한 사유가 없는 한 당해 행정정보를 제공하여야 한다.”(제1항)고 하여, 정당한 사유가 없이는 정보제공을 거부하지 못하게 하고 있어 정보이용의 주도적 권한은 제공을 요청하는 쪽에 있음을 알 수 있다. 물론 행정정보를 제공하는 경우에 행정정보의 이용·관리 등에 필요한 조건을 붙일 수 있으며 필요한 관계자료의 제출을 요구할 수 있고(시행령 제23조 제2항), 제24조에서는 이용목적 외의 목적으로 이용하는 행위, 수정·가공 등 변형시키는 행위, 제공받은 행정정보 또는 그 변형된 행정정보를 스스로 구축한 행정정보인 것처럼 취급하는 행위 및 다른 기관에 다시 제공하는 행위 등 제공된 정보의 이용제한을 규정하고 있으나 그 위반에 대한 제재는 규정되어 있지 않다.

행정기관간 정보공동이용도 일정한 목적과 범위에만 제한된다고 하면

그러한 정보의 공유·통합은 한정적일 수 있다. 그러나 그 부분에서 나타나는 위험은 과소평가되어서는 안된다. 또한 공동이용을 중개하는 네트워크나 정보기기의 안전성도 고려되어야 한다.[41] 개인 식별자의 정확성이 확보되지 않으면 잘못된 정보의 공동이용과 집적으로 피해가 발생할 수 있다. 미국에서는 컴퓨터연결의 결과 많은 복지사기를 색출하였지만 한편으로 매사추세츠주에서는 무고한 복지수혜자들이 사기행위를 한 것으로 처리되어 법원에서 자신들의 무죄를 다투는 일이 발생하기도 하였다. 우리나라에서도 외교통상부의 여권발급전산망과 연결된 경찰청의 신원조회전산망이 세밀하지 못한 정보를 제공하여 범죄자와 이름이나 생년월일만 같아도 부적격자로 판정되어 2만여 명이 여권발급을 받지 못한 경우가 있고, 또 주민등록번호의 잘못된 처리로 인하여 범죄피의자로 오인되어 수차에 걸쳐 경찰에 연행되어 조사를 받은 사례도 소개된다.[42] 물론 정보의 통합과 공유가 반드시 한 개인에 관한 정보의 오류나 왜곡을 초래한다고 단언할 수는 없다.[43] 그러나 그러한 위험이 존재한다는 사실이 간과되어서는 안될 것이다.

따라서 행정정보공동이용의 원칙에도 불구하고 개인정보보호의 원칙은 더욱 중요하게 인식되어야 하며, 각 행정기관이 수집한 목적에 충실하게 분리처리됨을 원칙으로 하여야 할 것이다. 또한 시스템 자체가 안정성을 확보할 수 있어야 한다.

(4) 정보관리의 보안성의 문제

---

41) 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(제14조).

42) 서유창, 「개인정보보호법 제정배경과 시행성과」, 《수사연구》 1996년 4월호, 17면.

43) Paul F. Kendall et al., Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use, 21st Annual International Conference on Data Protection and Information Privacy, Hong Kong 7-8 (Sept. 1999) (http://www.pco.org.hk/english/infocentre/files/kendall(formatted).doc)(2006. 12. 24. 검색)

정보가 수집행정기관을 넘어서서 이용되는 경우 정보관리에서의 안전성 확보(보안), 책임, 감독의 원칙은 더욱 절실하게 요구된다. 기술적으로는 다양한 방법을 통하여 보안성을 확보할 수 있다고 하지만, 문제는 이러한 시스템 자체의 작동을 관리하는 담당자를 어떻게 감독하느냐이다. 처리기관 내부의 불법적은 유출이나 외부에서의 침투에 의하여 정보가 누출될 가능성은 상존한다. 아무리 고도의 기술이 동원된다 해도 직접 담당하는 사람의 도덕적 윤리적 타락에 대처할 방법은 마땅하지 않다. 법원을 통한 소송절차는 이미 발생한 엄청난 피해를 구제하는 데 적합하지 않다. 그런 점에서 컴퓨터 관리자의 윤리의식은 어쩌면 법제도보다도 더 중요한 과제라고 할 수 있을 것이다. 또한 앞에서도 지적하였지만 기술개발과 운영을 "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"고 하고 있으므로 특히 외주업체에 대한 보안확보에 특히 주의하지 않으면 엄청난 정보의 유출로 인한 피해가 발생할 수 있을 것이다.

5. 소결

전자정부사업은 행정의 투명성·효율성·민주성을 높임으로써 국민의 삶의 질을 향상시키는 것을 목표로 제시하고 있다. 정보수집 및 활용의 적합성, 입력정보의 정확성, 정보처리의 충실성과 정보관리의 보안성에서 일정한 문제를 나타내고 있다. 완벽한 시스템의 구축을 달성하기란 어려움이 있겠지만, 일단 국민의 삶의 질을 향상시키는 것을 목표로 추진되는 사업이라면 그 평가기준은 기본적 인권의 보장이 되어야 하고 특히 정보인권이 잣대로 제시되어야 할 것이다. 앞에서 언급한 것과 같이 이 사업은 그 동안 정보인권을 보호하기 위하여 제시된 개인정보처리의 기본원칙

에 비추어 여러 측면에서 문제점을 갖고 있음을 알 수 있다. 당초 예정한 2003-2007년까지의 사업기간의 막바지에 다다라 있지만 아작 사업이 종료되지 않았고 사업내용을 보다 충실하게 할 수 있는 가능성이 충분히 있으므로 앞에서 언급한 문제점이 시정될 수 있는 방향으로 개선하여야 할 것이다.

제 3 장 개인정보의 공유·통합의 법적 문제점

전자정부사업은 행정기관간 정보의 공동이용을 통하여 행정효율성을 높이려 한다. 결국 정보의 공유와 나아가서는 통합을 수반하는 것이다. 이 장에서는 전자정부사업의 핵심이라 할 수 있는 정보의 공유와 통합이 가지는 문제점에 대해 살펴보고자 한다.

1. 개인정보의 공유·통합의 경향

정보사회에서는 정보기술의 발전과 보다 정교한 정보 확보의 필요성에 따라 정보를 통합 또는 공유하게 된다. 정부기관 사이에서만 공유하는 것은 아니다. 금융기관들이 대출 등 신용정보를 공유하는 것은 대표적이다. 이를 뒷받침하는 것은 금융정보망의 구축과 금융기관의 현실적인 필요성이다. 학교의 학생과 교원에 관한 정보(NEIS)도 마찬가지이다. 학생 또는 교원이 근무하는 학교 단위가 아니라 전국의 학교를 하나의 거대한 시스템으로 결속하고 정보를 공유한다면 전학이나 전근 및 상급학교 진학관계 등 학교간에 이뤄지는 많은 일처리가 매우 용이해 질 것이다. 조세부과를 담당하는 국세청으로서도 연말세금정산과 관련하여 각종의 조세관련 사항을 통합한다면 세금의 탈루를 막는 데 매우 중요한 역할을 할 것이다. 각 기관이 개별적으로 수집하여 보유하는 정보를 다른 기관이 공유하고 서로 가진 정보를 상호이용할 수 있도록 한다면 정보의 신뢰성을 높이고 다른 정보를 통하여 새로운 정보로 가공이 가능해진다는 점에서 정보의 공유와 통합은 정보사회의 기술발전에 따라 나타날 수 있는 중요한 현상이라 할 것이다.[44] 특히 2001년에 발생한 9·11 테러사건 이후 대테러작전 또는

44) 실업급여 중복 또는 불법수혜자의 색출이나 실업대책의 효율성을 ㄴ옾일 수 있을 것이다. 이에 관해서는 “정부가 지난해부터 추진해 온 실업대책과 관련, 감사원이 지난해 11월부터 두 달간 공공근로자, 실업급여자, 직업훈련생 등의 명단을 전산대조한 결과 6천여 명이 부정 또는 중복 수혜자인 것으로 밝혀졌다. ”(중앙일보 1999. 3. 24.자) “노동부 관계자는 5일 『구직등록, 실업

공공의 안전 확보라는 명분하에 정보의 통합과 공유라는 흐름을 강하게 뒷받침하고 있는 것으로 보인다.

그러나 문제는 이러한 정보의 공유·통합에 의하여 국가기능을 수행하고 공공의 안전을 확보하는 데는 긍정적일 수 있으나 이와 함께 또 다른 위험이 가중된다는 점이다. 각 신용카드 회사가 가지고 있는 거래 내역, 통신회사가 가지는 통화기록, 위치정보기록, 금융회사가 가지는 신용정보, 경찰과 검찰이 가지는 범죄기록, 교통위반기록, 행정기관이 가지는 인적사항 및 재산보유기록, 의료보험회사가 가지는 의료기록 등을 통합하면 이들이 단편적으로 각각 존재할 때와는 다른 새로운 정보의 확보가 가능해질 수 있다는 것이다. 통합됨으로써 얻는 정보는 기존 정보의 연장선에서가 아니라 전혀 새로운 내용이 될 수 있다. 단순한 첩보(intelligence)가 다양한 정보와 분석을 통하여 정보(information)로 가공되는 것과 같은 이치이다. 과거 '전지적 작가시점(全知的 作家視點)'에서만 가능하던 한 인간의 삶의 총체적인 모습을 이제는 통합정보를 장악한 자가 빅브라더(Big Brother)로서 관리할 수 있게 된다는 점이다. 한 인간의 컴퓨터에 의해 관리되는 정보수집장치에 접하는 모든 것을 종합할 경우 삶의 총체의 상당부분이 노출될 수 있다. 유선 또는 무선 전화통화, 신용카드 사용, CCTV 촬영, 인터넷접속 등으로 통하여 개별적으로 수집되는 정보가 공유 또는 통합된다면 한 인간의 삶의 모습은 상당 부분이 그대로 드러나게 된다. 개별적인 정보만으로는 판단하기 곤란하거나 다양한 가능성이 추정될 수 있으나 다른 정보와 크로스체크되면서 매우 정교하게 가공될 수 있게 된 것이다.

1970년대 초반에 미국에서는 컴퓨터의 연결을 통하여 한 인간의 삶의 내용과 양태를 어느 정보 알 수 있는지를 말해주는 예[45] 가 소개된 적이

급여, 실업자 대부 등 3대 데이터베이스에 이어 최근 직업훈련과 공공근로 데이터베이스의 전산입력 작업을 완료, 이들 5대 데이터베이스의 연계운영이 곧 가능해진다』고 말했다. 실업관련 5대 데이터베이스의 통합전산망이 가동되면 직업훈련을 받으면서 공공근로사업에 참여하는 등의 부정 및 이중 수혜가 즉각 확인돼 실업대책의 효율성이 높아질 것으로 기대된다."(조선일보 1999. 5. 5.자)는 내용의 신문기사 참조.

45) 양창수, 「정보화사회와 프라이버시의 보호」, 《인권과 정의》, 대한변호사협회, 1991. 3., 72

있다. 은행정보, 지출정보, 전화통화내역 등 조합하여 놀랄 정도의 내용을 알 수 있다는 것이다.

"저축 있다(90% 확실).
전분성분이 지나치게 많은 아침식사. 아마도 비만.
휘발유 3갤런 주유. 차는 폴크스바겐. 금주만으로도 12갤런 구입. 직장까지의 9마일을 차로 가는 이외에 무엇인가 하고 있음이 분명하다.
아침 7시 57분에 휘발유 주유. 회사에 지각하였을 것이다.
전화 328-1826[그가 전화한 번호. 이하 같다.]는 셔디 레인의 것. 셔디는 1962년에 도박죄로 체포된 일이 있다.
전화 308-7928 고급남성이용실. 머리가 벗어진 사람 또는 최신 유행 전문.
전화 421-1931 라스베가스행 예약(처는 동반하지 않음). 금년 3번째의 라스베가스에의 여행(처 동반 없음). 같은 시기에 라스베가스에 누군가 다른 사람과 갔는지 파일을 조사하고 그 사람의 전화번호와 대조하기로 한다.
현금 120달러 인출. 모든 합법적 물건구입은 전국사회보험크레디트카드로 할 수 있는데, 이는 이상한 일이다. . . . .
점심 도중 술을 마셨다.
극히 비싼 여자용 내의를 샀다. 그의 처의 사이즈가 아니다.
전화 369-2436 미스 스위트 로크스. 비싼 버본酒를 샀다. 최근 30일 사이에 버본주를 5병이나 샀다. 꽤나 술을 좋아하든가, 상당히 즐거운 일이 있든가 둘 중의 하나이다. . . . .
2시간 30분 동안의 행적은 불명."

그러나 과거보다 컴퓨터기술이 발전하고 수집된 정보가 매우 많으며 정보통합이 가설적인 것이 아니라 실제 많이 이뤄지고 있는 지금은 이 정도를 훨씬 넘어서고 있다. 신용카드 사용이 보편화되고, 거래의 대부분에 전자지문을 남기고 있다. 현금으로 거래를 하더라도 세금혜택으로 유혹하는 현금영수증의 발급으로 전자지문을 남기게 된다. 국민의 상당수가 가입한 휴대전화의 사용은 더욱 심각한 문제를 수반한다. 요금부과 및 분쟁에 대비하여 전화통화내역과 문자 수·발신 내용을 보유하는 것은 기본이

면 각주 7에는 컴퓨터의 연결에 의하여 한 인간의 생활내용 및 양태에 대해 어느 정도 알 수 있는지를 보여주는 외국의 예가 소개되고 있다.(Malcolm Warner & Michael Stone, The Data Bank Society : Organizations, Computers and Social Freedom (1970))

고 나아가 이동중 전화연결을 위해서 휴대폰의 소재지역을 계속 확인하게 된다. 가입자의 핸드폰이 어느 지역에 있는지, 어디로 이동하는지를 추적하는 것은 이동통신서비스제공의 기본이기 때문이다. 현재 이동통신 가입자의 위치추적서비스까지 제공하고 있다. 이러한 현실에서 한 인간의 삶의 모습은 개별적인 정보의 공유와 통합으로 인하여 더욱 적나라하게 드러날 위험에 처하게 된다. 단지 그 모습을 있는 그대로 받아들이는 것을 넘어서서 그 사람을 분석하고 원하는 목적을 달성하기 위한 방안을 마련하는 기초자료가 된다면 이러한 정보는 인간의 통제와 조종에 악용될 소지를 넓게 열어놓고 있다는 점에서 사생활의 비밀과 자유뿐 아니라 삶의 자기결정권의 문제를 근본적으로 박탈할 소지를 크게 하고 있다고 생각된다. 특히 정치적 의사결정에 관련하여 특정한 정파에게 이러한 정보가 장악될 경우 자유로운 의사의 표현과 토론을 통하여 공동체의 의사가 결정되는 정치적 형식인 민주주의에도 심각한 위협이 될 것이다.

기술의 발전과 정책의 변화로 인하여 개별적으로 또는 단편적으로 존재하는 정보가 통합되고, 전지적 작가시점처럼 한 인간의 일거수일투족까지도 알 수 있게 된다면 그 사람은 삶의 주체가 아니라 다른 사람에 의하여 조종되고 통제될 가능성이 높아지게 된다는 점에서 인간의 삶의 독립성과 주체성을 바탕으로 한 민주주의의 원칙에 근본적으로 모순되는 현실이 초래될 수 있는 것이다.

2. 우리나라에서의 개인정보의 공유·통합의 문제사례

전자정부사업 이전에도 정보의 통합과 공유를 추진한 사례는 적지 않다. 전자정부사업이 범정부적 차원에서 추진되는 것이라면 전자주민카드사업[46]이나 교육행정정보시스템(NEIS)와 같이 국지적 차원에서 정보의 통합과 공유를 위한 사업도 찾을 수 있다.

---

46) 김승환, 「전자주민카드제도의 위헌성」, 《민주법학》 제13호, 1997, 245면 이하.

가. 교육행정정보시스템(NEIS)

국가인권위원회는 2003. 5. 12. 교육인적자원부의 교육행정정보시스템(NEIS)에 관한 개선 권고에서 교육인적자원부가 추진하는 교육행정정보시스템(NEIS)의 운영에 대하여 교육인적자원부장관에게 교육행정정보시스템의 27개 개발영역 가운데, 사생활의 비밀침해 등 인권침해 소지가 있는 교무/학사, 입(진)학 및 보건 영역은 입력 대상에서 제외하고, 교원인사기록 중 별지목록 기재 항목은 사생활의 비밀침해 등 인권침해의 소지가 있으므로 입력항목에서 제외되도록 '교육공무원인사기록및인사사무처리규칙'을 개정하고, 개인정보의 누출로 인한 사생활 비밀침해 등 인권침해가 없도록 학교종합정보시스템(CS)에 대한 보안체계 강화 조치를 강구할 것을 교육인적자원부에 권고하였다.

1997년 이전까지 학교현장에서는 학교생활기록부, 학생건강기록부 등 교육을 목적으로 학생들로부터 수집된 정보를 수기로 기록해 오다가, 1997년 수기 작성한 학교생활기록부, 학생건강기록부 기록 결과를 컴퓨터에 입력하도록 하는 SA(Stand Alone) 시스템을 도입·보급하기 시작하여 전자문서화의 첫 발을 내딛었다. 교무업무를 지원하는 CS(Client Sever)도 1997년 보급하기 시작했는데, CS는 업무처리를 자동화 하여 SA에 비해 효율을 높이고 보급 학교 내 컴퓨터를 LAN으로 연결하여 학교 내 서버에 정보를 집적 관리하도록 설계되었다. CS는 초·중등교육법 제25조, 학교보건법 제7조, 학교신체검사규칙 제9조, 교육기본법 제23조 등 규정에 근거하여 추진되어, 초등학교·중등학교·고등학교생활기록부전산처리지침(교육인적자원부 훈령 제587호)학생건강기록부전산처리및관리지침(훈령584호)에 근거하고 있으며 초·중등학교종합정보관리시스템운영규정(훈령588)에 의거 운영되었다.

