발 간 등 록 번 호
11-1620000-000328-01

정부 정보자원의 인권적 관리에 관한 연구

2011년 10월

국가인권위원회

제 출 문

국가인권위원회 위원장 귀하

본 보고서를 「정부 정보자원의 인권적 관리에 관한 연구」에 관한 국가인권위원회 연구용역의 최종보고서로 제출합니다.

2011. 10

연구 기관 : 고려대학교 산학협력단, 정부학연구소

연구 기간 : 2011년 4월 1일 ~ 2011년 10월 10일

연구 책임자 : 최흥석(고려대학교 행정학과 교수)

공동 연구원 : 이철주(고려대학교 정부학연구소 선임연구원)

한승주(고려대학교 정부학연구소 선임연구원)

이준일(고려대학교 법학과 교수)

연구 보조원 : 김태호(고려대학교 행정학과 박사과정)

연보라(고려대학교 행정학과 석사과정)

본 보고서는 연구용역수행기관의 결과물로서, 국가인권위원회의 입장과 다를 수 있습니다.

< 요 약 문 >

전자정부의 확립과 정보자원의 구축으로 시스템 측면에서는 세계적인 수준으로 발전하게 되면서 이제 정부는 상당량의 정보를 수집·관리하고 처리해야하는 합리적인 정보자원관리자가 되어야 하는 동시에 국민 개인 정보의 보호자가 되도록 노력할 필요가 있다. 특히 정부가 상당량의 정보자원을 확보하면서도 빅브라더라는 우려와 경계를 불식하기 위해는 국가의 정보자원관리 과정을 관리적 시각과 인권적 시각에서 함께 다뤄야 할 필요가 있으며 정보인권의 보장을 위한 구체적인 체계를 구축해야 한다. 정보를 정부 조직 목적의 달성을 위한 효율적 자원이자 보호해야할 권리임을 인식해야 하는 것이다. 따라서 조직 관리의 거시적 합리성 확보를 위해서도 정부 정보자원관리에의 사회적 반발을 자세히 검토하고 이를 기반으로 인권적 정보자원관리 체계를 구축해야할 때이다.

정부 정보자원의 인권적 정보자원관리 구축과 관련하여 본 연구에서는 정보자원생애주기에 따라 크게 네 부분으로 구성하여 연구를 진행하였다. 첫째, 현재 정보자원관리가 어떻게 되고 있는가? 한국의 법체계 부문을 검토하여 정보자원생애주기별 정보자원관리 원칙과 현재 법체계의 괴리를 확인하여 우리의 현재적 수준을 진단하면서 미국, 독일의 정보인권과 관련된 법규정을 비교하면서 시사점 도출하였다. 둘째, 전자정부 구축 과정에서 효율성 가치와 인권적 가치가 충돌했던 대표적 갈등사례(교육, 형사사법, 보건의료 정보시스템)를 통해 정보생애주기 단계별로 어떤 문제가 발생하였는지, 발생한 갈등의 원인이 무엇이었는지를 구체적으로 분석하였다. 셋째, 정부 정보자원의 실질적 관리 실태를 중앙 및 지방정부 부서들을 대상으로 설문조사 및 인터뷰 하여 관리 실태와 관리 원칙과의 괴리를 확인하고 시사점을 도출하였다. 넷째, 앞의 분석에 근거하여 정부 정보자원의 인권적 관리 프레임을 구성하고 관련 내용을 제안하도록 하였다.

먼저 정보자원의 인권적 관리와 관련한 법체계 분석 결과, 미국은 OMB를 통해 개인정보영향평가 등을 예산편성에 반영하는 중앙관리기구

중심의 관리체계라는 특징을 보였으며, 독일은 중앙관리기구인 BDI가 존재하지만 각 부처를 중심으로 강력한 책임과 독립적 권한을 기반으로 한 내부통제체계라는 특징을 보였다. 반면, 한국은 중앙관리기구를 구성하고 있으나 집권적 관리체계가 약하고 부처별로 관리되고 있으나 책임과 권한이 불분명하고 중첩되어 있었다.