NEIS는 모든 교육행정기관 및 초·중·고등학교를 인터넷으로 연결하여 단위학교 내 행정정보는 물론 전 교육행정기관에서 처리해야하는 업무를 인

사, 예산, 회계, 교무/학사, 보건 등 27개영역[47]으로 나누어 전자적으로 연계 처리하기 위한 시스템이다. 각 시·도 교육청(전국 16개 시·도 교육청)에 데이터베이스 서버를 두고 시·도 교육청은 시스템에 대한 행정적·재정적 지원을, 교육인적자원부장관과 시·도 교육감은 시스템의 유지·관리를 하되 직접 입력정보에 접근할 수는 없고, 권한을 인증받은 각급 학교의 담당교사가 필요한 개인정보 등을 입력하고 관리하는 교육행정정보시스템으로서 교육

47) 27개 항목은 아래와 같다.

단위업무	세 부 내 용
기획	주요업무,기관평가
공보	보도자료 관리
법무	법률정보, 판례정보, 법령질의해석
감사	감사계획 및 결과, 감사현황 분석, 감사자료 공유, 사이버 감사
재산등록	재산등록 대상 및 내역관리, 재산신고
교육통계	학교현황, 학생현황, 교원현황, 시설현황, 주요업무통계 등
입(진)학	초등학교 취학, 중학교 입학, 고등학교 입학 등
장학	교육과정, 연구학교, 장학정보, 학생행사관리, 연구대회 등
교무/학사	학교교육과정, 학적, 성적, 학생생활기록부, 학생생활, 교과용도서
검정고시	원서접수, 성적처리, 고사장 관리, 합격처리 및 각종 통계산출
평생교육	평생교육 시설 및 교육프로그램 관리, 학원 및 교습소 관리
보건	학교보건실 관리, 학교환경관리, 건강기록부 및 보건 통계
체육	학교체육시설관리, 운동부 및 선수관리, 각종현황 및 통계관리
교원인사	정·현원, 임용시험, 인사기록, 임용발령, 호봉, 전보, 평정, 승진, 연수, 상훈 및 징계, 복무, 기간제교사, 전문직 임용, 자격검정관리
일반직 인사	정·현원, 임용시험, 인사기록, 임용발령, 호봉, 평정, 승진, 연수, 상훈 및 징계, 복무
급여	월급여, 연봉제, 명절휴가비, 연가보상비, 성과상여금, 연말정산, 기여금, 건강보험, 국민연금, 고용보험
민원	제증명, 유기한 민원, 진정/건의/질의, 정보공개, 현황통계 등
비상계획	민방위 편성, 민방위 해제, 민방위 교육훈련, 공익근무요원 편성, 공익근무요원 관리
법인	법인정보, 예·결산, 법인 대장
시설	시설사업관리, 학교시설승인, 학교시설사용승인, 시설유지관리, 시설현황, 수용계획
재산	공유재산관리계획, 재산대장관리, 사용허가/대부관리, 폐교재산활용관리
물품/교구/기자재	취득/운용관리, 재물조사, 수급계획, 교구기준안 관리, 교구현황관리, 실험 실습재료관리, 기자재 기준안관리, 기자재 현황관리, 기자재 통계
예산	예산편성, 예산배정, 예산이월, 예산운용, 예산통계
회계	세입, 세출, 세입세출외 현금, 계약/압류, 결산, 자금
학교회계	예산, 세입, 세출, 결산, 세입·세출외 현금, 세무관리, 발전기금
급식	학교급식통계, 급식관리, 급식외 관리, 급식분석
시스템	코드관리, 시스템연계, 보안, 사용자 인증 및 권한관리, 로그관리, 인터페이스관리, 배치작업관리, 업무처리승인관리

행정의 생산성·투명성을 획기적으로 확보하고, 교원 업무의 획기적 경감시키며 학부모에게 인터넷 서비스 제공하는 한편 졸업증명서·경력증명서 등 일반국민에 대한 민원서비스 제공하고 이전에 사용되던 학교종합정보시스템(CS)의 보안 문제를 해소하고자 도입된 것이다.

이러한 CS 또는 NEIS는 과거 수작업의 단점을 시정하는 장점을 나타내지만 컴퓨터에 의해 연결되고 개인식별자를 통하여 정보의 통합까지 쉽게 가능하게 한다는 점에서 인권위원회의 결정이 내려진 것이다.

나. 전자주민카드사업

전자주민카드는 주민등록증, 인감증명, 지문정보, 건강정보 등 각종 신분증의 내용을 한 장의 전자카드에 담아 행정업무의 효율성을 증진시키고 새로운 편의를 제공하여 국민복지카드로서의 기능을 수행하는 한편, 전자카드의 보안성을 바탕으로 국민의 사생활 보호를 꾀한다[48]는 목적으로 추진되던 1995년부터 추진되던 사업이다. 그러나 이 사업에 대해서는 국민의 사생활의 비밀과 자유를 심각하게 침해할 가능성이 있다는 이유로 반대캠페인이 전개[49]되었으며 김대중 정부가 들어서면서 중단되었으나 현재 도입을 위한 움직임이 있다고 한다.

전자주민카드에 수록된 정보는 이미 각 기관별로 수집되어 보관되던 정보로서 새롭게 수집되는 정보는 특별히 없을 수 있다. 그러나 중요한 것은 정보가 당초 수집된 목적을 넘어 다른 기관과 공유되며 활용될 가능성을 높임으로써 정보관리의 보안성에 위험을 가중시키며, 특히 기존에 단편적인 정보로만 존재하던 개인이 이제는 정보를 공유하는 기관에 의하여 매우 상세한 정보에 의하여 뚜렷하게 사적 정보가 파악될 가능성이 커진다는 점이다. 즉 정보주체의 개인정보자기결정권이 침해된다는 것이다. 이를 통하여 개인의 사생활이 관리자에게 드러나며 결국 국민이 정보관리

48) 한국전산원, 『전자주민카드사업의 타당성 분석』, 1996, 43면 이하.

49) 반대론의 대표적인 문헌으로는 김승환, 「전자주민카드의 위헌성」, 《민주법학》 제13호, 1997; 김기중, 「전자주민카드와 전자감시사회」, 정보법학회 1997. 3. 17 발표문 참조.

자에 의하여 지배 또는 통제당할 위험이 크다는 점에서 문제가 있다.

이러한 사업추진과정에서 드러나는 문제의 하나는 이러한 사업에 관한 헌법적 차원의 검토가 결여되어 있다는 점이다. 위헌적 사업을 추진하는 것은 사업추진에 소요된 예산을 낭비하고 새로운 사업추진을 위하여 많은 시간과 인력까지 필요로 하게 된다는 점이다. 결국 이러한 사업을 추진함으로써 이득을 얻는 것은 사업에 필요한 프로그램의 개발을 담당하는 기업체이며, 대형프로젝트를 발주하여 사업을 추진하는 일부 관료들이 아닐까?

3. 외국에서의 정보의 공유·통합 - 미국의 컴퓨터 연결과 관련된 논의

컴퓨터연결(computer matching)이란 정보의 유사점 또는 상이점을 찾아내기 위하여 둘 이상의 데이터베이스를 사로 연결하는 컴퓨터의 이용을 말한다. 컴퓨터 연결은 여러 기관이 보유하는 기록의 비교함으로써 자료의 범위와 내용이 풍부해지고 그 결과 자료의 정확성과 신뢰성을 높일 수 있다는 장점이 제시된다. 미국에서는 컴퓨터 연결과 관련하여 여러 장점이 지적되었다. 첫째, 과거 복지사기의 결과 매년 수백만 달러가 낭비되었기 때문에 복지사업에 있어서 사기행위를 추방하는 것이 복지행정에 대한 국민의 신뢰를 유지하기 위해 필요하다는 것이다. 둘째, 기존의 한정된 수의 파일을 무작위로 추출하여 상호대조하는 방법은 시간낭비 철저하지 못한 단점이 있다. 과거 인력부족과 기술부족으로 인한 한계를 극복하여 업무수행의 효율성이 비약적으로 증대된다는 점이다.

그러나 이러한 컴퓨터 연결에 대해서는 비판이 강력하게 제기되었다.[50] 주된 비판의 근거로는 다음과 같다. 첫째, 사람들이 두려워하는 인적 자

50) 변재옥, 「입법소개: 1988년의 컴퓨터연결 및 프라이버시보호법」, 《미국헌법연구》 제1호, 1990, 7면.

료에 대한 일종의 조작이다. 둘째, 새로이 형성되려는 아직은 희미한 정보프라이버시의 법적 개념의 연약한 기초를 파괴할 가능성이 있다. 셋째, 사람은 자료의 부품으로 취급되어서는 안된다. 넷째, 분리된 소규모의 자료은행에서 그때그때 필요에 의한 연결도 집적되면 개인의 프라이버시에 대한 위협은 다를 바 없다. 다섯째, 분리된 자료은행에서 발견되는 개인의 기록을 연결시키기 위하여 확인번호(identifying number)를 이용하는 것은 컴퓨터기술의 남용이다. 여섯째, 복지혜택을 받기위한 사기를 폭로하기 위하여 연결사업을 추진하는 것은 의미 있지만, 특정한 목적을 위하여 개인으로부터 수집된 정보가 그 정보의 유통을 통제할 기회도 없이 다른 목적을 위하여 다른 의미로 사용되는 것이다. 자기정보통제권을 인정하면 동의없이 개인에 관한 자료를 유통시키는 일은 프라이버시권의 침해라고 보아야 한다. 일곱째, 어떤 특질을 가진 자를 색출하기 위하여 수백만 명에 관한 컴퓨터 파일을 검사하는 컴퓨터 연결작업은 자동 인적자료처리에 관한 가장 위험한 사용방법이다. 여덟째, 정보의 연결을 통하여 새로운 정보체계를 만들어 낸다. 현재의 컴퓨터기술은 기존의 기록시스템의 경계를 허물 수 있는 잠재력을 가지고 있다. 결국 어느 기록시스템에 입력된 개인정보를 다른 기록시스템이 이용할 수 있고 나아가 거대한 통합자료연결망이 형성된다는 등이다.

이러한 논란의 결과 1974년에 제정된 프라이버시보호법(The Computer Matching and Privacy Protection Act of 1988)에 예외규정을 두었다. 연방법전 Title 5 Sec. 552a(Records maintained on individuals) 정의(a)에 의하면, 컴퓨터연결이란 연방복지프로그램에 의한 현금지급 또는 현물지원의 신청자·수급인의 자격을 확인·결정할 목적으로 또는 연방복지프로그램에 의한 지급 또는 채무불이행의 공제를 목적으로 둘 이상의 자동기록시스템(automated systems of records) 또는 기록시스템과 비연방기록 사이의 컴퓨터에 의한 대조(comparison)를 의미하거나 또는 둘 이상의 자동화된 연방직원·급여명부의 기록시스템 또는 하나의 연방직원·급여명부 기록과 비연방기록과의 컴퓨터에 의한 대조를 의미

한다고 한다.

그러나 몇 가지 사항은 컴퓨터 연결로 보지 않는다고 하여 예외를 인정하고 있다. 컴퓨터연결의 제외사유로 명시된 것은 1) 인적 식별자(personal identifiers)가 없는 집합적 통계자료를 만들기 위한 연결 2) 특정한 개인의 권리·수혜·특권에 관한 결정에 사용되지 않는 특정 자료, 연구·통계사업을 지원하기 위한 연결 3) 형사법집행에 관한 활동을 주된 기능으로 하는 행정기관에 의한, 특정인에 대한 증거수집을 목적으로 하는 연결 4) 1986년 내국세법전 제6103조(d)에 의한 조세행정을 목적으로 하는 조세정보의 연결 5) 연결목적이 연방직원에 대한 재정·인사·징계 기타 불리한 조치에 사용되지 아니하는 경우에 있어서, 일상행정목적으로 실시되는 주로 연방인사에 관계되는 기록을 사용하는 연결 또는 행정기관의 기록만을 사용하는 행정기관에 의하여 실시되는 연결 6) 대외방첩을 위하여 또는 연방직원 또는 연방계약직원의 보안검사를 위한 배후조사를 위하여 실시되는 연결 7) 1986년 내국세법 제6103(k)(8)에 의한 징수를 위한 연결 7) 사회보장법(Social Security Act) 제202(x)(3)조 또는 제1611(e)(1)조에 따른 연결 등이다.[51]

이러한 컴퓨터연결과 관련되는 사례를 들 수 있다. 우선 Jaffess v. Secretary, Dep't of Health, Educ. & Welfare 사건이다.[52] 원고 Jaffess는 보훈국(The Veterans Administration)으로부터 연금을 받았고 다른 사회보장제도에 의해서도 보조금을 받았다. 그런데 퇴역군인에게 지급되는 연금은 사회보장법 등에 의하여 지급되는 다른 국가기관들로부터 받는 보조금에 따라 상이하게 결정되도록 규정되어 있었다.[53] 이 법에 따르면 보훈국이 지급하는 연금을 수령인들은 매년 그들의 소득변화를 신고해야 했다. 그러나 원고는 사회보장법에 의하여 수령한 액수를 재향군인국에 신고하지 않았는데 보훈국은 복지부가 제공하는 사회보장연금을 받

51) 번역은 변재옥, 앞의 글, 56면에서 인용함.

52) 393 F. Supp. 626, 628 (S. D. N. Y. 1975)

53) 38 U. S. C. §521 (1988)

는 사람들의 기록과 보훈국이 지급하는 연금을 수령하는 사람들의 기록을 컴퓨터로 연결, 검토하였다. 이러한 연결을 통하여 보훈국은 원고가 신고의무를 이행하지 않았음을 발견하였고 재향군인국은 원고에게 연금액 삭감을 통지하였다. 이에 대하여 원고가 소를 제기하였으나 법원은 이러한 원고의 주장을 기각하였다.

다른 사건은 1982년에 교육부가 학자금을 대출받고도 아직 변제하지 못한 대학생들의 명단과 현직에 있거나 이미 퇴직한 연방공무원들의 명단을 컴퓨터로 대조한 사건이다. 이러한 컴퓨터연결로 인하여 갚을 수 있음에도 불구하고 아직 갚지 않은 금액이 3천4백만 달러에 달한다는 것이 드러났다.[54] 그런데 1982년 채무변제법(Debt Collection Act)에 따르면 공무원이 연방합중국에 대하여 채무를 지고 있는 경우에, 이를 갚지 못한다고 있는 것이 해당 기관이나 다른 기관의 장에 의하여 확인될 경우 법으로 정해진 기간 동안 다달이 일정액을 해당 개인의 월급에서 압류하도록 규정하고 있었다.[55]

4. 전자정부와 행정정보의 공동이용

가. 행정정보의 공동이용의 의의와 필요성

행정업무의 효율성을 높이고 질 높은 정책정보의 산출하며 국민의 불편을 해소하기 위하여 행정정보 공동이용의 필요성이 증대하고 있음에 따라 행정정보의 공동이용이 제도화되고 있다. 정보의 공동활용 또는 이용이란 컴퓨터 시스템과 네트워크를 바탕으로 하여 국가기관과 공공기관이 각 국가기관별로 업무수행 목적상 보유하고 있는 전자적 정보를 효율적인 업무

54) 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)

55) 5 U. S. C. §5514 (a)(1) (1988)

수행과 행정의 투명성을 확보하고, 이를 바탕으로 한 차원 높은 대민서비스를 위하여 기관내 부문과 부문 또는 기관과 기업, 기관과 개인 사이에 정보를 공동으로 함께 사용하는 것[56]이며 정보자원관리의 최적화를 위한 제도라고 평가된다.

행정정보를 얻는 방법으로는 회의 등 직접적 대면접촉을 통한 공유, 문서교환 및 전자적 방법 등을 생각할 수 있으나, 정보전달의 신속성, 정확성, 대량처리, 시간적 장소적 한계의 극복, 종이절약, 노동력 절약에는 전자적 방법에 의한 공유가 가장 유리하다고 평가된다. 물론 전자적 방법에 의한 정보의 공유에는 공공자료의 디지털화, 국가 및 공공기관의 정보화를 전제로 하며, 국민 또는 기업으로부터 수집한 정보를 모든 정부기관에서 공유하고 재사용할 수 있어야 한다.[57] 또한 정보보호문제, 프라이버시 문제, 비용부담 문제 등 애로도 존재한다[58]고 지적된다.

이러한 문제를 해결하기 위하여 과거 행정정보공동이용에관한규정(1998. 3. 28. 대통령령 제15745호)이 시행되었으며, 현재는 전자정부구현을 위한행정업무등의전자화촉진에관한법률(2001. 3. 28. 법률 제6439호)이 제정되어 시행되다가 2006년 12월 8일에 전자정부법으로 개정(일부개정 2007.1.3 법률 제8171호; 시행일은 2007. 7. 4.)되었다. 2006년 11월 14일에는 “행정정보공동이용법안”이 제출되어 현재 국회에서 심의중이다.[59]

나. 정보공동활용의 구성요소 및 문제점

전자적 방법에 의한 행정정보공동이용에는 몇 가지 구성요소가 필요하다. 정보공동활용 이해관계자, 정보내용 및 응용기반, 정보유통기반, 정보

---

56) 김성태, 『전자정부론 - 이론과 전략』, 법문사, 2004, 389면.

57) 김성태 , 앞의 책, 389면.

58) 같은 책, 390면.

59) 이 법안은 인터넷 국회 홈페이지(http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=037881)에서 찾을 수 있다.

전송망기반 및 법령, 행정관행, 예산제도, 리더십의 지지와 관심 등 제도 환경이 그것이다.

이를 기초로 정보공동활용 유형[60]은 공통행정업무, 정책결정지원, 민원서비스, 열린정부(인터넷포털) 등으로 나눌 수 있다. 공통행정업무는 행정처리, 국가운영관리, 조직운영에 따르는 공통적 업무영역으로서 문서관리, 이사, 재정정보, 전자조달 등이 이에 해당한다. 법령에 근거를 두고 관련 업무를 수행하는 기관이 유지·관리하는 대장, 원부 또는 장부 등이나 이에 갈음하는 파일(이하에서는 법정대장"이라고 한다. 주민등록표, 호적부, 토지 및 건물등기부 등)은 공동이용의 대상이 되기 쉽다. 이 업무와 관련해서는 제공기관과 이용기관의 책임과 의무관계가 명확해야 하며, 공동활용되는 정보와 관련업무가 사전적으로 명시화되어야 하며, 예상되는 문제발생과 여건의 변화에 대응할 수 있게 참여기관간의 사전조정이 구조화되어 있어야 한다. 특히 DB 개발에서 참여기관간의 자료항목의 분류나 프로그램, 시스템의 호환성이 보장되어야 한다[61]고 한다.

정책결정지원과 관련해서는 국내외 정책관련기관에서 제공되는 통계, 문서, 문헌 등이 그 대상이 되며 수집하는 자료의 목록을 제공하여 상호간의 정보수집의 역할분담을 결정하는 것이 중요하며 동일한 기관이나 문헌에 대한 중복적 자료수집을 줄이고 정보제공이 참여기관에 동시에 이뤄져야 한다. 특히 일부정보를 제공하지 않고 감추는 행위를 억제하고 중복되는 자료수집활동에 참여한 인력과 자원을 다른 자료수집으로 돌려야 한다고 지적된다.

민원서비스는 기존 업무처리방식과 상충되지 않는 점진적이고 계획된 방식이 도입되어야 하며, 일선 인력에 대한 충분한 교육훈련 필요하다고 한다.

인터넷 포털(열린정부)와 관련해서는 언론이나 일반국민에게 제공되는 많은 행정정보를 국민이 보다 쉽게 접근할 수 있도록 통합 제공하고, 홍

60) 김동욱, 「행정정보공동이용의 효율적 추진」, 《국가기간전산망저널》 제3권 제2호, 1996. 6. 김성태, 앞의 책, 390면 이하에서 재인용.

61) 김성태, 앞의 책, 396면.

보, 정책해설자료를 체계화하여야 한다고 지적된다. 이를 위해서는 각 기관에서 제공되는 정보를 받아 관리할 수 있는 네트워크 장비와 네트워크 관리기술이 중요한 요건이 된다.

그러나 그 동안 이러한 행정정보의 공동이용은 잘 이뤄지지 않았으며 최근에 들어 전자정부사업의 일환으로 행정정보공동이용이 적극 추진되고 있으며, 행정자치부에 이를 담당하는 행정정보공유추진지원단이 만들어져 활동하고 있다. 그 동안 행정정보의 공동이용을 적극 주장해온 입장에서는 정보공동활용 저해요인을 다음[62]과 같이 지적하고 있다.

1. 국가차원의 정보화정책 수립 부재
2. 법령상의 문제: 정보공개, 프라이버시, 보안, 책임규정
3. 기술적인 문제
4. 집행조직상의 문제(추진체계의 문제)
5. 전문인력의 문제
6. 재원확보의 문제
7. 조직문화(행태적) 문제
8. 정보의 권력수단화(독점화) 문제
9. 정치적 지지력 부족
10. 업무적 문제
11. 정보화 인식부족
12. 정보사용에 따른 부담 문제
13. 정보공동활용에 대한 정보부족 문제(대상정보, 정보소재,접근방법 등)
14. 이해관계의 불균형 문제(중요시되는 정보의 I/O, 정보량 측면 불균형의식)
15. 정보보호와의 갈등 및 국민의 지지 부족

정보공유를 위한 전제조건인 문서의 전자화는 서서히 진행되고 있다. 행정정보공유추진 실무를 담당하고 있는 행정정보공유추진단의 조사(2006년 9월)에 의하면, 39개 중앙행정기관과 지방자치단체에서 관리하고 있는 법정대장 875종 가운데 65% 정도인 565건이 전자화되었거나

62) 김성태, 「전자정부 조기구현을 위한 행정정보공동활용 저해요인 분석: Fish-bone Analysis의 적용」, 《한국정책분석평가학회보》 8권 1호, 1998. 9. 김성태, 399면 이하에서 재인용.

전자화가 진행중[63]이라고 보고된다.

행정정보보유기관은 대부분의 행정정보가 포함하는 재인정보 누설의 위험과 행정정보를 공유함으로써 정보의 오·남용이 발생할 경우 정보보유기관의 부담이 크다는 점으로 인하여 소극적인 경향이 나타난다[64]고 한다.

다. 행정정보 공동이용 추진[65]

행정정보의 공공이용은 각종 민원사항의 처리를 위하여 제출되는 구비서류의 감축이 가장 직접적인 이유가 된다. 또한 증명서를 제출할 경우 발생하는 위·변조의 문제와 증명서에 포함되는 불필요한 정보의 제공과 노출의 위험성을 해결하고자 하는 것도 부가적인 이유가 된다고 한다. 이를 위하여 2006년 7월 20일 국정과제회의에서 '행정정보 공공이용 현황 및 개선방안'을 논의하여 행정정보의 공동이용을 국정과제로 추진하기로 하고 국무총리 소속으로 행정정보공유추진위원회를 설치하고 그 위원회에 실무기구로 행정정보공유추진단을 두어 행정정보 공동이용 사업을 추진하고 있다. 정부의 행정정보공유사업의 기본적 골격을 정한 법안이 앞에서 언급한 '행정정보공동이용법안'이다. 이 법안의 별표에서는 공동이용할 행정정보로 주민등록표, 부동산등기부, 법인등기부 등 70여 종을 적시하고 있다(뒤의 표 참조).

2005. 1. 31.부터 주민등록등·초본 정보 등 24종은 이미 공동이용이 개시되었으며, 2006. 9. 1.부터는 10개 행정정보에 대한 공동이용을 확대하

---

63) 심현정, 「행정정보공동이용제도에 대한 이해와 관련 법제의 발전방향」, 《법제》 2007년 1월호, 91면.(2006년 9월 현재. 단위: 건)

	계	'04 이전	'05	'06	'07	'08	'09
전자화 완료	487	353	75	59			
전자화 추진	78			29	27	13	9
전자화 미추진	310						
합계	875	353	75	88	27	13	9

64) 심현정, 앞의 글, 92면.

65) 이 내용은 심현정, 앞의 글, 94면 이하에서 정리한 것임.

였고, 2007. 3월부터는 공장등록증 등 7개 행정정보를 추가로 확대할 계획이며, 나머지 정보는 2007년 하반기에 추진할 예정이며 2007년까지 완료할 예정이다.

공공기관은 1차적으로 2006. 9. 1부터 국민건강보험공단, 국민연금관리공단, 근로복지공단, 한국전력공사 및 신요보증기금 등 5개 공공기관에 대하여 11개 행정정보의 공동이용 시범사업을 실시하여 2007. 3월부터는 공무원연금관리공단 등 29개 공공기관으로 이를 확대하고 있다. 금융기관에 대해서는 2007년 3월부터 우리은행 등 2개 은행에 대하여 시범사업을 실시하고 있다.

행정정보공동이용법안의 [별표]

행정기관 및 공공기관의 공동이용 대상 행정정보(제6조제1항 관련)

번호	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 법적지위에 관한 법률」 제7조제5항에 따른 국내거소신고사실증명에 관한 정보	법무부
6	「출입국관리법」 제88조제1항에 따른 출입국에 관한 사실증명 정보	
7	「출입국관리법」 제88조제2항에 따른 외국인등록사실증명에 관한 정보	
8	「부동산등기법」 제14조 및 제41조의2제1항제4호에 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」 제38조제2항에 따른 지방세 납세증명서에 관한 정보	
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」 제2조제1호가목에 따른 토지대장에 관한 정보	

18	「지적법」 제2조제1호가목에 따른 임야대장에 관한 정보	
19	「지적법」 제2조제1호가목에 따른 지적도에 관한 정보	
20	「지적법」 제2조제1호가목에 따른 임야도에 관한 정보	
21	「산업집적활성화 및 공장설립에 관한 법률」 제16조에 따른 공장등록에 관한 정보	산업자원부
22	「광업법」 제43조에 따른 광업원부에 관한 정보	
23	「대외무역법」 제14조제2항에 따른 수입승인에 관한 정보	
24	「석유 및 석유대체연료 사업법」 제10조에 따른 석유판매업의 등록에 관한 정보	
25	「국민기초생활 보장법」 제2조제2호에 따른 국민기초생활 수급자에 관한 정보	보건복지부
26	「장애인복지법」 제29조에 따른 장애인등록에 관한 정보	
27	「오수·분뇨및축산폐수의처리에관한법률」 제24조의2에 따른 축산폐수배출시설설치허가 및 신고에 관한 정보	환경부
28	「폐기물관리법」 제24조제2항에 따른 사업장폐기물배출 신고에 관한 정보	
29	「국가기술자격법」 제13조에 따른 국가기술자격증에 관한 정보	한국산업인력공단
30	「건설기계관리법」 제3조제3항에 따른 건설기계등록증에 관한 정보	건설교통부
31	「건설기계관리법」 제7조에 따른 건설기계등록원부에 관한 정보	
32	「건설산업기본법」 제9조에 따른 건설업의 등록에 관한 정보	
33	「건설기계관리법」 제13조제4항에 따른 건설기계검사증에 관한 정보	
34	「건설기계관리법」 제21조에 따른 건설기계사업의 신고에 관한 정보	
35	「건축법」 제8조제1항에 따른 건축허가에 관한 정보	
36	「건축법」 제18조제2항에 따른 건축물 사용승인서에 관한 정보	
37	「건축법」 제29조에 따른 건축물대장에 관한 정보	
38	「건축사법」 제23조에 따른 건축사 업무의 신고에 관한 정보	
39	「토지이용규제 기본법」 제10조제1항에 따른 토지이용계획확인서에 관한 정보	
40	「부동산가격공시및감정평가에관한법률」 제11조에 따른 개별공시지가에 관한 정보	
41	「자동차관리법」 제7조에 따른 자동차등록원부에 관한 정보	
42	「자동차관리법」 제8조제2항에 따른 자동차등록증에 관한 정보	
43	「자동차관리법」 제48조제1항에 따른 이륜자동차의 사용신고에 관한 정보	
44	「주택법」 제29조제1항에 따른 주택 또는 대지의 사용검사에 관한 정보	
45	「선박법」 제8조에 따른 선박국적증서에 관한 정보	해양수산부
46	「선박법」 제26조의2에 따른 선적증서원부에 관한 정보	
47	「선박안전법」 제9조제1항에 따른 선박검사증서에 관한 정보	
48	「수산업법」 제8조에 따른 어업면허에 관한 정보	
49	「어선법」 제13조에 따른 어선의 등록에 관한 정보	
50	「해양오염방지법」 제23조제1항에 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」 제248조제1항에 따른 수출입신고에 관한 정보	관세청
58	「병역법」 제5조제3항에 따른 병적관리에 관한 정보	병무청
59	「도로교통법」 제80조에 따른 운전면허에 관한 정보	경찰청
60	「특허법」 제85조에 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	

라. 행정정보공동이용법안의 문제점

행정정보공동이용 사업이 가지는 문제점은 크게 개인정보의 보호, 보유기관의 책임부담 등을 지적할 수 있다. 여러 가지 문제점을 해결할 목적으로 정부에서는 '행정정보공동이용법안'을 마련하여 국회에 제출한 상태이다. 그러나 현재 존재하는 여러 법률의 문제점을 해결하기 위하여 행정정보 공동이용에 관한 법률안을 마련하고 있지만 이 법안은 다음에서 지적하는 것과 같은 문제점을 안고 있다. 물론 우선적으로 개인정보보호가 확보되어야 한다. 이를 위해서는 공공기관의 개인정보 보호에 관한 법률을 개정할 필요가 있다. 여기서는 구체적인 논의를 하지 않는다.[66]

66) 기존의 연구로는 강경근, 『행정정보의 공동이용에 따른 법적 과제』, 한국법제연구원, 2001. 12 참조.

(1) 개인정보보호

이 법안은 주로 행정의 효율성과 국민의 편의를 위하여 행정정보의 공동이용에 초점을 맞추고 있어 개인정보보호의 문제를 직접 언급하고 있지 않다. 그러나 정보의 공유가 확대되면 확대될수록 정보의 누설 위험성은 증가할 수밖에 없다는 것은 확실하다. 이 점에서 공동이용의 기본원칙으로 개인정보보호의 원칙이 명시되는 것이 좋다고 생각된다. 효율성과 편의성을 위하여 추진되는 사업에 필연적으로 따르는 위험이라면 법안에 그 위험을 감소시키기 위한 큰 틀이 마련되어야 한다고 생각하기 때문이다.

제7조 제3항에서는 행정정보 외에 국가정책의 수립과 행정업무를 수행하기 위한 주요 판단자료로서 특정 개인을 식별할 수 없는 형태로 가공된 행정정보를 공동이용할 수 있다고 하나, 개인을 식별할 수 없는 형태로 누가 가공하고 만약 직접 개인을 식별할 수 있는 정보는 없으나 여러 정보를 종합하여 개인을 식별할 수 있을 경우에 발생하는 개인정보보호의 문제와 책임부담의 문제에 대해서는 명확한 규정을 두고 있지 않다.

또한 제9조의 공동이용의 제한과 관련하여 행정자치부장관이 공동이용을 승인하지 않을 사유가 상당히 광범위하게 정하여져 있음을 알 수 있다. 즉 개인정보보호를 위하여 공동이용이 제한되는 것이 좋은 면이 있으나, 추진 이유로 제시하듯이 종이 증명서의 제출로 인하여 불필요한 정보가 누출될 위험을 감소시키기 위한 정보공유라면 지나치게 판단의 여지를 넓게 두는 것은 오히려 개인정보보호의 취지에 부합하지 않는다는 비판을 받을 수 있을 것이다.

(2) 공동이용의 승인주체

정보공동이용을 승인하는 주체가 행정정보의 보유기관이 아니라 행정자치부장관으로 되어 있다.(법안 제9조 제1항). 행정자치부장관은 공동이용을 승인하는 경우에는 보유기관과 미리 협의하여야 한다. 보유기관은 정보의 보유와 관리의 주체로서 정보의 누설로 인한 일차적인 책임을 져야

할 주체임에도 정보공유와 관련하여 협의만 할 뿐 결정의 실질적 권한이 배제된 점은 문제가 발생할 여지가 있다.

(3) 정보주체의 확인

정보를 공동으로 이용하기 위해서는 증명서와 같은 형태로 서류를 제출하여야 했던 정보주체의 정보사용에 대한 요구가 있어야 한다. 그러나 정보주체와 정보이용을 요청하는 사람이 동일인진지를 확인하기 위해서는 많은 노력이 기울여져야 한다. 예를 들어 인감증명의 발급을 위하여 예전에는 직접 인감을 가지고 있고, 신분증을 대조하여 인감을 발급하였으나 지금은 전산입력된 인감을 발급하는 데는 인감도장이 필요하지 않으므로 본인 확인 여부가 결정적이 된다고 할 수 있다. 이를 위하여 엄격하게 본인 여부를 확인하도록 하고 있고 인감증명법 제13조 제4항에서는 “인감증명의 발급신청을 받은 인감증명발급기관은 주민등록증 등에 의하여 본인이나 법정대리인 또는 위임을 받은 자임을, 미성년자 또는 한정치산자의 경우에는 그 법정대리인의 동의여부를 확인한 후 복사방지를 위한 특수용지를 사용하여 별지 제14호서식의 인감증명서를 발급하여야 하고, 별지 제15호서식의 인감증명발급대장에 수령인이 본인인 경우에는 서명 또는 무인을, 대리인인 경우에는 무인을 받은 후 이를 교부하여야 한다. 이 경우 인감증명발급기관은 주민등록증 등에 의하여 신청인의 신분확인이 곤란한 때에는 제7조 제3항의 규정에 의한 방법으로 이를 확인할 수 있다. <개정 2003.9.29, 2005.1.15>”고 규정하고 있다. 임간증명법 제7조 제3항의 내용은 “증명청은 제2항의 규정에 의한 방법으로 신분확인이 곤란한 경우에는 인감신고인의 무인을 주민등록전산자료와 전자적 방법으로 대조하여 확인할 수 있다. <신설 2005.1.15>”는 것으로서 제2항에서 정한 바와 같이 주민등록증, 자동차운전면허증, 장애인등록증(주민등록번호 및 주소가 기재되어 있지 아니한 장애인등록증을 제외한다) 또는 여권(재외국민인 경우에는 여권, 외국인인 경우에는 외국인등록증, 국내거소신고자인 경우에는 국내거소신고증과 여권을 말한다.)에 의하여 직접 확인이

어려운 경우를 말한다.

오늘날 신분증에 담긴 사진만으로는 본인식별이 어렵고 부정확한 방법에 의한 본인확인은 정보주체에게 큰 피해를 가져올 수 있으므로 엄격한 확인은 필요하다. 그러나 문제는 “신분확인이 곤란한 경우에는 인감신고인의 무인을 주민등록전산자료와 전자적 방법으로 대조하여 확인할 수 있다”고 하지만, 실제 이러한 인감증명을 발급하고 있는 일선 행정기관에 전자적 방법을 이용할 수 있는 기기가 비치되어 있지 않기 때문에 이와 같은 전자적 방법에 의한 신원확인이 어려운 경우가 많다는 점이다. 결국 본인확인을 위하여 본인에게도 지문을 채취하는 방법이 활용되고 있다. 이는 과도한 정보제공의 요구라는 점은 말할 필요조차 없다.