또한 법제상 개인정보의 수집/생성, 저장, 분배/공유, 폐기에 관한 규정이 나라별로 큰 차이를 보이고 있지는 않았으나, 독일의 경우 이의제기권이라 하여 정보주체의 자기정보결정권을 존중하고 구체적인 권한을 정보제공요구권, 수정요구권, 삭제요구권, 차단요구권으로 상세하게 기술하고 보장하고 있었다. 미국의 경우는 정보의 수집, 이용, 유지보수, 공유 등에 관계된 모든 기록을 작성하고 정기적으로 갱신하고 보고 및 평가하는 구체적인 관리체계를 구축하고 있었다. 우리의 경우, 정보관리에 관한 여러 원칙들이 이제 막 통합적으로 구축되고 있는 단계로서 아직까지는 포괄적 예외 규정, 법제간의 중첩, 선언적 규정 등의 문제가 제기될 수 있다. 관련 법규정 간의 통합성, 일관성을 높이고 세부적인 규정과 내부통제를 위한 구체적인 방안 마련 등이 필요할 것으로 보인다.

한편, 갈등사례를 통한 정보자원 관리 실태를 살펴볼 수 있는데, 정보자원의 인권적 관리와 관련하여 효율성 가치와 인권적 가치가 충돌했던 대표적 갈등사례로 교육행정정보시스템(NEIS), 형사사법통합정보체계(KICS), 보건기관정보통합 사례를 분석하였다. 이러한 분석대상은 정보의 성격, 서비스의 성격, 시간의 구분이라는 이유에 따라 선정하였다. 갈등사례 분석결과, 정보자원 관리의 기술적 측면의 강화를 우선시 하면서 이에 대한 사회적 문제를 예방할 수 있는 법적, 제도적 측면에서의 조치가 부족하여 갈등을 일으켰다고 해석 할 수 있다. 각 정보자원생애주기별로, 수집 및 생성에서는 공통적으로 정보 주체의 동의 없이 개인 정보를 수집하거나 포괄적인 규정으로 인한 정보수집으로 인해 정보주체의 선택권이 부여되고 있지 않음이 나타나고 있으며, 저장과 관련해서는 정보의 저장 및 보관과 관련한 보다 엄격한 규정의 필요성이 나타나고 있다. 공유에 대해서

는 정보자원의 목적외 사용에 대한 우려와 정보주체의 동의를 얻지 않은 공유가 문제로 나타났고, 사용에 대해서는 보유목적외의 사용을 폭넓게 인정하고 있는 점, 폐기와 관련하서는 폐기에 대한 불명확한 규정이나 규정이 없는 경우로 인해 갈등이 나타나고 있다고 볼 수 있다.

정부 정보자원의 인권적 관리와 관련한 법체계와 갈등사례 분석의 결과와 더불어, 정부의 정보자원 관리 실태를 파악하기 위해 중앙 및 지방정부 총 346개 부서 정보관리 담당자를 대상으로 설문 조사를 실시하였다. 분석 결과, 첫째, 현재 정부는 정보자원 관리를 통해서 정보의 신뢰성, 이용편의성, 조직목적 달성에 긍정적인 효과를 낳고 있으나, 새로운 정보가치의 창출, 시민참여, 맞춤형 서비스제공 등 적극적 정보관리의 효과는 미비한 것으로 판단되었다. 부서의 정보자원관리로 정보의 신뢰성을 높였다는 응답은 전체의 약 69%, 국민의 이용편의성을 높였다는 응답은 약 65%, 효과적인 조직목적 달성을 이루고 있다는 응답은 약 63% 등으로 나타난 반면, 새로운 정보가치 창출 효과를 낳았다는 응답은 전체의 약 38%, 국민의 결정권 및 참여가능성을 높였다는 응답은 약 46% 등에 그치고 있었다.

둘째, 특히 정보관리를 통해 국민의 참여가능성이 어느 수준에 이르고 있는가에 대해 정보공개의 수준은 어느 정도 높다고 판단되지만 정보내용 수정, 국민의 감시 가능성, 접근 가능성 등은 여전히 낮은 수준에 있다고 볼 수 있었다. 정보공개법과 같은 구체적 법규정이 마련되어 있는 정보공개의 경우 정보공개 수준이 높다는 응답이 약 33%대인 반면, 부서의 정보관리과정에 국민이 접근할 수 있는 가능성이 높다는 응답은 약 21%, 정보관리과정에 대한 국민의 감시가능성이 높다는 응답은 약 20% 등으로 국민의 적극적 참여와 선택의 가능성은 상대적으로 낮은 수준을 나타내고 있었다.