(4) 금지행위

법안 제23조에서는 이용기관의 소속 직원의 다음 행위를 금지하고 있다.

1. 행정정보를 제9조제1항에 따라 승인받은 공동이용의 목적 외의 용도로 사용하는 행위
2. 제9조제1항에 따른 승인을 받지 아니하고 공동이용하거나, 승인을 받은 공동이용의 범위를 넘어서 공동이용하는 행위
3. 제11조에 따른 공동이용의 승인철회 또는 중단 후에 공동이용하는 행위
4. 공동이용 행정정보를 행정자치부장관의 승인 없이 다른 기관에게 다시 제공하는 행위
5. 제21조에 따른 접근권한을 등록하지 아니하고 공동이용하는 행위
6. 공동이용 행정정보를 위법한 방법으로 위조·변경·훼손하는 행위
7. 공동이용 행정정보를 해당 처리업무 단위별로 열람하거나 출력하여 사용하는 외에 다른 컴퓨터나 저장장치 등에 저장하는 행위. 다만, 정책정보를 공동이용 하는 경우를 제외한다.

마땅히 금지되어야 할 행위들이다. 그러나 다음의 문제가 있다.

첫째, 공동이용 행정정보를 해당 처리업무 단위별로 열람하거나 출력하

여 사용하는 외에 “다른 컴퓨터나 저장장치 등에 저장하는 행위”는 정책정보를 공동이용하는 경우를 제외하고는 금지된다. 정보이용의 한계와 이용방법을 명시한 것이라고 할 수 있다. 그러나 “컴퓨터”나 “저장장치”의 개념이 명확한가는 의문이다. 이 조항의 금지사항을 위반하면 제26조에 의하여 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하게 되므로 이 문제는 죄형법정주의의 문제이기도 하다. 이 조항은 디지털 파일의 형태로 저장하는 행위를 염두에 두고 규정된 것으로 보이지만 일반적인 저장소 이외의 방법이 사용될 수도 있으며 굳이 디지털 파일이 아니더라도 정보를 저장하는 방법은 가능하다. 예를 들어, 필름을 사용하는 사진기를 사용하여 컴퓨터 화면을 찍는 것은 어떤가? 디지털 사진기를 사용하면 어떤가? 디지털 사진기를 사용하여 저장하는 정보는 보유기관이 제공하는 정보와 크게 보아 다르지 않다고 할 수 있지만 엄격하게 말하면 상당 부분 다른 정보이다. 디지털 사진기로 저장하는 정보는 화면정보이며 화면을 분석하여 일정한 정보를 읽어낼 수 있을 뿐이기 때문이다. 형사처벌의 대상으로 삼을 행위라면 보다 명확한 개념이 사용되어야 할 것이다.

제 4 장 정보인권의 관점에서 본 형사사법정보통합체계의 문제점

형사사법통합정보체계구축 사업은 전자정부조성사업의 일환이며 대통령 훈령에 근거를 두고 진행되는 사업이다. 법원, 검찰, 경찰과 교정에 이르는 형사사법정보를 큰 틀로 통합함으로써 형사사법업무의 표준화 및 전자화, 형사사법정보의 공동활용. 대국민 형사사법서비스의 품질제고 등을 그 목표로 한다고 한다.[67] 그러나 이러한 통합체계 구축사업은 다음과 같은 헌법적 문제점을 안고 있다. 우선 미국에서의 형사사법정보의 공유·통합과 관련된 제도 및 법적 문제에 관한 논의를 소개한 후 우리나라에서의 형사사법정보통합체계구축사업의 문제점을 언급하기로 한다.

1. 미국의 형사사법정보의 공유·통합사업

가. 사법정보시스템 통합(Justice Information System Integration)

사법정보시스템의 통합이란, 널리 연방과 주의 법집행기관, 법원, 건사, 교정당국 등을 포함한 국가의 사법체계의 구성기관들이 수직적으로(기관 내부 상하간) 그리고 수평적으로(기관간) 형사사법정보를 용이하고 효과적으로 공유할 수 있도록 하는 일련의 절차를 말한다. 정보시스템의 통합을 통하여 보다 완전하고 정확한 정보를 필요한 때 즉시 이용할 수 있도록 한다는 구상이다. 여기서 통합(Integration)이란 국가의 사법 관련 기관의 외부에 초월적으로 존재하는 별개의 정보시스템을 만드는 의미는 아니라고 한다. 이러한 통합체계 안에서 각 기관은 자신의 정보를 관리하고 관리권한 있는 자만이 정보를 이용할 수 있다.

---

67) 형사사법정보통합체계사업이 가지는 문제점 전반에 관해서는 김희수, 『개인정보 수집·저장·이용의 적법성과 한계(정보인권 관점 등에서 본 형사사법통합정보체계)』, 국가인권위원회, 2006. 12에 자세하게 논의되고 있으므로 본 보고서에서는 이 보고서가 다루지 않은 부분에 관해서만 간단하게 언급하고자 한다.

이러한 사법정보시스템의 통합의 장애로 지적된 것은 기술적 문제가 아니라 법적, 정책적 문제였다. 누가 정보를 보유하는가, 누가 접근할 수 있는가, 어떻게 활용할 것인가, 어디에 보관할 것인가, 비용부담은 누가 하는가 등의 문제가 해결되어야 한다고 지적된다.[68]

FBI의 베트남전반대 시위자에 관한 존안정보의 폭로에 대한 분노의 결과로 1974년 프라이버시보호법이 제정되어 그 동안 정보수집 축적에 대한 통제가 이뤄져 왔다. 이러한 사법정보통합 움직임은 2001년 9·11사건 이후 여론이 급변하여 대테러움직임에 따라 법집행기관의 정보에 대한 요구가 급증하게 됨으로써 더욱 촉진되는 양상을 띤다.

나. 콜로라도주 형사사법정보통합체계(CICJIS)

1) 개요

콜로라도주형사사법정보통합시스템(Colorado Integrated Criminal Justice Information System: CICJIS)는 4개의 주 기관과 1개의 준 주형사사법기관-콜로라도주 수사국(CBI), 법원(Judicial Brach), 교정부(DOC), 청소년국(DYC) 및 콜로라도 지역 변호사위원회-의 개인정보시스템을 컴퓨터상 하나의 형사사법시스템으로 연결하는 것이다. 콜로라도주는 1974년부터 형사사법정보통합시스템을 구축하기 위하여 노력을 기울여 왔으며, 1998년 미국연방의 주로서는 최초로 이 시스템을 구축하였다.

C.R.S. 16-20.5-101.5에 의하면, CICJIS의 목적은 (1) 공공의 안전 (2) 의사결정 (3) 구성원의 생산성을 증진하고 (4) 적시에 정확하고 완전한 정보에 대한 접근할 수 있도록 하는 것 등 4가지로 규정되어 있다.

CICJIS 운영위원회(Executive Policy Board)는 5개 기관의 담당부서의

68) NGA Center for Best Practices에서 발행한 Issue Brief "Improving Public Safety through Justice Information Sharing" 참조.(NGA Center for Best Practices는 주지사와 정책참모들을 위한 자문기관이다. 따라서 이 문서는 정책결정자의 관점에서 작성된 자료이다.) (http://www.nga.org/portal/site/nga/menuitem.1f41d49be2d3d33eacdcbeeb501010a0/?vgnextoid= 3e16aa9c00ee1010VgnVCM1000001a01010aRCRD 2006. 12. 20. 검색) 아래의 서술 내용은 대체로 이 기관 발행문서에서 요약된 것이다.

장으로 구성되며, 시스템의 운영을 총괄하고 이에 관한 정책을 수립한다. 각 기관의 담당부서의 장은 CICJIS Task Force에 각각 1인씩을 지명하여 시스템의 작동을 매일 점검도록 하고 있다. 주지사와 콜로라도주 대법원장은 CICJIS정보센터의 장(CIO)을 지명하여 운영위원회에 보고하게 하며, CIO는 CICJIS 중앙통제소에 관한 사무를 관장한다.

2) 감사관의 보고(2003년 7월)로 본 문제점[69]

콜로라도 주 의회의 감사관이 감사한 결과는 이러한 통합시스템이 가지는 문제를 어느 정도 보여 준다. 우리의 경우에도 충분히 참고할 내용이라 생각된다.

(1) 데이터의 완전성 문제

CBI의 범죄정보센터(CCIC)가 법원의 콜라도통합정보통신망(ICON)의 사건판결과 그 사건 피고인의 체포 및 구속 기록(Record of Arrest and Prosecution: RAP sheet)을 연결시킬 때 결정 연결(Disposition Match)이 이뤄진다. 법원담당자(Judicial Staff)의 말에 의하면 CICJIS 시스템은 1998년 5월부터 중죄(felony)결정된 것을 전송(transfer)하기 시작했으나 2000년 1월 이전까지는 중죄결정 연결비율(matching rate)을 공식적으로 산정하지 않았다고 한다. 2003년 6월 현재 누계로 결정연결사건비율은 약 88%이다. 결정을 사건과 연결시키지 않은 것은 범죄일지기록이 불완전하거나 정확하지 않다는 의미라고 할 수 있다. CICJIS 운영위원회는 사건이 연결되지 않은 원인을 밝혀 각 기관이 비(非)연결율을 높일 수 있도록 협조하여야 하며, 1998년 5월 이후의 형사사건의 결정으로서 아직 연

69) 콜로라도 주 형사사법정보시스템(CICJIS)에 대한 감사는 주 감사관실에 주정부의 모든 부처, 기관의 업무수행에 대한 감사권한을 부여한 C.R.S. Section 2-3-103에 근거하여 이뤄졌다. 감사는 일반적으로 인정되는 정부감사기준에 의거하여 이뤄졌다. 감사는 2003년 1월부터 6월까지 실시되었다.

결되지 않은 결정을 연결시켜야 하고, 또한 1998년 5월 이전의 결정이라도 전자적 수단에 의하여 이용이 가능한 것은 결정을 연결할 수 있는 가능성을 고려하여야 한다.

(2) 시스템의 기능성 문제

최근(2003년초)까지 CICJIS 사용자는 저장시스템 내의 가해자와 관련된 올바른 주(州)신분증명(State Identification: SID)을 무력화할 수 있는 잘못되거나 상이한 SID를 수작업으로 입력하였다. 2003년 2월 CICJIS 프로그램은 CICJIS 버전 2.0을 사용하기 시작했으며, 이 프로그램은 전송중에 차이가 인식될 경우 각 기관에게 이 사실을 통지해 준다. 각 기관은 정보의 전송이 완료되기 전에 이러한 오류를 정정하게 된다. CICJIS 프로그램을 운영하는 데는 데이터오류의 효과적 보고와 오류 확인결정을 감시하는 것이 중요하다. CICJIS 운영위원회는 자주 발생하는 오류의 원천을 확인하고 문제해결방안을 수립하는 한편 시스템전반에 걸친 데이터의 완전성을 높이기 위한 지표를 개발하는 등의 방법에 의하여 데이터의 완전성을 높여야 한다.

(3) 정보의 상위(相違)

CICJIS 시스템은 피고인이 형사적 성인으로 또는 미성년으로 선고되었는지에 따라 Judicial mittimus를 DOC 또는 DYC에 자동으로 전송한다. 수감명령장(mittimus)이란 DOC 또는 DYC에 피고인을 구금하도록 하는 법원의 명령이다. 표본 10건의 성인에 대한 수감명령장(mittimus)을 조사한 결과 표본 가운데 6건 또는 60%에서 ICON 데이터에 나타난 손해배상액(restitution amount)이 DOC의 교정정보시스템(Department of Corrections Information System: DCIS)에서와 차이를 보였다. 이러한 조사결과는 청소년에 대한 수감명령장(mittimus)에 대한 조사에서도 비슷하게 나타났다. 20건의 표본 가운데 11건 또는 55%에서 DYC의 콜로라도 Trail System과 ICON 사이에 연결에 문제가 발견되었다. 교정부

(DOC)는 좀더 상세한 배상 및 판결선고 정보를 얻고, ICON으로부터 정보를 upload하기 위하여 DCIS로 프로그램을 변경시킬 실현가능성을 평가하기 위하여 CICJIS시스템에 관한 의문을 항상 새롭게 갱신하여야 한다. Department of Human Services는 DYC 담당자들이 현재의 배상잔고를 확인할 수 있도록 ICON에 직접 접근하여 사용할 수 있는 능력을 갖추도록 보장하지 않으면 안된다.

(4) 시스템 사용교육 필요성

CICJIS 시스템은 1998년에 실시되었지만 사용자들 모두가 언제나 시스템의 성능(capabilities)을 활용할 능력을 가지는 것은 아니라는 것을 발견하였다. CICJIS 프로그램 활용교육은 제한적으로만 이뤄졌으며, 교육의 대부분은 5개 기관마다 각 기관이 보유하는 정보시스템 교육으로 이뤄졌다. 그러나 5개 기관 가운데 3개 기관은 CICJIS 시스템사용방법까지 설명하는 사용자 매뉴얼이 없었다. CICJIS 운영위원회는 5개 기관과 함께 각 기관시스템교육 속에 CICJIS 교육을 포함시키도록 하여야 하며, CICJIS를 개괄하는 문서를 만들고, 교육수요를 파악하는 조사를 해야 한다.

(5) 전자지문채취

콜로라도 주 카운티의 3분의 2는 보다 효과적인 지문채취방법인 Livescan 프로그램을 이용하지 않고 있다. Livescan은 지문 기타 체포정보가 전자적으로 법집행기관의 기록장치에서 CBI로 즉시 제출되도록 하고 있다. Livescan 기술은 그밖에도 다른 장점을 가지고 있다. 예를 들어, 실시간으로 지문카드를 전송함으로써 신원을 속이는 피체포자의 신원을 적절하게 확인할 수 있다. 통계에 의하면, RAP sheet에 기록된 사람의 45%는 적어도 1개 이상의 별명을 갖고 있다 한다. 더욱이 지문의 질이 CBI 기준을 충족하지 못할 경우 지역의 법집행기관에 신속하게 통보되어 당사자가 구금된 상태에서 지문을 다시 채취할 수 있게 된다.

CICJIS 운영위원회는 Livescan 기계를 취득하기 위하여 연방정부로부터 재원을 확보하기 위하여 계속 노력하여야 하며, 카운티에 필요한 유지, 지원 및 접속을 제공하기 위하여 계획을 추진해야 한다.

3) CICJIS의 미래

CICJIS 시스템의 초기설계과정에서 시스템 전반에 적용되는 형사사법데이터유형에 한계를 설정하였다. 그 결과 이 시스템에서는 모든 유형의 형사사법정보를 교환하는 것은 아니다. 경범죄가 그 예이다. CICJIS 프로그램은 전략적으로 모든 완전한 형사기록을 제공하기 위하여 이러한 한계를 설정하기 위하여 추가조치를 취하여야 한다고 인식하였다. CICJIS 프로그램의 사용이 확장됨에 따라 모든 주에 걸친 형사사법정보접근의 유일한 지점이 되어야 할 필요가 있다. CICJIS운영위원회는 콜로라도 형사사법커뮤니티의 사용자의 수요를 주기적으로 측정하고 CICJIS 프로그램이 대상과 정보를 추가하도록 범위를 확장함으로써 CICJIS 프로그램이 확대사용될 수 있도록 하여야 한다.

CICJIS운영위원회는 프로그램의 방향을 정립하며, CICJIS Task Force는 시스템의 작동을 매일 점검한다. C.R.S. Section 16-20.5-103은 CICJIS 관리기구의 구성원을 정의하고 있으나, CICJIS 시스템의 확대가 위원회의 구성에 어떤 영향을 미칠지에 대해서는 예상하지 못하고 있다. 모든 관련자들의 의견을 효과적으로 대변하려면 위원회는 구성원을 확대할 여지를 둔 메커니즘을 만들어야 한다. 더욱이 CICJIS CIO position를 조직배치하는 것은 법령과 일치하지 않는다. CICJIS 운영위원회는 장래의 발전을 포용하고 need clarification of CIO position를 포함한 법령변화도 추구할 수 있도록 현재의 관리구조를 검토하지 않으면 안된다.

다. 형사사법정보통합시스템과 프라이버시권 침해 논의

1) 형사사법정보통합시스템은 프라이버시보호환경을 어떻게 변화시키는가?

형사사법정보통합은 공공의 안전(public safety)을 강화하고자 하는 의도를 제시하며 추진된다. 이를 위하여 형사사법정보의 공유·통합이 이뤄지고, 우리 나라에서는 아직은 고려 대상 밖이지만, 나아가 통합된 정보의 판매도 가능해지는 상황이 초래될 수 있다. 특히 공공의 안전에 관련되는 업무를 수행하는 기업의 경우 그러한 정보에 대한 수요가 강하며, 정부기관 역시 공공의 안전을 확보한다는 취지에서 정보공유가 이뤄질 가능성도 매우 높다고 할 수 있다.

그러나 이러한 공공의 안전을 이유로 한 형사사법정보통합작업은 의도하지 않은 결과를 낳을 수 있다. 피해자, 증인, 법집행공무원 기타 사법절차에 관여한 사람들의 인적사항과 활동내용들의 상세한 기록들이 보안 허술로 유출될 경우 피해를 발생시킬 수도 있다.

특히 기술의 발전과 이를 반영한 정책의 변경에 따라서 민사와 형사사법정보가 거의 완벽하게 집결될 수 있다. 이러한 발전 때문에 전통적인 프라이버시 보호정책으로는 대처하지 못하는 새로운 이슈가 발생한다. 과거에는 개인을 식별할 수(personally identifiable) 없는 정보가, 이제는 통합되고 종적 횡적으로 공유되면서 개인별로 식별될 수 있게 된 것이다.