셋째, 현재 정부가 스스로 판단하는 정보관리의 위험성 수준의 경우, 국민의 프라이버시를 침해할 가능성에 대해서 약 18%만이 그렇다고 응답하고 있어 사회적 우려가 급증하는 현실과 괴리를 보이고 있었다. 전반적

으로 정보관리의 위험성을 크게 인식하지 못하고 있는 상태로 나타났지만 가장 높은 위험성으로 인식된 분야는 프라이버시 침해가능성이었고 이어서, 불투명한 운영으로 인한 위험성(약 11%), 정부의 국민감시 위험성(약 13%) 등의 순으로 나타났다. 반면, 위험성 인식이 가장 낮은 분야로는 정보내용의 오류로 인한 국민의 피해가능성, 정보오남용으로 인한 피해가능성 등으로 각각 6%와 9% 수준에 그쳤다.

넷째, 정부의 정보관리체계는 전 부처를 포괄하는 운영체계를 구축하지 못한 채, 부처를 중심으로 운영되는 체계로 나타났다. 또한 부처 내에서 부서별 자율성은 낮으며 부서 간 문제를 조정할 체계 역시 미흡한 수준으로 나타났다. 즉, 현재 정부의 정보자원은 각 부처를 중심으로 관리되고 있으며 부처 간의 배타성을 조정할 전 정부적 관리 구조가 미흡하고 부처 내부에서도 부서간의 갈등을 해결할 공식구조가 미비함을 보여주는 것이다. 전 부처를 포괄하는 중앙집권적 운영수준을 묻는 질문에 약 40%가 그렇다고 응답한 반면, 부처별 운영 수준에 대해서는 약 72%가 그렇다고 응답하고 있어 부처별 중심의 관리 현실을 확인할 수 있었으며 부서간 문제를 조정하는 체계가 존재하는가에 대한 응답은 약 33%에 그쳤다.

다섯째, 한편 정보관리에 관한 절차가 어느 정도 공식화되어 있는가에 대한 조사 결과, 구체적인 문서 지침 존재 여부(그렇다 약 66%), 구체적인 기록관리 정도(그렇다 약 57%), 법제 간 충돌과 중첩 정도(그렇다 약 13%), 법제의 공백 정도(그렇다 약 13%) 등은 상대적으로 공식화된 편으로 평가되고 있었다. 즉, 부서의 정보관리 과정이 법제나 절차에 따라 운영되는 편이라고 평가하는 것인데 이 결과는 정보관리상의 법제가 모호하고 포괄적 예외 규정이 많아서 자의적으로 관리되고 있다는 비판과는 충돌되는 것이다. 이 결과는 그동안 각 부서가 오랜 법제상의 공백과 충돌 상황에서 관행적으로 적용해온 해석기준이 존재하고 있어서 일선에서 혼란을 느낄 여지가 적을 수 있다는 차원에서 해석할 수 있을 것이다.