이러한 사법정보 공유 및 통합은 미국에서는 지난 10여 년간 관심을 기울여 왔으며, 특히 9·11 테러 이후에 역점을 기울여 왔다. 그 결과 사법정보에 대해 법집행공무원, 검찰, 교정공무원 및 법원이 손쉽게 접근할 수 있게 되었다(접근성 향상). 그러나 이와 함께 개인의 프라이버시에 대한 관심도 고조되었다.

이러한 논의에서 핵심적인 것은 통합정보체계를 통하여 집합된 정보가 기존의 개별적인 정보와 근본적으로 다른 것인가 하는 점이다.

이에 대해 연방대법원의 한 판례[70]에서는 다음과 같이 언급하고 있다.

---

70) U.S. Department of Justice et al. v. Reporters Committee for Freedom of the Press et al., 489 U.S. 749(1989)

"이 사안의 핵심은 정보의 집적(compilation)에 의해 다른 방법으로는 얻을 수 없는 다른 정보를 얻는 것이 정보의 공개라는 것으로 표현되는 프라이버시보호의 차원을 바꾸는 것이냐의 문제이다. 개별적으로 보관중인 법원의 문서, 카운티 문서고, 지방경찰서의 문서를 부지런히 뒤져서야 얻을 수 있는 공공기록과 정보관리를 담당하는 한 기관에서 컴퓨터로 처리된 정보는 엄청난 차이가 있다는 것은 확실하다."

즉 단편적인 정보와 집적된 정보는 엄청난 차이가 있다는 점을 인정하고 있는 것이다. 특히 통합된 사법정보기록은 단편적인 정보에 비하여 큰 차이가 있다. 사법정보기록은 일정단계에서는 공공정보가 되지만, 체포부터 교정에 이르는 사건의 전과정을 파악하는 것은 직접 몸을 움직여 법원, 검찰과 경찰, 기록보관소에 가서 기록을 찾아내는 과정을 거치지 않으면 안된다. 그러나 이제는 개인기업과 단체가 직접 찾아가지 않고도 전자적으로 정부가 또는 기업이 운영하는 사이트를 통하여 순식간에 정보에 접근할 수 있게 된다. 이러한 정보의 거래는 미국의 각 주(州)에서 주된 수입원이 되고 있다. 예를 들자면, 2005년 어떤 주에서 운전면허발급정보를 판매하여 3억-4억의 수익을 올렸다. 미국 전역에는 약 2억 2700만 정도의 운전자가 있으며 주가 이들에 관한 정보를 50센트 내지 6달러에 판할 경우 그 수입은 엄청나다. 그 밖의 다른 범죄내역 또는 조세내역 등 자료를 판매하는 경우 그 수입은 훨씬 큰 것이 된다.

형사사법정보공유에서 나타나는 프라이버시에 관한 가장 중요한 변화 실제에서의 모호함(practical obscurity)이 감소하는 것이라고 할 수 있다. 통합시스템은 인물이나 사건에 관한 중요정보의 수집과 보고만 아니라 데이터베이스에 대한 검색능력을 높이기 위한 것이다. 달리 표현하자면 정보에 대한 접근장벽을 없앰으로써 사법작용을 강화하고자 하는 것이다. 그러한 장벽이 실제적 모호함의 요소가 된다.

"우리는 우리의 삶이 사적이라 함은 공중의 접근으로부터 개인의 정보가 완벽하게 차단되는 것을 말하는 것이 아니라, 대개는 수백만의 사람들에 관한 정보의

바다 속에 있다는 것을 의미한다는 점은 잘 알고 있다. 개인의 정보가 백사장에 떨어진 바늘에 불과하여 보통의 경우는 누구도 그것을 찾으려고 하지 않기 때문에 사적(private)이라는 것이다. 이러한 익명성은 (이러한 정보를 디지털화하여 축적하는 분석기술에 의하여) 정보에 대한 접근성이 증가하면서 점차 사라지고 있다."[71]

최근까지만 해도 공적기록에 접근하는 것은 접근하기가 어려웠으며, 부분적으로만 가능했다. 한 사람에 관한 정보를 찾기 위해서는 여러 기관의 기록을 뒤지 않으면 안되었다. 법원의 기록을 열람할 수 있더라도 찾아야 할 법원이 여러 곳이었다. 사람들은 대부분 자기 이웃이 어떤 혐의로 기소되었는지를 굳이 알려 하지 않기 때문에 진짜 관심을 가진 사람만이 자료에 접근할 수 있었고 불확실함을 없애려고(loss of practical obscurity) 씨름하지 않으면 안되었다.[72]

U.S. Department of Justice v. Reporters Committee for Freedom of the Press[73] 판결에서도 "부지런히 법원파일을 뒤져서만 알 수 있는 공적 기록과 한 군데 보관되어 컴퓨터로 정리된 정보는 엄청난 차이가 있다."는 취지[74]를 설시하고 있다.

컴퓨터에 의한 정보처리와 공유는 수집과 분석이 용이하게 되어, 개별적으로 별 게 아닌 정보도 종합적으로 보면 개인의 전모를 파악할 수 있게 한다. 정보는 정보를 낳는다. 사회보장번호는 그 자체로 정보라고 하기에 어려움이 있으나 이를 통하여 금융, 교육 및 의료정보에 접근할 수

71) Solove, Access and Aggregation: public Records, Privacy and the Constutuion, 86 Minnesota Law Review, 1137(2002), 1178면.

72) Amy Harmon, As Public Records Go Online, Some Say They're Too Public, New York Times, 2001. 8. 24. 자.

73) 489 U.S. 749(1989)

74) FBI가 연방과 주의 법집행기관으로부터 제공받은 정보를 전과기록 또는 인명별범죄기록(체포, 기소, 평결, 구금 등 일련의 기록.)으로 집적하여 보관함. 언론자유를 위한 기자위원회에서 정보공개법(FOIA)에 근거하여 Charles Medico에 관한 전과기록공개를 청구(matters of public record)하였으나 FBI가 거부하여 지방법원에 공개청구소송을 제기한 사건이다.

있게 한다.

2) 어떠한 위험을 초래하는가?

(1) 누구에게, 어떠한 위험이 있는가?

우선 범죄와 관련없는 개인이 사법시스템에 노출될 위험이 지적되어야 한다. 피해자, 증인, 어린이, 정보제공자, 배심원, 법원과 법집행공무원에 관한 정보가 알려져서 피해를 입을 가능성이 생기는 것이다. 예를 들어 정보수집 및 검색기술을 가지고 범죄의 의도를 가진 자가 법원 및 법집행기관의 기록에 접근하여 익명으로 된 사건의 피해자나 증인을 알아낼 수 있게 된다. 법원의 기록이 개인정보를 가명이나 익명으로 하여 처리하더라도 다른 정보와 연결할 경우 피해자나 증인을 알아낼 수 있는 것이다. "하나 또는 여러 정보를 함께 고려하고 정보의 맥락과 수집경로 등을 개인을 식별하고 특정하는 데 충분하다." 개별적으로는 무의미한 정보가 사법정보시스템에 의하여 공유되고 통합됨으로써 정보의 결합과 새로운 정보의 가공을 가능하게 함. 법원의 정보에 이름과 나이만 있어도 경찰기록에서 운전면허번호와 인종이 기록된 내용과 결합하면 개인을 식별할 수 있게 되어 그 피해자와 증인을 알아낼 수 있게 된다.

(2) 잘못된 또는 불완전한 정보의 기록으로 인한 위험

부정확한, 불완전한 또는 정보기록이 다른 사람에 연결된 경우 피해가 발생할 수 있다. 예를 들어, John H. Doe라는 사람을 체포하면서 John N. Doe라는 인물로 기록하면, 무고한 사람이 피해를 입게 된다. 그 피해는 직장을 잃거나 일자리를 얻을 수 없게 되는 등 상상 이상이다. 2005년 플로리다에서는 성범죄자의 잘못된 주소가 수백 번 텔레비전에 방영됨으로써 어느 부부가 안전에 위협을 받았다. 더 심한 경우는 텍사스에서 남자 4명이 27살 먹은 정신지체장애인을 심하게 폭행한 사건인데, 그 이유는 그 장애인의 주소지가 아동학대자가 사는 주소지로 텍사스 주의 인

터넷명단에 등록되어 있었기 때문이었다고 한다.

이러한 불완전한 정보는 책임의 문제를 야기한다. 특히 성범죄자의 명단을 하나의 포털로 연결하는 정부정책은 이러한 문제를 더욱 크게 한다. 여러 주가 함께 구축하여 일반인이 접근할 수 있는 사이트로서 어떠한 다른 사이트와 비교를 허락지 않는 내용을 가지고 주의 정보에 접근하는 진입로가 될 수 있다. 주마다 다른 공개 기준을 가진 경우는 문제이다. 정보에 접근하는 공중은 명단에 포함된 사람들이 재범죄 가능성이 낮은지 높은지를 알 길이 없다.

불완전한 정보의 문제는 정보를 판매하는 경우에 더욱 심각하다. 주가 부정확한 또는 불완전한 정보를 정보회사에 판매하는 경우 이미 주가 통제할 수 있는 범위 밖으로 나간 정보를 어떻게 정정할 수 있겠는가? 사법정보시스템을 통하여 부정확하고 불완전한 정보를 공유하여 개인이 피해를 입는 경우 누가 책임을 지는가? 미국 법무부 자료에 의하면 오하이오주에서 어떤 사람의 사회보장번호가 범죄인의 것으로 기록된 경우가 있었다고 한다. 그 오류가 시정되었을 때는 이미 개인정보회사에 판매되고 전국적으로 유포된 이후였다. 이미 정보가 판매되어 그 사람은 직장과 가정을 잃게 되었다.

(3) 내부자의 불법사용의 문제

정보관리기관의 내부에서 공적인 또는 비(非)공적인 정보에 접근할 수 있는 사람에 관련된다. 2002년 12월 미연방Drug Enforcement Administration의 요원인 Emilio Calatayud는 기관의 컴퓨터에 저장중인 정보를 외부 정보회사에 판매한 대가로 22,500달러를 받은 혐의로 징역과 벌금형을 선고받았다. 이러한 경찰 또는 법원서기가 피해자의 소재를 알아내려고 정보에 불법적으로 접근하여 폭력분쟁에 휘말릴지 않도록 할 장치가 무엇인가?

"전국적으로 상호 연결된 네트워크와 통신체계에 의존하는 것은 내부자의

활동으로부터 발생하는 위험을 증가시킨다. 더욱이 단 한사람의 내부자로 인하여 기관의 데이터, 체계, 기업활동 평판 등에 광범위하고 회복하기 어려운 피해를 유발할 수 있다"[75]

(4) 동일성 도용(Identity Theft)의 위험

예를 들자면, 법원에서의 이혼절차기록에 주소, 생일, 신용정보, 사회보장번호, 배우자와 자녀정보가 포함된다. 범죄자들이 정보기록을 통째로 사거나 인터넷을 통하여 입수함으로써 이 정보에 합법적으로 접근할 수 있다. 이 정보를 이용하여 신용카드를 발급받거나 대출을 받을 수도 있다. 이러한 사건은 미국 외의 지역에서 발생할 수 있으며, 러시아 마피아가 최근에 부쩍 활개를 치고 있다는 점도 염두에 둬야 한다.

(5) 청소년기록에 대한 접근의 위험

과거 청소년들의 기록 보호에 많은 수단을 동원하였으나, 최근 정보공유기술의 발달로 인하여 정보에 대한 침해가 심해지고 있다. 아이오와(Iowa)주에서는 최종적인 결정이 어떠했는지에 상관없이 10세 이상의 개인이 포함된 모든 사건의 정보기록이 무료 또는 유료로 제공되었다. 14세 소년이 차량절도혐의로 기소되었으나 무죄평결을 받은 사건기록도, 최종결론이 아니라 기소되었다는 사실에 기초하여 잠재적 또는 장래의 고용주가 볼 수 있는 상태에 놓인다(preemployment check). 기술의 발전으로 볼 때 장차 별 노력없이도 고용주가 이러한 정보를 볼 수 있게 될 것이다. 이렇게 되면 평범한 직장을 구하려 할 때도 이러한 정보검색을 거치지 않으면 안되게 될 것이다.

기소되었으나 유죄평결을 받지 않은 사건은 고용에 영향을 주지 않도록 보호되어야 한다. 그러나 정보가 광범위하게 이용될 수 있으므로 법령을 시행하고 차별여부를 입증하는 것은 어려움이 있다.

(6) 폐쇄된 또는 파기된 기록의 위험

75) U.S. Secret Service. Insider Threat Study

기소되었으나 무죄로 결정된 경우 그는 사회적 지위의 상실, 기용기회 상실, 대출거부 등의 불이익을 입지 않도록 형사기록의 파기를 요구할 수 있다. 그러나 정보가 기관간에 공유되고 정보사업자에게 판매되고 인터넷에 공개되면 형사기록을 파기한다는 것은 불가능해진다. 과거에는 기록의 파기는 파일과 자료의 파기를 의미하였지만 이제는 기록은 전자적인 것이어서 세계 어느 곳에서도 접근할 수 있으므로 과연 국가가 무고한 개인을 보호할 수 있을 것인가? 과연 이제 기록의 '파기'란 무엇을 의미할 것인가?

마찬가지로 유죄평결을 받고 일정 기간 복역하고 재범을 하지 않고 일정기간이 경과한 경우 기록의 폐쇄를 요청할 수 있다. 직업을 얻는 데 장애가 될 수 있기 때문이다. 그러나 이미 다른 기관과 외부에서 공유하고 있는 상황에서 과연 어떻게 기록을 폐쇄할 것인가? 고용, 주택대출, 그 밖의 서비스를 받는 데 차별의 근거가 된다면 근본적인 사법시스템에 대한 의문이 제기될 수 있다. 입법자의 의도가 그러한 범죄인들이 복역 또는 원상회복을 해 준 뒤 일정기간이 경과한 뒤에까지 그러한 피해에 노출되도록 한 것은 아니잖는가?

3) 정보공유·통합시스템의 운영사례

물론 9·11사건 이전에도 국세청은 납세자의 자산, 운전경력, 전화번호 기타 개인통계자료를 수집하여 왔다. FBI와 경찰관(U.S. Marshall)은 몇 가지의 키워드만 가지고 자동차, 운전자, 선박기록에 접근할 수 있으며, 담보권(liens), 양도기록(deed transfer), 전화번호, 군인인사기록, 선거인명부(voter rolls)까지도 알 수 있다. 정보공유에 대한 요구는 연방정부에서 테러리스트정보인식시스템(Total Information Awareness Proposal(Terrorist Information Awareness)), 탑승객사전검색시스템(Computer Assisted Passenger Prescreening System(CAPPS II))을 통하여 전국적으로 정보의 수집, 분석, 공유를 추구하게 된다.

정보의 수집과 통합을 하는 기관들로는 연방통계국(U.S. Census Bureau), 연방범죄종보센터(National Crime Information Center(NCIC))[76], 내국세청(IRS), 사회보장청(Social Security Administration), 자동차청(State motor Vehicle Administration) 등이 있다.

정보공유·통합시스템으로는 TSA의 CAPPS II, FBI의 Carnivore system(DCS1000로 명명됨), 테러리스트정보 인식시스템(Terrorist Information Awareness System(TIA)) 등이 있으나 이들 시스템에서는 그 원정보(raw data)가 공적책임을 거의지지 않는 기관이나 기업의 통제를 받게 되거나 그럴 가능성이 있는 경우가 있다.

CAPPS II는 정부와 상업용 데이터베이스가 보관중인 정보를 신속하게 검색하여 비행기 탑승승객의 위험도를 적색, 황색, 녹색으로 분류하며 안전검색의 정도(level of security scrutiny)를 결정한다. 문제 없는 경우 녹색으로 정상적인 검색이 이뤄지며, 황색은 잠재적 또는 알 수 없는 위험요소를 나타내며 짐 또는 신체 검색이 강화된다, 적색은 법집행공무원들이 여행을 허가하기 전까지는 탑승 안되는 단계이다.[77]

FBI의 Carnivore는 인터넷서비스사업자를 통하여 인터넷접속 및 이메일 수발신 상황을 모니터하고 있으며, 이전에는 TIA에 의하여 신용카드, 고용, 의료, 인터넷서비스제공자 정보 등으로 계속 저장하여 제공하도록 요구되었다. 그러나 의회는 TIA가 공적 책임성(public accountability)을 결여하였다고 판단하여 국방부, CIA와 법무부가 사업의 프라이버시 문제와 시스템의 작동범위를 명확히 하기 전까지는 보급 및 시행을 금지하기로 하였다. 연방 상원은 CAPPS II 사업에 대해서도 유사한 보고서를 요구하였다.

프라이버시에 대한 침해는 국가권력에 의해 거대하게 침해되는 것이 아

76) 중죄(felony) 또는 중한 misdemeanor를 범한 범죄인 리스트, 64,000여의 연방 또는 주 정부기관 및 외국기관의 정보를 수집 보관한다.

77) GAO REPORT to Congressional Committees on Aviation Security: Compyter-assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385, p. 7.

니라 이제는 슬금슬금 이뤄지며, 사적 회사에 의한 침해가 더욱 중요하게 부각되고 있다고 지적된다.[78]

정보의 공유는 단순히 정보를 교환하는 것을 넘어서서 정부는 사람들이 인터넷에서 무슨 책을 사고 읽는지, 지불은 어떤 방식으로 하는지, 여행 예약, 전화와 이메일, 의료 및 은행거래기록 등에까지 관심을 갖는다.[79] 이러한 정보의 통합과 공유를 통하여 사람들은 점차 감시를 받게 된다. 정보시스템에 따라서 그러한 감시는 악용될 수 있다.[80] L.A.의 한 경찰관은 사회유명인사의 법집행관련 경찰서의 컴퓨터기록을 언론에 수백차례 판매한 사례도 보고된다.[81] 뉴햄프셔주 대법원은 스토커(Liam Youens)에 의해 살해(1999. 10. 15.)당한 한 여자(Amy Boyer)의 가족이 스토커가 피해자의 소재를 알아내기 위하여 고용한 인터넷정보판매업자를 상대로 제기한 소송이 주법상 적법한 것이라고 판결하였다.[82] 정보가 통합되면 통합될수록 공개로 인한 위험은 그만큼 더 커진다. 물론 정보의 통합과 공유가 반드시 한 개인에 관한 정보의 오류나 왜곡을 초래한다고 단언할 수는 없다.[83]

---

78) Privacy Schmrivacy? Drafting Privacy Policy In An Integrated Justice System(and Why It's Important), p. 7. Illinois Integrated Justice Information System(IIJIS)에서 2004. 6.에 펴낸 자료.(http://www.icjia.state.il.us 참조). 일리노이주의 사법정보통합시스템(Illinois Integrated Justice Information System(IIJIS))은 Illinois Executive Order No. 16(2003)에 근거한다.

79) Jim McKay, Big Brother:Is He Watching You?, Government Technology, Apr. 2003(http://www.govtech.net/magazine/story.phtml?id=45918)

80) CNN의 2003년 5월 19일 보도에 의하면 로스엔젤레스에서 어떤 사설탐정이 그가 싫어하는 야구코치의 뒷조사를 위하여 불법적으로 컴퓨터기록을 뒤진 일이 있었다고 한다. http://www.cnn.com/2003/US/West/05/19/police.corruption.ap/

81) http://www.usatoday.com/tech/news/2003-04-09-policy-celebrity_x.htm

82) Remsburg v. Docusearch, Inc., 816 A.2d 1001(N.H. 2003); Peter Page, Internet Data Seller Can Be Sued in Stalking-Murder Case, LAW.COM, Mar. 10. 2003. (http://www.law.com/jsp/article.jsp?id=1046833530025)

83) Paul F. Kendall et al., Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use, 21st Annual International Conference on Data Protection and Information Privacy, Hong Kong 7-8(Sept. 1999) (http://www.pco.org.hk/english/infocentre/files/kendall(formatted).doc) (2006. 12. 24. 검색)

4) 프라이버시 보호를 위한 정책결정의 고려사항

이러한 사법정보통합작업을 하는 데는 비단 공공의 안전만 내세우는 것이 아니라 프라이버시 보호, 안전성, 공개소송회피 등을 고려하기 마련이다. 일리노이, 미네소타, 위스콘신 주 등은 민감하고 개인적인 정보를 보호하기 위한 체계적 방안을 모색하고 있다.

이러한 구상에서 고려되어야 할 주요사항은 다음과 같다.

①사법정보공유구상에서 프라이버시보호정책을 발전시키기 위한 통합적 절차를 수립함.

②개인정보가 위험에 처해질 수 있는 취약요소와 지점을 확인함.

③사법정보공유구상에서 위험성이 있다고 생각되는 프라이버시 보호법제를 검토함.

④사법정보통합구상을 관할하는 전국적인 프라이버시보호원칙을 마련함.

⑤다양한 맥락과 환경에서 정보를 보호하는 프라이버시보호정책을 발전시킴.

⑥책임을 강화하고 전국적인 최저한의 보안기준을 마련함.

통합사법정보시스템에서의 프라이버시 보호는 앞에서 언급한 바와 같이 목적특정, 수집제한, 정보의 질, 사용제한, 보안성, 관리공개, 당사자참여, 책임성의 원칙 등 개인정보보호의 원칙에 입각하여 이뤄져야 한다.

(1) 정보의 보존과 파기(life cycle)

종이문서는 보관에 한계가 있어서 현실적인 필요에 의해 보존기간을 정하였으나, 컴퓨터에 의한 정보저장은 사실상 무한한 저장능력을 제공함에 따라 저장과 파기가 프라이버시보호의 중요한 주제가 된다. 현재의 문서파기관련 법령을 형사사법정보통합시스템에 적용할 경우 법령의 적용 예

외가 되는 범죄기록들이 상당수 있을 수 있다는 점이 지적된다. 이 쟁점에 관하여 다음이 고려되어야 한다.

①기록을 봉인(폐쇄)할 경우 통합정보시스템에서 정보이용의 가능성에 어떤 영향을 미치는가?

②기록의 파기는 통합정보시스템에서 정보이용의 가능성에 어떤 영향을 미치는가?

③기록은 정말 파기될 수 있는가?

④통합정보시스템이 보유하는 정보의 2차적 유포에 관하여 적절하게 공지하고 있는가?

⑤정보가 한 번 공개되면 영원히 공개되는 것이 되므로, 공적 기록을 얼마 동안 보유할 것인가?

⑥정보의 보존과 파기원칙은 공적인 것이 아닌(non-public) 정보의 보유에 더 잘 적용할 수 있는가?

(2) 정보에 대한 개인의 접근권

자신에 관한 정보에 접근할 권리가 보장되어야 한다. 당사자의 정보에 대한 접근가능성을 판단하는 프라이버시위원회가 필요하다. 이 쟁점에 관하여 다음이 고려되어야 한다.

①얼마나 신속하게, 얼마나 자주 시스템이 정보주체가 요구하는 정보를 제공하는가?

②어떠한 형식과 방법으로 정보가 제공되는가?

③시스템에 저장중인 정보의 어느 정도가 개인과 관련되어 있다고 생각하는가?

④이러한 정보에 정보가 어떻게 활용되고 있는지, 활용되고 있기는 한지, 누구에게 공개되는지 등에 관한 내용을 포함하는가?

⑤잘못된 정보를 정정하는 행정기준은?

(3) 사법정보시스템의 책임성

사법정보시스템이 포함하는 정보가 적절하지 않게 유포될 경우 직업상실, 사회적 지위저하 등 위험이 있다. 그 궁극적인 위험은 결국 공중이 지게 되므로 시스템은 프라이버시정책에 걸맞는 책임확보장치를 마련해야 한다. 이 쟁점에 관하여 다음이 고려되어야 한다.

①정보공개법(FOIAs)이 통합사법정보시스템의 운영에 어떠한 영향을 미치는가?

②연방헌법 수정 제1조와 커먼로(common law)에 의한 법원기록 접근이 통합사법정보시스템에 어떠한 영향을 주는가?

③통합사법시스템이 보유하는 정보에 공중이 접근했다고 추정할 근거가 있는가? 있다면 그러한 추정은 어느 정도까지 프라이버시 정책에 영향을 주는가?

④ 통합시스템이 프라이버시정책에 따르도록 하기 위해서는 어떠한 행정절차가 있어야 하는가? 개인은 구제절차를 밟기 전까지는 피해를 감수하여야 하는가?

⑤피해당사자는 피해를 구제하기 위하여 다른 어떠한 수단을 취할 수 있는가?

(4) 통계정보의 이용가능성

통합시스템은 쉽게 통계정보를 만들 수 있다. 체포건수, 기소건수, 평결건수, 석방 및 선고형량, 재범율 등 통계가 쉽게 만들어진다. 이 경우에도 다음 사항이 고려되어야 한다.

①통합시스템이 이러한 처리능력이 있는지, 없다면 그러한 처리능력을 갖도록 해야 하는지?

②시스템이 이러한 통계를 처리할 수 있다면 이러한 보고서의 내용으로 공개될 것인지 아닌지가 결정되어야 한다.

(5) 피해자, 증인에 관한 정보의 접근가능성

대개의 형사사건의 경우 형사피해자는 신체의 안전에 대한 중대한 필요

가 있다. 안전을 확보하기 위하여 어떠한 범죄피해를 당하였는지나 주소와 상담내역 등을 비밀로 하는 등 광범위한 구제수단이 강구되어야 한다. 프라이버시가 침해될 경우 범죄피해자를 법적으로 보하기 어려워진다. 경찰수사기록, 법정 심리내용, 피해배상자료, 피해진술 등을 누가 보지나 않을까 하는 염려 때문에 범죄피해자가 당국에 신고하거나 형사절차에 참가하지 못한다. 따라서 이 경우에 다음 사항이 고려되어야 한다.

①범죄피해자에 관한 정보를 수집하는 목적은 뭔가?

②가해자 또는 일반인들에게 정보가 공개되면 범죄피해자와 그 가족이 무슨 해를 입을 것인가?

③위험이 있는데도 이런 정보를 기록해야 하는가?

④특정기관의 임무수행을 위한 정보라면, 어떤 정보가 기록되어야 하며, 어떤 방법으로 공유되어야 할 것인가?

(6) 가해자와 피해자의 건강정보에 대한 접근가능성

사법정보시스템이 수집한 건강정보는 다른 경우라면 비밀이 되는 진료 및 정신건강에 관한 정보를 포함한다. 이 기록에는 피해자의 HIV 바이러스 감염 여부에서부터 가해자의 의료시설 입원기록까지 포함될 수 있다. 프라이버시 정책결정에는 피해자와 가해자의 이에 관한 기록들이 수집·공유되는 데 적절한 목적을 반드시 가지도록 해야 한다.

(7) 사회보장번호의 수집, 사용, 배포

정보는 정보를 낳는다. 사회보장번호는 그 자체로 아무 것도 아니지만, 금융정보, 교육정보, 의료정보 등 다른 정보에 접근하는 중요한 정보가 된다. 최근 들어 동일성 도용의 예가 많이 발생하고 있다. 수집목적의 범위 안에서만 사용되어야 한다.

5)소결

통합사법정보시스템에서 프라이버시권을 보호하기 위해서는 개인정보보

호의 원칙이 관찰될 수 있도록 하여야 한다. 특히 기관간 정보를 공동이용하는 것이므로 다른기관이 정보를 본래의 수집목적에 한정하여 최소한만 사용하도록 하여야 한다. 즉 정보공유에는 정보수집 및 사용의 목적특정의 원칙이 특히 중요하다.

공동사용되는 정보가 특정된 목적을 벗어나는 것인지 여부를 판단하기 위하여 미국 법무부는 프라이버시정책 가이드라인에서 목적특정의 원칙에 관하여 다음 지표를 제시하고 있다. 우리의 경우에도 참고가 될 만한 내용이라 생각된다.

①정보공유에 관한 법령(legal provisions)이 있는가? 어떤 기관과 정보를 공유하고 또 어떤 기관과 정보를 공유하지 않는가?

②주 헌법, 법령, 판례, 법령해석에서 기관이 보유하는 정보의 공개와 일반인의 정보에 대한 접근의 범위에 대해 언급하고 있는가?

③일반인의 정보접근에 대한 법집행의 예외가 있는가? 있다면 그 예외의 범위는 얼마나 넓은가? 어떤 유형의 정보에 대해 예외가 적용되는가?

④예를 들어 체포나 유죄평결과 같은 특정유형의 정보에 대해 어떠한 예외가 인정되는가?

⑤정보의 특정한 사용에 관한 어떠한 법적 예외가 있는가? 배경조사(background check), 고용을 위한 정보조회(preemployment check)나 비사법적(非司法的) 사용을 위하여 정보를 제공하는 것에 관한 법률규정이 있는가? 추가공개를 금지하는 조건으로 정보가 공개되는 예가 있는가?

⑥일반인이 다른 기관보다 법원의 정보에 접근하기가 더 용이하도록 규정이 되어 있는가? 이러한 규정은 언제 적용되는가? 사건처리과정에서 언제 다른 기관의 사법정보가 법원의 정보로 도입되는가?

⑦정보중개인(information brokers) 또는 제3자에게 정보판매를 허용하는 규정이 있는가? 대량이전(transfer)이 허용되거나 금지되는 특정영역 또는 유형이 있는가? 정보중개인에게 이전된 정보의 사용을 통제할 수 있는가?

⑧기관이 보유하는 정보에 접근하려는 이의 신원을 확인하는 수단은 무엇인가? 정보를 공유한 사람이나 기관의 기록을 보관하는 수단은 무엇인가?[84]

84) U. S. Department of Justice, Bureau of Justice Assistance, Privacy Policy Development Guide, Washington D.C.:2006.

2. 우리나라 형사사법정보통합체계구축사업의 몇 가지 문제점

가. 사생활의 비밀과 자유 및 정보자기결정권의 침해

1) 사생활의 비밀과 자유

헌법 제17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.”고 규정하고 있다. 사생활의 비밀과 자유 또는 프라이버시권은 그리 오랜 역사를 가진 것은 아니다. 미국의 Thomas M. Cooley가 프라이버시권을 ‘홀로 있을 수 있는 권리(right to be let alone)'로 이해한 이래 이러한 견해는 Warren과 Brandeis의 공동논문에서도 확인된다. 이러한 프라이버시권은 국가권력에 의한 사적 영역의 침해의 중지 또는 배제라는 소극적 측면의 권리이다. 자신을 드러내지 않을 권리, 자신에 관한 정보를 말하지 않을 권리 또는 이것이 침해될 경우 그 방어 또는 침해배제를 구할 권리의 문제가 된다.

그러나 오늘날 프라이버시권의 문제는 단순한 드러내지 않을 권리라는 소극적인 측면에만 국한되지 않는다. 자신의 의사와 상관없이 사생활에 관한 부분이 파악되고 유통되는 지경에 이르렀으며, 특히 놀라운 컴퓨터 기술의 발전에 따라 개인정보의 대량수집과 처리 및 유통이 가능해지게 되었기 때문이다. 특히 과거 개인에 관한 정보가 단편적으로 수집되고 일부분만 통합되어 파악된 반면 컴퓨터를 이용한 정보처리기술의 발전은 각종의 정보를 종합하여 처리할 수 있도록 해 줌으로써 이제 바야흐로 개인의 일거수일투족을 감시당할 지경에 이른 것이다. 결국 개인의 사생활의 비밀과 자유를 누린다는 것은 단순히 소극적인 차원에만 머무는 것이 아니고 이제 적극적으로 자신에 관한 정보를 통제하는 것을 포함하지 않으면 안 되게 된 것이다. 즉, 누가 언제 어디서 자신에 관한 정보를 수집·보유·활용하고 있는지, 즉 자기에 관한 정보의 흐름을 통제할 수 있는 권리로 이해되지 않으면 안 되는 것이다.

이러한 문제는 미국의 컴퓨터연결 및 프라이버시보호법(1988년)의 제정과정에서도 드러난다. 이 법은 프라이버시보호법(1974년)을 대체한 입법[85]인데, 연방 및 주의 기관의 컴퓨터를 상호 연결함으로써 연방정부의 지불과오의 발견, 차금징수의 증대, 사회보장사기의 색출 등의 효과를 의도하고 이로써 연방정부의 예산절감을 추구하고 있다.[86] 그러나 이러한 컴퓨터 연결사업에 대하여 제기되는 비판은 첫째, 소규모 정보도 필요에 의하여 연결되면 개인의 프라이버시를 위협할 수 있으며, 둘째, 목적을 특정하여 수집된 개인정보가 다른 국가기관의 공유 등 유통에 대한 통제의 기회도 부여되지 않은 채 다른 용도로 당연히 사용되게 된다는 점이다. '정보공유'의 확대는 당초 정보가 수집되면서 특정된 목적을 넘어서서 정보가 사용된다는 것을 말한다. 비유하자면 첩보에 불과한 것이 정보가 연결됨으로써 새로운 정보로 가공되는 것을 의미한다. 이는 정보주체가 동의하지 않은 새로운 정보의 수집이라고 할 수 있을 것이다. 이러한 상황은 사생활의 비밀과 자유의 문제가 자신에 관한 정보의 적극적 통제에 밀접하게 관련되어 있음을 뜻하게 된다고 할 수 있다.

특히 현대 정보사회에서는 그 중요성이 더욱 부각된다. 이 권리와 관련해서는 국가권력 등 공권력에 의한 침해뿐 아니라 사인에 의한 침해도 매우 중요하게 부각된다. 법률에 합치되고, 국가안보, 공공의 안전 또는 국가의 경제적 복리, 질서유지와 범죄의 방지, 보건 및 도덕의 보호, 또는 다른 사람의 권리 및 자유를 보호하기 위하여 민주사회에서 필요한 경우 이외에는, 이 권리의 행사에 대하여는 어떠한 공공당국의 개입도 있어서는 아니된다(유럽인권협약 제8조). "모든 사람은 사회 속에서 살기 때문에, 사생활의 보호는 필연적으로 상대적인 것이다. 그러나 권한 있는 공공기관은 동 규약에서 인정하는 사회이익에 있어 필수적인 경우에만 개인

85) 이에 대해서는 변재옥, 「입법소개: 1988년의 컴퓨터 연결 및 프라이버시 보호법」, 《미국헌법연구》 제1호, 1990, 33면.

86) 연방 보건교육복지부(Department of Health, Education and Welfare)가 주 복지수혜자 명부와 연방고용명부를 대조하여 불법으로 복지혜택을 받고 있는 범법자를 색출하기 위하여 컴퓨터 연결사업을 실시하였다고 한다. 변재옥, 앞의 글, 37면.