여섯째, 정보자원의 생애주기별 관리 실태를 살펴보면, 수집/생성 단계에서는 부처별 수집관리 구조로 운영되고 있으며 다른 부처에서 같은 정

보를 가지고 있더라도 따로 정보를 수집하여 보유한다는 응답이 약 42%에 이르고 있어 부처 간 정보수집의 배타성을 확인할 수 있었다. 또한 수집된 정보의 목록이 구축되어 있으나(‘그렇다’ 약 69%) 국민에게 공개되는 정도는(‘그렇다’ 약 46%) 이보다 낮게 나타나고 있었다. 저장 단계에서는 정보유출에 대해 국민이 감시할 수 있는 체계가 구축되어 있다는 응답이 약 35%에 그쳐 정보유출에 대한 외부감시 체계는 미흡한 편으로 볼 수 있었다. 정보공유 단계에서는 정보공유의 범위 면에서도 부족하고 공유 절차상 용이성도 미흡한 것으로 평가되고 있었는데 부처나 부서 간의 정보 공유의 범위가 넓다는 응답이 약 20% 남짓이었으며 공유가 원활하게 이뤄지고 있다는 응답 역시 약 27%에 그쳤다. 이는 정부의 정보공유 효율성도 충분한 효과를 낳지 못하는 수준으로 볼 수 있을 것이다. 한편 공유 과정을 기획 및 통제할 제도가 구축되어 있는가에 대해서도 약 35% 정도만이 그렇다고 응답하고 있었다. 이 결과는 현재 정부가 정보공유의 범위를 확대시키고 절차를 개선하여 효율적 공유를 도모함과 동시에, 정보공유로 인한 정보유출과 오남용을 막기 위한 통제 절차를 동시에 마련해 나가야할 단계임을 보여준다고 할 것이다. 정보사용 단계에 있어서도 부서에서 정보의 오남용을 막기 위한 자율적인 제한 관행이 존재하는가에 대해 약 29%만이 그렇다고 응답하고 있어 현재 정부 부서의 자율적인 관리 관행 수준은 매우 낮은 것으로 볼 수 있었다. 마지막으로 정보폐기 단계에서는 규정에 따른 폐기는 잘 지켜지고 있으나 폐기의무가 명확하게 규정되지 않은 상황에서는 보관하려는 경향이 존재하는 것으로 나타났다. 당장 불필요한 정보라고 파기하기보다는 보관한다는 응답이 약 19%로 높지는 않았으나 현재 폐기에 관한 규정이 구체적이지 못하고 모호한 현 상황에서는 적절한 폐기가 이뤄지지 못할 것으로 볼 수 있었다.

일곱째, 중앙 정부에 비해 지방 정부 수준에서 정보관리의 수준이 더 열악함을 알 수 있었는데, 중앙 정부의 부서들에 비해 지방 정부의 부서들이 국민의 프라이버시 침해가능성 등 정보관리의 위험성 수준을 더 높게 우려하고 있었으며 정보관리 상 국민의 참여가능성도 더 낮은 수준으

로 평가하고 있었다. 또한 정부부서와 현업부서 사이에서도 정보관리 실태에 대한 인식 차이가 나타났는데 정보부서의 경우 정보관리의 효과성을 더 긍정적으로 평가하는 동시에, 프라이버시 침해가능성 등 위험성도 더 높게 인식하는 것으로 나타났다.

정보자원의 인권적 관리에 대한 법체계, 갈등사례분석, 정부부서의 관리 실태 등을 종합하여, 정보자원의 인권적 관리를 보다 강화할 수 있는 정부 정보자원의 인권적 관리 프레임을 본 연구에서는 아래의 표와 같이 제시하고 있다.

또한 정보인권을 위한 정보자원관리 거버넌스 설계상의 시사점을 도출할 수 있었는데, 먼저, 정보인권을 위한 법체계 부문에서는 법 규정, 소관부서 등을 살펴볼 때 규제중첩이 발생할 우려가 있으므로 개관 간의 조직적 배열에 일차적인 관심을 가져야 할 것으로 보인다. 정보자원관리가 시간적(장기), 공간적(범 부처)으로 상당한 노력이 필요하다는 점에서 정보자원을 일관성 있고 체계적으로 운영할 수 있는 조직이 필요하며 범정부적으로 공공기관에 대한 업무조정을 할 수 있는 능력과 인력이 확보되어야 할 것이다. 둘째, 정보인권을 위한 조직운영 부문에서는 정보주체의 권리에 대한 인식 부족을 극복하고 국민을 중요 행위자로 인식할 것이 요구된다. 개인정보보호는 조직에서 지켜야할 제도가 되지 못하고, 원칙대로 일일이 따르기 힘들고 불편한 비현실적인 원칙(현재 법제상의 공백, 중첩, 충돌 등)이 나타날 때 제도적으로 해결하기 보다는 대부분의 개인들이 기존의 관행대로 처리하고 있음을 예상해 볼 때 정부 전체의 조직 운영에서 정보인권적 시각을 반영한 정보자원관리가 조직 전반적으로 내재화되고 일체화될 필요가 있다. 셋째, 정보인권에 대한 인식 부문에서도 국민에 대한 정보를 실질적으로 다루고 있는 정부조직과 그의 구성원이 정보인권에 대한 인식론적 전환이 필요하다. 정보자원을 다룸에 있어 입력 오류 및 부주의한 관리, 자원의 미폐기 등의 문제가 야기 될 수 있음에도 이러한 문제들은 모두 통제 가능하다고 믿고 있었는지도 모른다. 이러한 점에서 그동안 정부는 정보자원과 관련된 사항은 단지 내부 관리방식의 변화라고만 인식하여 내