의 사생활과 관련된 정보를 요구할 수 있어야 한다."(시민적 및 정치적 권리위원회가 채택한 일반논평 16, 제32차 회기, 1988년)[87]

또한 이 위원회에서는 다음과 같이 언급하고 있다. "컴퓨터, 데이터 뱅크 및 기타 장치를 통해 개인정보를 수집하고 보관하는 것은 공공기관 또는 개인, 사설단체를 불문하고 반드시 법률로써 규제되어야 한다. 또한 어떤 개인의 사생활에 관한 정보가, 그것을 획득, 소지, 사용할 법률상 권한이 없는 자의 손에 닿거나, 동 규약에 부합하지 않는 목적으로 이용되지 않도록 당사국이 효과적인 조치를 취하여야 한다. 자신의 사생활을 최대한 효과적으로 보호하기 위해 모든 개인은 자신의 정보가 자동정보파일(automatic data files)에 저장되었는지, 저장된다면 어떠한 정보가 어떠한 목적으로 저장되었는지를 이해하기 쉬운 형식으로 확인할 권리를 갖는다. 모든 개인은 또한 어떤 공공기관 또는 개인 또는 사설단체가 그들의 파일을 관리하고 있는지에 대해 확인할 수 있어야 한다, 만약 그러한 파일이 부정확한 개인자료를 포함하거나 또는 법률에 위반하여 수집·처리되었을 경우 모든 개인에게 수정 및 삭제를 요청할 권리가 주어져야 한다."[88]

사생활의 비밀과 자유는 이러한 정보와 관련된 내용과 함께 주거 및 통신 등에서의 비밀과 자유도 보장한다. 어느 누구도 그의 사생활, 가정, 주거 또는 통신에 대하여 자의적이거나 불법적인 간섭을 받거나 또는 그의 명예와 신용에 대한 불법적인 비난을 받지 아니한다. 모든 사람은 그러한 간섭 또는 비난에 대하여 법의 보호를 받을 권리를 가진다.(시민적·정치적 권리규약 제17조) 그 본질은 개인이 간섭을 받지 않고 살 권리이다.

주민등록에서와 같이 강제적인 지문채취, 사진정보의 제공 등 국가권력에 의한 정보의 수집이 문제된다. 교통법규 위반과 관련하여 혈중알콜농도를 측정하기 위하여 혈액검사용 혈액을 채취한 경우나 친자확인을 위하여 강제로 샘플을 채취하는 등 강제적인 의학적 검사가 문제될 수 있다.

87) 시민적 및 정치적 권리위원회·고문방지위원회, 『유엔 인권조약 감시기구의 일반논평 및 일반권고』,국가인권위원회, 2006, 40면.

88) 시민적 및 정치적 권리위원회가 채택한 일반논평 16: 제17조 사생활에 대한 권리

성생활은 개인의 사생활에 속하지만, 미성년자와의 성행위, 동성애, 낙태 등에 대해서는 논란이 있다. 유럽인권위원회에서는 동성간 성행위에 대한 처벌문제에 관하여 그 제한의 정당성에 관한 부분을 협약당사국과 유럽의 의식변화를 고려하여 심리하고 있다. 한 예로 영국성범죄법에서 21세 이하(법적으로 동의를 요하지 않는 연령. 1994년에 18세로 함) 남성과의 동성간 성행위를 처벌한데 대하여 위원회는 '타인의 권리와 자유의 보호라는 관점에서 정당화하였다. 다만, 북아일랜드에서 남성간 동성애를 모두 금지하는 법률은 도덕의 보호나 타인의 권리와 자유의 보호를 위하여 민주사회에서 필요한 것이라고는 생각되지 않는다고 하였다. 성전환자에 대해여 법률상의 지위변화를 협약당사국이 거부한 경우 사생활을 존중받을 권리의 침해가 되는지에 대해 논란이 있다. 성전환자의 개명과 성(性)의 변경, 혼인의 권리 등이 문제된다.

수사과정에서 개인의 사생활이 드러나게 된다. 사무소 겸 주거로 사용하고 있는 곳을 저작권법위반으로 수색한 사건에 대하여 유럽인권위원회는 이 수사는 사생활을 간접적으로 침해하였으며, 이러한 간섭은 타인의 권리보호를 위하여 또는 민주적 사회의 필요가 있어야 한다고 하였다. 시위중인 사람을 사진촬영하여 개인사진을 증거자료로 제출하고 범죄와 관련된 서류, 사진, 지문 등 기록을 보관하는 것은 공공의 안전 및 무질서의 방지를 위하여 민주적 사회에서 필요가 있다고 보았다.

현대 정보사회에서 고도의 감시장비의 발달로 인하여 사생활에 대한 감시 가능성이 매우 높아지고 있다. 우편과 전화에 대한 감시는 법률에 의할 경우 일정한 경우 정당화될 수는 있어도 그것은 민주주의를 수호한다는 명분하에 민주주의를 해치고 위험을 초래할 수 있기 때문에 매우 엄격하게 해석되어야 한다.

어느 누구도 그의 주거 또는 통신에 대하여 자의적이거나 불법적인 간섭을 받거나 또는 그의 명예와 신용에 대한 불법적인 비난을 받지 아니한다.(시민적·정치적권리규약 제17조 제1항)

주거의 자유는 개인의 삶의 공간을 장소적으로 보호하기 위한 것이다.

주거란 가족의 생활공간인 주택뿐 아니라 사람이 거주하기 위하여 점유하고 있는 모든 건조물과 시설을 말하며, 주거를 둘러싼 정원 등도 포함된다.

통신은 우편이나 전신, 전화 따위로 정보나 의사를 전달하는 행위를 말하며, 그 수단은 이메일, 인터넷 등 다양하다. 유럽인권협약에서는 통신의 자유를 표현의 자유의 하나로 규정(“공공당국의 간섭을 받지 않고 국경에 관계없이 정보 및 사상을 주고받는 자유”)하고 있다. 비밀리에 전화통화를 도청하거나 녹음하는 행위는 이 권리의 침해이다. 이 점은 수형자의 경우에도 마찬가지이지만, 수형자의 권리를 법률에 의하여 제한하고, 일반인이 그 법률에 따라 자기의 행위에 대한 법적 판단을 예측할 수 있다면 그 법률에 의한 제한이 가능하다. 통신의 자유가 보장된다 하여 방송, 텔레비전 또는 영화 사업자에 대한 국가의 허가제도를 금지하는 것은 아니다. 또한 이러한 자유의 행사에는 의무와 책임이 따르므로, 법률에 의하여 규정되고, 국가안보, 영토의 일체성이나 공공의 안전, 무질서 및 범죄의 방지, 보건과 도덕의 보호, 타인의 명예나 권리의 보호, 비밀리에 얻은 정보의 공개 방지, 또는 사법부의 권위와 공정성의 유지를 위하여 민주사회에서 필요한 형식, 조건, 제약 또는 형벌에 따르게 할 수 있다.(동 협약 제10조 제2항) 개인에 대한 사회적 평가인 명예와 경제적 평가인 신용도 보호된다.

2) 개인정보자기결정권

오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다. 정보사회로의 이러한 급속한 진전에 직면하여 개인정보 보호의 필요성은 날로 증대하고 있다. 이러한 현실에서 사생활의 비밀과 자유라는 기본권

은 자기정보에 대한 통제권을 필연적으로 수반한다. 이러한 개인정보자기결정권은 헌법재판소의 판례에 의하면 “인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장되는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리”를 말한다. 이는 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리이며, 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보를 그 보호대상으로 한다. 그러나 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다고 해석된다. 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다(, 공보 105, 666, 672).”고 본다.[89] 국가권력에 의하여 개인정보자기결정권을 제한함에 있어서는 개인정보의 수집·보관·이용 등의 주체, 목적, 대상 및 범위 등을 법률에 구체적으로 규정함으로써 그 법률적 근거를 보다 명확히 하여야 하지만, 개인정보의 종류와 성격, 정보처리의 방식과 내용 등에 따라 수권법률의 명확성 요구의 정도는 달라질 수 있을 것이다. 일반적으로 볼 때 개인의 인격에 밀접히 연관된 민감한 정보일수록 규범명확성의 요청은 더 강해진다고 할 수 있다.

이러한 개인정보자기통제권의 보장을 위하여 공공기관의개인정보보호에 관한법률(이하 ‘개인정보보호법’이라 한다)에서는 제5조(개인정보화일의 보유범위)에서 “공공기관은 소관업무를 수행하기 위하여 필요한 범위안에서 개인정보화일을 보유할 수 있다.”고 하고, 제4조(개인정보의 수집)에서는 “공공기관의 장은 사상·신조등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의

89) 헌법재판소 2005.07.21, 2003헌마282 결정; 헌재 2005. 5. 26. 99헌마513 결정 등

가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.”고 규정하고 있다. 제9조 (개인정보의 안전성확보등), 제10조 (처리정보의 이용 및 제공의 제한), 제12조 (처리정보의 열람) 등을 규정하고 있으며, 아울러 정보주체의 열람 및 정정청구권도 인정[90]하고 있다.

3) 자기정보통제와 공공기관간의 정보공유

개인정보보호법 제9조 제1항에서는 “공공기관의 장은 개인정보를 처리함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성확보에 필요한 조치를 강구하여야 한다”고 하여 정보의 안정성을 확보하고 있다. 또한 정보의 수집목적에 그 이용을 제한하고 있으며 이 점은 제10조 제1항에서 “보유기관의 장은 다른 법률에 의하여 보유기관의 내부에서 이용하거나 보유기관외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니된다.”라고 한 것에서 나타난다. 다만 제2항에서 “1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우. 2. 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우. 3. 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우. 4. 통계작성 및 학술연구등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우. 5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우. 6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우. 7. 법원의 재판업무수행을

90) 제14조 (처리정보의 정정) ①제12조의 규정에 의하여 본인의 처리정보를 열람한 정보주체는 보유기관(다른 기관으로부터 처리정보를 제공받아 보유하는 기관을 제외한다. 이하 이 조에서 같다)의 장에게 서면으로 당해 처리정보의 정정을 청구할 수 있다. ②보유기관의 장은 제1항의 규정에 의한 정정청구를 받은 때에는 처리정보의 내용의 정정에 관하여 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다.

위하여 필요한 경우. 8. 기타 대통령령이 정하는 특별한 사유가 있는 경우"에는 보유기관의 장은 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있으나 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다고 규정하고 있다. 이러한 법률의 내용은 1981년의 OECD의 '프라이버시의 보호와 개인데이터의 국제적 유통에 관한 가이드라인'의 원칙을 충실하게 반영한 것이라고 평가된다. 이 가이드라인의 원칙으로는 수집제한의 원칙, 데이터 질의 원칙, 목적특정화의 원칙, 사용제한의 원칙, 안정보장의 원칙, 개인참여의 원칙, 책임의 원칙 등이다.

그러나 추진중인 형사사법통합정보체계는 이러한 개인정보보호법의 자기정보통제권 보장취지를 무색하게 하는 내용을 담고 있다. 이 사업의 법률적 근거로는 전자정부구현을위한행정업무등의전자화촉진에관한법률[일부개정 2006.10.4 법률 제8031호]을 들 수 있는데, 이 법률은 "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 목적"으로 하고 있으며, "행정기관의 주요 업무는 전자화되어야 하며, 전자적 처리가 가능한 업무는 특별한 사유가 있는 경우를 제외하고는 전자적으로 처리되어야 한다."(제8조 전자적 처리의 원칙)고 규정하고 있다. 또한 " 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."(제11조 (행정정보공동이용의 원칙))고 하고, "행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다."(제12조 (개인정보보호의 원칙))는 규정도 전자정부사업의 구체적 근거로 제시된다.

그러나 개인이 자기정보에 대한 통제권을 가지고 있고, 공공기관이 가지는 개인정보는 그 소관업무를 수행하기 위하여 필요한 것에 한정되며,

이를 다른 기관에게 제공하거나 공유하는 것은 특정한 경우에 한정되는데 반하여 이 법률은 그러한 구체적인 지정 없이 정보의 공유를 당연한 것으로 전제하고 있다. 그러나 개인정보의 종류 및 성격, 수집목적, 이용형태, 정보처리방식 등에 따라 개인정보자기결정권의 제한이 인격권 또는 사생활의 자유에 미치는 영향이나 침해의 정도는 달라지므로 개인정보자기결정권의 제한이 정당한지 여부를 판단함에 있어서는 위와 같은 요소들과 추구하는 공익의 중요성을 헤아려야 하며, 일반적으로 볼 때, 종교적 신조, 육체적·정신적 결함, 성생활에 대한 정보와 같이 인간의 존엄성이나 인격의 내적 핵심, 내밀한 사적 영역에 근접하는 민감한 개인정보들에 대하여는 그 제한의 허용성은 엄격히 검증되어야 할 것이며, 특히 범죄혐의 및 그 입증에 관한 정보는 매우 민간하고 중요한 개인정보이므로 그에 대한 자기정보결정권의 제한은 매우 중요한 공익적 요청이 있어야만 할 것이라고 생각된다. 또한 정보의 안정성 확보 역시 매우 중요하다. 자동화된 전산시스템으로 정보를 보유·관리하는 경우 정보에의 무단 접근, 정보결합, 정보전달, 공조에 의한 정보공유 등이 시공(時空)의 제한 없이 매우 손쉽게 일어날 위험성이 크므로 이러한 방식으로 처리되는 정보의 범위는 가급적 최소한으로 축소되어야 하고, 또한 보유기관은 그러한 위험으로부터 개인정보를 보호하는 일정한 조치를 취할 의무가 있다.

그러나 형사사법정보통합체계구축사업에서는 주로 소비자 또는 국민 중심의 행정, 국민을 고객으로 여기는 인식전환 등을 강조하면서 이 사업추진을 설명하고 있으나 이러한 이유는 매우 허구적이다. 이 사업에 의하여 구축되는 것은 경찰, 검찰, 법원 및 교정 등 국가의 사법기능을 수행하는 기관들이 보유하는 정보통합이며 그 통합에 의하여 편리함이나 이익을 얻는 것은 일반국민보다는 국가기관이라고 봐야 할 것이기 때문이다. 국민이 정보통합에 의하여 어떤 이익을 추가적으로 얻을 수 있을지는 파악하기 어렵다. “국민을 고객으로 여기는” 형사사법을 구축[91]하겠다고 하나 이 사업을 통한 주요고객은 법원이나 검찰이지 국민은 극히 부분적일

91) 국회의원 최규식이 주최한 “온 국민을 감시의 그물망에 묶어 두려는가?”(2006. 9. 26.)라는 제목의 정책토론회 발표집, 1면.

뿐이다. 이 점은 추진사업단에서 지적하는 현제도의 문제점에서도 드러난다. 여기에서 지적하고 있는 문제점은 첫째, 종이에 의한 형사사법업무수행, 둘째, 인력 및 시간낭비, 보안취약, 셋째, 체계적이고 통일적인 서비스 미비 등이다. 일반국민이 얻는 이점은 사건진행상황의 조회, 원활한 민원서비스 등인데, 이는 굳이 형사사법정보를 통합함으로써만 가능한 것은 아니다. 결국 정보주체의 정보를 통합하면서 내세우는 이유는 설득력이 없다.

또한 정보의 통합 또는 통합가능성은 단순히 정보의 통합을 넘어서서 새로운 정보의 수집 또는 가공이라는 의미를 가진다는 점에서 통합체계의 구축은 소관업무의 목적을 넘어서서 새로운 정보의 수집이라는 의미를 가지므로 별도의 법적 근거를 요한다. 전자정부구현을위한행정업무등의전자화촉진에관한법률은 전자정부구축을 위하여 원칙적인 정보공유를 규정하고 있을 뿐이지 정보주체의 정보통제권이라는 관점은 전적으로 결여되어 있다는 점에서 위헌적인 소지가 다분하다. '행정업무의 전자적 처리'를 통하여 '행정기관의 생산성·투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것'(제1조)이 그 입법목적이므로 정보의 단순한 공유를 넘어서 소관업무 이외의 정보를 열람할 수 있게 하고 나아가 통합된 정보의 분석을 통하여 새로운 사실의 파악까지 가능하게 한다면 이는 정당한 입법목적에 봉사하는 적합한 수단의 범위를 넘어서는 것으로서 수단의 적합성 또는 지나친 기본권의 침해를 초래한다는 점에서 피해의 최소성 요건을 충족하지 못하는 것이라고 생각된다.

나. 평등권의 침해 문제

형사사법 정보를 통합하는 경우 종이에 의한 사건관리를 전자화함으로써 인력과 시간 낭비 및 보안 문제를 해결할 수 있다고 한다. 검찰에서 경찰수사결과를 열람하고 법원이 검찰 및 경찰의 자료를 열람하는 데 드는 불편과 시간을 절약할 수 있는 장점이 있다고 설명된다. 그러한 효과

가 나타날 가능성은 존재한다. 그러나 이러한 편리성은 한편으로 그것이 편리한 것인 만큼 다른 측면에서 문제가 제기될 수 있다. 즉, 검찰이 경찰에서의 수사결과를 편리하게 열람·이용할 수 있고, 또한 법원이 검찰이나 경찰의 수사기록을 쉽게 열람할 수 있게 되는 데 반하여 검찰과 범죄성립 여부를 다투는 피의자 또는 피고인의 경우는 검찰이나 법원이 어떠한 자료를 보고 어떠한 심증을 형성하게 되는지를 알 수 없게 되어 자신에 대한 방어를 적절하게 하지 못할 수 있다는 점이다. 검찰과 경찰의 관점에서 작성된 사건기록 접근이 편리하면 편리할수록 법원은 검찰이나 경찰에 더욱 호의적이 되고 그 상대방인 피의자 또는 피고인은 적시에 방어권 행사를 할 수 없게 되어 더욱 불리해지는 것이다. 이 점은 전문증거에 관하여 반대심문이 불가능하다는 이유로 그 증거능력을 제한하는 취지와 같은 것이다.

이 점은 영장발부과정에서도 마찬가지이다. 영장의 발부는 법원이 피의자를 직접 신문하여 하므로 검찰과 당사자가 법정에서 영장 발부에 관하여 다퉈야 한다. 그러나 영장발부에 필요한 서류를 온라인으로 제출한다는 것은 피의자에 대하여 검찰의 정보에 대한 접근가능성을 보다 용이하게 함으로써 피의자의 방어권행사에 어려움을 초래할 가능성도 내재되는 것으로 보인다.