부적 담론과정만을 거치면서 정책을 정당화하고 외부관계자들과의 의사소통은 거의 진행하지 않는 형편인 것이다. 특히 정보자원 집적을 통한 활용에 있어서 이에 따른 효용은 이를 집적하는 기관에서 얻게 되나, 이에 따르는 위험은 정보의 주체인 일반국민이 부담하게 된다. 따라서 정보자원의 인권적 측면에서의 인식전환에 대한 초점은 위험이 잠재하지만 평소에는 직접적으로 느낄 수 없는 것들, 정보주체도 모르게 활용되어 정보주체에게 해를 끼칠 수 있는 부분에 대한 경각심과 인식론적 전환을 위한 교육, 훈련이 지속적으로 일관성 있게 추진되어야 할 것으로 보인다.

수집/생성	
제도	- 예외 조항의 축소/명확화를 위한 법제 정리 - 독립적 개인정보보호책임자 제도와 같은 내부통제 제도 강화 - 중앙관리기구의 권한 강화(시정명령권/과태료/허용취소) - 개인정보영향평가제도의 실천방안 구체화
관리	- 구체적인 행동 매뉴얼 제시 - 불필요한 정보수집 제재 규정마련 - 유효기간을 정한 수집 - 중앙관리기구의 사전 통제 강화
기술	- 정보통합으로 새로운 정보생성 규제
행태	- 정보수집자와 수집대상의 대등한 관계 구조 마련 - 수집 및 입력 상의 자의성 배제 - 제재 수단도 명확히 명시
저장	
제도	- 제재조치를 포함한 내부통제 강화 - 외부 감시 기구의 신설 - 자기정보열람권한의 적극적 보장
관리	- 개인정보보호 담당 부서의 업무전문성 강화 - 보안관리 상태의 정기적 검토 및 보고체계 운영 - 접근권한자의 신중한 선정 관리
기술	- 개인 저장장치에 보관 및 외부 반출 규제 - 망 분리 - 보안기술수준의 정기적 진단 - 필요에 따른 열람만이 가능하도록 DB이외의 공간에서 저장 불가
행태	- 보안관련 정기적 교육 강화 - 업무 관련 개인정보에 대해 정보처리자의 책임성 부여

공유	
제도	- 정보공유의 예외 사항을 구체적으로 제시 - 외부감시체제의 구성 - 공유 범위 및 절차의 합리적 확장
관리	- 투명한 정보공유 현황 공개관리 - 불가피한 정보공유 시 익명처리를 통해 사생활 침해를 최소
기술	- 시스템상의 연계 기록 공개 및 보고
행태	- 개인적 필요에 의한 무단열람 및 공유에 대한 처벌 조치 강화
이용	
제도	- 정보사용 범위를 명확히 규정 - 모호한 예외규정의 수정이 필요
관리	- 개인정보사용 내역에 대한 정보주체자의 접근을 용이하게 함 - 제3자에의 정보 제공시 관리강화 - 정보의 질 관리 체계 마련
기술	- 정보사용 용도의 명확한 제시 - 정보사용에 대한 등급제 - 열람기록 보존 및 정기적 감사 강화
행태	- 업무 관련 필요 정보를 정리하여 가이드라인을 제시 - 민감정보에 대한 차별적 관리
폐기	
제도	- 삭제청구권 보장 - 영구보관의 예외 축소 - 정보폐기와 관련한 평가를 각 정부조직 평가에 반영하도록 함
관리	- 모든 정보의 유효기간을 명시 - 폐기정보의 목록관리 및 정기적 보고체계 마련 - 개인정보의 폐기현황을 적극적 공개 - 수정 및 삭제 불가한 서류의 범위를 최소화함
기술	- 재생 불가능한 기술 구현 - 한 기관의 삭제가 관련 기관에서 연동될 수 있어야 함
행태	- 필요가 사라진 개인정보 보유 시 벌점 부여 등 인사평가에 반영하도록 함 - 부처의 정보폐기 의무 강화

<차 례>

Ⅰ. 서 론 ·····1

1. 연구목적 및 필요성 ·····1
2. 연구설계 ·····6

Ⅱ. 정보인권에 대한 선행연구 검토 ·····11

1. 정보인권에 대한 연구: 법적측면 ·····11
2. 정보인권에 대한 연구: 관리측면 ·····13
3. 선행 연구의 한계점 검토 ·····14

Ⅲ. 정보자원관리의 이론적 검토와 분석틀 구성 ·····17

1. 공공조직의 정보자원관리에 관한 논의 ·····17
2. 우리나라에서 공공조직 정보자원관리의 등장 ·····20
3. 정보자원관리의 인권적 모델 도출을 위한 분석틀 구성 ···31

Ⅳ. 우리나라 정보자원관리의 법규정 분석 ·····35

1. 전자정부법 ·····35
2. 개인정보보호법 ·····41
3. 개인정보 보호를 위한 기본 지침 ·····47
4. 우리나라 정보자원관리 법규정 분석의 시사점 ·····52

Ⅴ. 정보자원생애주기에 따른 국가별 법적 체계 비교 분석 ···55

1. 국제기구의 개인정보보호 원칙 ·····55
2. 미국의 정보자원관리의 법규정 분석 ·····65
3. 독일의 정보자원관리의 법규정 분석 ·····77
4. 종합분석: 한국과 미국, 독일의 정보자원관리 법규정 비교 ·····90

Ⅵ. 우리나라의 정보자원관리와 갈등사례 분석 ……107
1. 정보자원관리 관련 갈등 분석의 필요성 ……107
2. 갈등사례 분석 방법 및 기준 ……108
3. 정보자원생애주기에 따른 갈등사례 분석 ……113
4. 종합분석 ……164

Ⅶ. 정부의 정보자원관리 실태분석 ……167
1. 설문조사 개요 ……167
2. 정부 정보자원관리에 관한 실태 인식 ……170
3. 중앙부서 및 지방부서 간 인식 차이 ……193
4. 정보부서 및 현업부서 간 인식 차이 ……196
5. 종합분석 ……200

Ⅷ. 정부 정보자원의 인권적 관리 프레임 ……201
1. 정보자원의 수집 및 생성 ……201
2. 정보자원의 저장 ……204
3. 정보자원의 분배 및 공유 ……206
4. 정보자원의 사용 ……208
5. 정보자원의 폐기 ……210
6. 요약: 정부 정보자원의 인권적 관리 프레임 ……212