다. 국가기관간 권력분립의 문제

전자정부 구축을 위한 정보체계의 통합은 공공기관을 분립시켜 그 업무를 수행하도록 한 구성원리와 합치하지 않는다. 법원은 검찰과 당사자의 주장에 대하여 독립된 지위에서 재판을 담당하는 국가기관이다. 통합정보체계의 구축으로 법원이 검찰이 가진 정보를 쉽게 열람·이용할 수 있다면 검찰이 기소하고 법원에서 공방이 이뤄지는 법정중심주의 재판과는 거리가 생기게 된다. 현재의 법원의 재판과 관련하여 말하자면 통합정보체계는 현재의 방식을 넘어서서 별도의 장점을 가진 것이라고 보기는 어렵다.

제 5 장 결 론

1. 정보인권의 관점에서 전자정부사업에 대한 치밀한 법적 검토가 필요하다.

가. 개인정보 보호의 문제

전자정부 사업은 이를 통하여 행정의 투명성·효율성·민주성을 확보하고자 함이다. 국민의 관점에서는 보다 삶의 질이 향상되고 편리하며 기본적 인권이 보장되는 상황을 위함이다. 나아가 국민주권주의를 실현하는 길이어야 한다.

그러나 앞에서 살펴본 바와 같이 형사사법정보체계를 포함한 전자정부 사업의 추진과정에서는 그 사업 자체의 문제뿐 아니라 모든 사업의 전제라 할 수 있는 개인정보보호에 근본적은 문제가 제기된다. 공공기관 홈페이지에 들어 있는 개인정보가 검색엔진에 무방비 상태로 노출되어 있다는 보도는 충격적이다.[92] 심지어는 스스로 '국가과학기술 기밀유지에 관한 내용이어서 대외비'라고 밝힌 문서조차 검색이 가능한 상태이다.

공공기관이 가지는 개인정보가 일반인들이 사용하는 검색엔진에 의하여 쉽게 유출될 수 있는 수준의 보안상태라면 전자정부의 역점사항이라 할 수 있는 정보의 공동이용이라는 문제는 더욱 심각한 상황을 초래할 수 있기 때문이다. 정보관리의 보안성이 확보되지 않고, 보호되어야 할 개인정보가 무엇인지에 대한 의식이 낮은 상황에서 적극적으로 추진되는 사업은

92) 《한겨레》 2007. 1. 29.자 「공공기관 온갖 정보 줄줄 흘린다」라는 제목의 보도에 의하면, 검색사이트 구글을 통하여 공공기관의 개인정보 노출사례가 5400여 건이 확인된 것으로 나타났다. 여기의 공공기관에는 청와대를 포함한 정부 중앙부처, 입법·사법기관, 지방자치단체, 각급학교, 의료기관 등 452곳에 달한다고 한다. 이에 대해 한 보안전문가는 "관리자가 작업을 하면서 일시적으로 보안을 해제했거나 홈페이지 시스템이 허술해 보안이 설정되지 않았기 때문"이라고 분석하고 있다.

개인정보보호에 더욱 취약할 수밖에 없을 것이다.

이러한 국민의 정보인권이 고려되지 않는다면 이 사업은 엄청난 국가예산을 들여 기술개발과 운영을 맡게 될 기업의 매출신장에만 기여할 뿐 국민의 기본적 인권에는 오히려 악영향만 줄 가능성이 높은 것이다.

나. 공공기관간 정보의 공유와 기업과의 공유 문제

공공기관과의 정보 공동이용은 점차 공공기관이 보유하는 정보를 절실하게 필요로 하는 기업에게도 공동이용될 여지가 존재한다. 현재 정보통신망 이용의 상황은 금융기관, 전자상거래 업체 등 민간기업이 엄청난 개인정보를 보유하고 있다는 것이며, 특히 기업전산망의 보안이 문제될 경우 보유하고 있는 개인식별자를 통하여 광범위한 정보의 수집과 이를 통한 정보의 유출을 걱정하여야 한다.

2. 행정정보의 공동이용법률안의 내용수정이 필요하다.

전자정부사업의 하나로 추진중인 행정정보의 공동이용은 그 동안 정부기관이 다른 정부기관이 발행하는 증명서를 요구함으로써 발생했던 행정의 비효율과 비용의 낭비를 막는다는 점에서 긍정적이다. 그 동안 전자정부법에서 규정하던 것을 그 비중이 증가되어감에 따라 별도의 단행법률을 만들고자 법률안이 국회에 계류중이다. 행정정보공동이용 사업이 가지는 문제점은 크게 개인정보의 보호, 보유기관의 책임부담 등 여러 가지 문제점을 해결할 목적으로 마련하였다고 한다.

가. 개인정보의 보호

개인정보보호에 관한 부다 충실한 법제의 정비를 전제한다는 점은 아무

리 강조해도 지나치지 않는다. 정보의 공유가 확대되면 확대될수록 정보의 누설 위험성은 증가할 수밖에 없다는 것은 확실하다. 이 점에서 공동이용의 기본원칙으로 개인정보보호의 원칙이 명시되는 것이 좋다고 생각된다.

제7조 제3항에서 특정 개인을 식별할 수 없는 형태로 가공된 행정정보를 공동이용할 수 있다고 하나, 여러 정보를 종합하여 개인을 식별할 수 있을 경우에 발생하는 개인정보보호의 문제와 책임부담의 문제에 대해서는 명확한 규정을 두고 있지 않다. 또한 제9조의 공동이용의 제한과 관련하여 행정자치부장관이 공동이용을 승인하지 않을 사유가 상당히 광범위하게 정하여져 있는데, 추진 이유로 제시하듯이 종이 증명서의 제출로 인하여 불필요한 정보가 누출될 위험을 감소시키기 위한 정보공유라면 지나치게 판단의 여지를 넓게 두는 것은 오히려 종이증명서의 과도한 제출로 인하여 개인정보보호의 취지에 부합하지 않을 수 있다.

나. 공동이용의 승인주체

정보공동이용을 승인하는 주체가 행정정보의 보유기관이 아니라 행정자치부장관으로 되어 있다.(법안 제9조 제1항). 보유기관은 정보의 보유와 관리의 주체로서 정보의 누설로 인한 일차적인 책임을 져야 할 주체임에도 정보공유와 관련하여 협의만 할 뿐 결정의 실질적 권한이 배제된 점은 문제가 발생할 여지가 있다.

다. 정보주체의 확인

정보를 공동으로 이용하기 위해서는 증명서와 같은 형태로 서류를 제출하여야 했던 정보주체의 정보사용에 대한 요구가 있어야 한다. 그러나 정보주체와 정보이용을 요청하는 사람이 동일인진지를 확인하기 위해서는 많은 노력이 기울여져야 한다. 과거 인감증명의 발급을 위해서는 신분증,

인감도장을 가지고 행정기관에 출두하여 인영을 확인한 후 증명서를 발급받았으나 지금은 디지털 정보로 보관중인 인영을 출력하여 발급하므로 본인의 확인이 핵심적인 역할을 하게 된다. 그러나 신분증이 본인임을 확인하는 데는 한계가 있으므로 본인확인이 인감정보의 부정사용을 막는 핵심적인 역할을 하게 된다. 그러나 현재 채택하고 있는 전자적 방법에 의한 본인확인은- 이 자체도 문제가 제기될 수 있지만 - 예산상의 문제로 동사무소에 지문인식기가 설치되어 있지 않아 인감발급대장에 지문을 직접 채취하는 방식으로 이뤄지고 있어 개인정보자기결정권을 침해하고 있다.

3. 형사사법정보통합체계구축사업은 철저한 법적 검토가 필요하다.

형사사법통합정보체계구축 사업은 전자정부조성사업의 일환이며 대통령훈령에 근거를 두고 진행되는 사업이다. 법원, 검찰, 경찰과 교정에 이르는 형사사법정보를 큰 틀로 통합함으로써 형사사법업무의 표준화 및 전자화, 형사사법정보의 공동활용. 대국민 형사사법서비스의 품질제고 등을 그 목표로 한다고 한다. 그러나 형사사법정보통합체계구축사업은 특히 많은 문제를 안고 있으므로 철저한 검토가 필요하다.

가. 사생활의 비밀과 자유 등 기본권을 침해한다.

형사사법정보통합체계의 구축은 개인에 관한 정보의 통합을 통하여 개인정보가 통합관리될 가능성을 높인다. 이것은 사생활의 비밀과 자유를 제한하는 것이면서도 현재까지 법률적 근거를 찾을 수 없다. 특히 범죄를 범하여 피의자 또는 피고인이 된 자들뿐만 아니라 혐의가 없어 불기소되거나 무죄판결을 받은 경우, 사건의 수사·재판과 관련하여 진술을 한 참고인, 피해자, 증인 등에 관한 정보도 여과나 삭제가능성이 거의 배제된 채

집적될 가능성이 있다는 점은 더욱 심각한 문제이다. 소년범의 경우에는 범죄정보가 단기적으로만 의미가 있는 것이므로 장기적으로 범죄정보를 보관하는 것이 문제점으로 지적된다.

전자적 방법에 의한 정보의 공유와 통합이 이뤄지게 되면 재판과정에서 법원이 전자적 방법으로 잘 처리된 검사의 자료는 쉽게 접근할 수 있는데 반하여 피고인의 자료는 디지털화되지 않거나 재판과정의 공방을 통해 드러날 가능성이 있다는 점은 결국 법원을 설득할 기회가 불평등해질 가능성도 배제하지 못하므로 평등권에서도 문제가 발생한다고 생각된다.

나. 현재 전자문서를 형사재판과정에서 사용하기 어렵다.

전자문서가 문서로서의 보장적 기능을 수행하기 위하여는 진정성, 무결성, 신뢰성, 원본성을 확보하기 위한 기술적 수준에 이르러야 할 뿐 아니라 기존의 문서와 동일한 가치를 인정하는 법제도가 정비되어야 한다. 그러나 이에 대해서는 합의가 존재하지 않음은 물론 입법도 전혀 되어있지 않은 상태이다. 제도를 미리 구축해 두고 법적 근거를 뒤에 마련하면 된다는 사고방식은 법치주의의 관점에서 매우 위험한 것이라는 점은 두말할 필요가 없을 것이다.

다. 권력분립주의에 반할 소지가 있다.

법원은 검찰과 당사자의 주장에 대하여 독립된 지위에서 재판을 담당하는 국가기관이다. 형사사법정보통합정보체계의 구축으로 법원이 검찰이 가진 정보를 쉽게 열람·이용할 수 있다면 검찰이 기소하고 법원에서 공방이 이뤄지는 법정중심주의 재판과는 거리가 생기게 된다.

4. 전자정부사업의 법적 검토 필요성

이상에서 살펴본 바와 같이 전자정부사업은 효율성과 함께 부패통제를 할 수 있게 하고 민주주의의 실현에도 긍정적으로 기여하는 바가 크다.

하지만 현재 전자정부사업은 단기간에 법적 검토가 비비한 채 사업을 추진함으로써 국민의 기본적 인권의 침해를 수반한 여지를 매우 넓게 하고 있다. 특히 이 보고서에서 다룬 행정정보의 공동이용과 형사사법정보통합체계의 구축은 적지 않은 인권침해를 수반한다는 점에서 행정정보공동이용 과정에서 발생할 수 있는 기본권침해를 예방하는 법적 정비가 필요하며, 특히 형사사법정보통합체계구축사업은 법적 근거도 없으며 아직 전자문서가 재판과정에서 증거로 사용될 수도 없는 현실이므로 엄격한 법적 검토와 함께 사업전반에 대한 재검토가 이뤄져야 한다고 생각된다.

참 고 문 헌

감사원, 『전자정부 구현사업 추진실태 감사결과』, 2003. 6.

강경근, 『행정정보의 공동이용에 따른 법적 과제』, 한국법제연구원, 2001.

권태웅, 「미국의 전자정부법제와 추진전략」, 《법제》 통권 제554호, 법제처, 2004.

김성태, 『전자정부론』, 법문사, 2004.

김일환, 「미국의 개인정보보호법제에 관한 연구」, 《미국헌법연구》 제10호, 1999.

김일환, 「행정정보의 공동이용으로부터 정보자기결정권의 보호에 관한 헌법상 고찰」, 《공법연구》 제32집 제4호, 2004.

김준한, 「공공부문 기업정보의 공동 활용에 관한 연구」, 《한국행정연구》 1998년 겨울호(제7권제4호).

경건, 「전자정부구현을 위한 법제 동향과 과제」, 2000.10.24. 한국법제연구원 워크샵발제문.

국가인권위원회, 『금융기관과 인터넷에서의 개인정보 공유현황 실태조사』, 2003.

김승환, 「전자주민카드제도의 위헌성」, 《민주법학》 제13호, 1997.

김희수, 「형사사법 통합정보체계 문제점」, 국회의원 최규식 주최 정책토론회 자료집 “온 국민을 감시의 그물망에 묶어 두려는가?”(2006. 9. 26.) 발제문.

변재옥, 「입법소개: 1988년 컴퓨터연결 및 프라이버시보호법」, 《미국헌법연구》 재1권, 1990.

서유창, 「개인정보보호법 제정배경과 시행성과」, 《수사연구》 1996년 4월호.

시민적 및 정치적 권리위원회·고문방지위원회, 『유엔 인권조약 감시기구의 일반논평 및 일반권고』, 국가인권위원회, 2006.

심현정, 「행정정보공동이용제도에 대한 이해와 관련 법제의 발전방향」, 《법제》 2007년 1월호
양창수, 「정보화사회와 프라이버시의 보호」, 《인권과 정의》, 대한변호사협회, 1991. 3.
이인호, 『개인정보보호법제의 현대화방안에 관한 연구』, 국회사무처 법제실, 2005.
임지봉, 『미국의 전자정부 법제』, 한국법제연구원, 2001.
임규철, 『개인정보보호법제』, 푸른세상, 2004.
장용근, 『전자민주주의의 헌법적 연구』, 서울대학교 법학박사학위논문, 2004.
정부혁신지방분권위원회, 「전자정부 로드맵」, 2003.
정영화·송기춘·황성기·황성진, 『개인정보보호 감독기구 도입을 위한 법제도 개선방안연구』, 한국정보보호센터, 2000.11.
정재황, 「프랑스법에서의 개인정보의 보호에 관한 연구」, 《공법연구》 제34집 제4호, 2006.
조동기, 「정보화사회와 프라이버시」, 한국언론학회·한국사회학회 엮음, 『정보화시대의 미디어와 문화』, 세계사, 1998.
G7 GOL운영위원회 지음, 원성묵·김장현 옮김, 『세계의 전자정부와 전자민주주의』, 커뮤니케이션북스, 1999.
한상희, 「국가감시와 민주주의-공공영역의 창출을 위한 헌법해석」, 프라이버시보호네트워크 제2차 공동토론회 자료집 『개인정보의 국가등록/관리제도의 문제점』, 2001.
한국법제연구원, 『개인정보보호법제의 정비방안에 관한 연구』, 1997.
한국전산원, 『공문서전자유통방안』, 1996. 12.
한국전산원, 『전자정부 개념 정립 및 구현 방안에 관한 연구』, 1996. 12.
한국전산원, 『미국의 전자정부를 향한 도정』, 1997.
한국전산원, 『미국 전자정부법 분석 및 시사점』, 2003. 7. 9.

한국전산원, 『행정정보공동이용을 위한 법제전략 연구』, 2005.
한국전산원, 『인적정보의 공동활용에 따른 기술적·제도적 프라이버시 보호대책』, 1997.
한국전산원, 『부의 문서유통, 1997.
행정자치부, 『전자정부법의 이해와 해설』, 2001.
행정자치부, 『전자정부사업 연차보고서』, 2005.
형사사법통합정보체계추진단, 『형사사법 통합정보체계 구축사업 - 추진경과 및 사업내용』, 2006. 9. 26.
홍성욱, 『파놉티콘-정보사회 정보감옥』, 책세상, 2002.
황승흠, 「전자정부의 법과 국가」, 《법과사회》 제20호, 법과사회이론학회, 2001.
Cate, Fred H., Privacy in the Information Age, Brookings Institution Press, 1997.
Flaherty, David H., Protecting Privacy in Surveillance Societies, The University of North Carolina Press, 1989
Holmes, Douglas, *eGOv, eBusiness strategies for Government*, London: Nicholas Brealey Publishing, 2001.
Amy Harmon, As Public Records Go Online, Some Say They're Too Public, New York Times, 2001. 8. 24. 자.
Illinois Integrated Justice Information System(IIJIS), Privacy Schmrivacy? Drafting Privacy Policy In An Integrated Justice System(and Why It's Important), p. 7.
Kendall, Paul F. et al., Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use, 21st Annual International Conference on Data Protection and Information Privacy, Hong Kong 7-8 (Sept. 1999)(http://www.pco.org.hk/english/infocentre/files/kendall(formatted).doc)

Jim McKay, Big Brother:Is He Watching You?, Government Technology, Apr. 2003(http://www.govtech.net/magazine/story.phtml?id=45918)

NGA Center for Best Practices, Issue Brief "Improving Public Safety through Justice Information Sharing"

Solove, Access and Aggregation: public Records, Privacy and the Constutuion, 86 Minnesota Law Review 1137(2002)

U.S. Department of Justice et al. v. Reporters Committee for Freedom of the Press et al., 489 U.S. 749(1989)

GAO REPORT to Congressional Committees on Aviation Security: Computer-assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385

U. S. Department of Justice, Bureau of Justice Assistance, Privacy Policy Development Guide, Washington D.C.:2006.