Ⅸ. 결론 ……215
1. 연구요약 및 시사점 ……215
2. 제언: 정보인권을 위한 정보자원관리 거버넌스 설계 ……218

참고 문헌 ……223

부록 1. 설문조사지 ·····227

부록 2. 정보자원관리 관련자 인터뷰 전문 ·····239

<표 차례>

<표 1-1> 전자정부 발전지수 상위 10개국 순위 및 점수 ·····1
<표 3-1> 행정정보 공동이용 현황 ·····22
<표 3-2> 행정정보 공동이용 현황 ·····24
<표 3-3> 공공분야 사이버침해사고 발생현황 ·····25
<표 3-4> 개인정보 관리실태 점검 항목 ·····28
<표 3-5> 정부 정보자원관리 현황(As-Is) 파악과 정보자원의 인권적 관리 프레임(To-Be) 도출을 위한 분석틀 ·····33
<표 4-1> 전자정부법의 정보자원생애주기에 따른 분류 ·····39
<표 4-2> 개인정보보호법의 정보자원생애주기에 따른 분류 ·····45
<표 4-3> 공공기관 개인정보보호 지침의 정보자원생애주기에 따른 분류 ·····50
<표 5-1> UN 개인정보보호원칙의 정보자원생애주기에 따른 분류 ·····57
<표 5-2> OECD 개인정보보호 8원칙의 정보자원생애주기에 따른 분류 ·····60
<표 5-3> APEC 개인정보보호원칙의 정보자원생애주기에 따른 분류 ·····63
<표 5-4> 프라이시법의 정보자원생애주기에 따른 분류 ·····66
<표 5-5> OMB Circular(회람) A-130의 정보자원생애주기에 따른 분류 ·····70
<표 5-6> 미국 전자정부법의 정보자원생애주기에 따른 분류 ·····75
<표 5-7> 독일 연방정보보호법(BDSG)의 정보자원생애주기에 따른 분류 ····85
<표 5-8> 독일 통신법(TKG) 및 전자매체법(TMG)의 정보자원생애주기에 따른 분류 ····88
<표 5-9> 정보자원 수집/생성 단계에서의 법제 비교 ·····92
<표 5-10> 정보자원 저장 단계에서의 법제 비교 ·····95
<표 5-11> 정보자원 분배/공유 단계에서의 법제 비교 ·····98
<표 5-12> 정보자원 사용 단계에서의 법제 비교 ·····101
<표 5-13> 정보자원 폐기 단계에서의 법제 비교 ·····104
<표 6-1> NEIS 시스템 업무 영역(27개 영역) ·····115
<표 6-2> NEIS의 정보자원 생애주기에 따른 이슈 ·····130
<표 6-3> 단계별 사업 추진 내용 ·····135

〈표 6-4〉 KICS의 정보자원 생애주기에 따른 이슈 ·····145
〈표 6-5〉 보건의료정보통합의 정보자원 생애주기에 따른 이슈 ·····162
〈표 6-6〉 각 사례의 정보자원 생애주기에 따른 특징적 이슈 ·····166
〈표 7-1〉 표본의 특성 ·····169
〈표 7-2〉 정보관리의 효과성에 관한 인식 ·····171
〈표 7-3〉 정보관리의 국민 참여가능성에 관한 인식 ·····173
〈표 7-4〉 정보관리의 위험성에 관한 인식 ·····175
〈표 7-5〉 정보관리 체계에 대한 인식: 집권성 ·····176
〈표 7-6〉 정보관리 체계에 대한 인식: 자율성 ·····177
〈표 7-7〉 정보관리 체계에 대한 인식: 공식성 ·····178
〈표 7-8〉 정보수집에 관한 인식: 수집 최소성 ·····180
〈표 7-9〉 정보수집에 관한 인식: 책임성 ·····180
〈표 7-10〉 정보수집 실태에 대한 인식: 공개성 및 참여성 ·····181
〈표 7-11〉 정보저장에 관한 인식 ·····183
〈표 7-12〉 정보공유에 관한 인식: 공유의 범위와 원활성 ·····185
〈표 7-13〉 정보공유에 관한 인식: 공유과정의 통제 체계 ·····186
〈표 7-14〉 정보의 사용에 관한 인식: 목적외 사용 통제 ·····187
〈표 7-15〉 정보의 사용에 관한 인식: 정보의 정확성 관리 ·····189
〈표 7-16〉 정보의 폐기에 관한 인식: 폐기 실태 ·····190
〈표 7-17〉 정보의 폐기에 관한 인식: 폐기 체계 ·····191
〈표 7-18〉 정보의 폐기에 관한 인식: 외부 통제 ·····192
〈표 7-19〉 정보관리의 위험성에 대한 인식 비교: 중앙 vs. 지방 ·····193
〈표 7-20〉 정보관리의 국민 참여가능성 인식 비교: 중앙 vs. 지방 ·····194
〈표 7-21〉 정보관리의 효과성에 관한 인식 비교: 중앙 vs. 지방 ·····195
〈표 7-22〉 정보관리의 효과성에 관한 인식 비교: 현업 vs. 정보 ·····196
〈표 7-23〉 정보관리의 국민 참여가능성 인식 비교: 현업 vs. 정보 ·····197
〈표 7-24〉 정보관리의 위험성에 관한 인식 비교: 현업 vs. 정보 ·····198
〈표 7-25〉 정부의 정보자원관리 실태 인식상 특징 ·····200
〈표 8-1〉 정부 정보자원의 수집생성과 관련된 인권적 관리 프레임 ·····203

〈표 8-2〉 정부 정보자원의 저장과 관련된 인권적 관리 프레임 ·····205
〈표 8-3〉 정부 정보자원의 분배 및 공유와 관련된 인권적 관리 프레임 ·····207
〈표 8-4〉 정부 정보자원의 사용과 관련된 인권적 관리 프레임 ·····209
〈표 8-5〉 정부 정보자원의 폐기와 관련된 인권적 관리 프레임 ·····211
〈표 8-6〉 정부 정보자원관리와 관련된 인권적 관리 프레임(To-Be) ·····212

〈그림 차례〉

〈그림 1-1〉 본 연구의 분석 흐름 ·····6
〈그림 3-1〉 행정정보공동이용 경과 및 계획 ·····21
〈그림 3-2〉 연도별 해킹 등 사이버 침해 사고 발생건수 ·····24
〈그림 3-3〉 전자정부 서비스 보안수준 실태조사 결과 ·····25
〈그림 3-4〉 공공기관의 개인정보관리 체계 ·····27
〈그림 6-1〉 NEIS 개념도 ·····114
〈그림 6-2〉 NEIS 추진경과 ·····117
〈그림 6-3〉 KICS 시스템 개념도 ·····132
〈그림 6-4〉 형사사법 정보시스템 흐름도 ·····136
〈그림 6-5〉 보건의료정보화 체계도 ·····151
〈그림 6-6〉 보건의료정보화 시스템 구성도 ·····152

Ⅰ. 서 론

1. 연구목적 및 필요성

1) 정부 정보자원관리의 중요성 부각

1980년대 국가행정전산망사업이 진행되고, 1995년 8월에 제정된 「정보화촉진기본법」에 따른 1996년의 '제1차 정보화촉진 기본계획'과 1999년의 '전자정부 종합실천계획', 2001년 11대 전자정부 과제를 선정하여 정보자원 관리에 대한 본격적인 계획을 진행되면서 <표 1-1>과 같이 우리나라가 추진한 전자정부의 성과는 전 세계적으로 인정받고 있다.

<표 1-1> 전자정부 발전지수 상위 10개국 순위 및 점수

국가명	2008년 평가결과		2010년 평가결과		비고
	지수 값	순위	지수 값	순위	
한국	0.8317	6	0.8785	1	↑5
미국	0.8644	4	0.8510	2	↑2
캐나다	0.8172	7	0.8448	3	↑4
영국	0.7872	10	0.8147	4	↑6
네덜란드	0.8631	5	0.8097	5	-
노르웨이	0.8921	3	0.8020	6	↓3
덴마크	0.9134	2	0.7872	7	↓5
호주	0.8108	8	0.7863	8	-
스페인	0.7228	20	0.7516	9	↑11
프랑스	0.8038	9	0.7510	10	↓1

자료: 국가정보화 백서(2011)

특히 정보화 시대의 정부는 방대한 양의 정보를 수집, 보관, 처리하는 정보집약적 행위자이며 정보의 관리는 정부 생산성과 국민 신뢰 향상을 위해 이미 그 중요성이 부각되어 왔다. 이러한 전자정부의 구축으로 상당

량의 정보가 디지털화되면서 정부가 소유 및 관리하는 정보의 양과 범위는 엄청나게 증가하고 있다. 이에 따라 금융전산망, 연구교육전산망, 국방전산망, 행정전산망, 치안전산망 등 국가기간전산망과 과학기술정보, 교육문화정보 등 부처별로 관리 중인 다양한 정보 등 이렇게 방대한 정보자원을 정부가 어떻게 관리할 것인가는 정부 생산성을 결정짓는 중요한 측면으로 여겨지게 되었다. 그리고 정부의 정보자원은 재정자원, 인적자원, 천연자원 등과 마찬가지로 정부, 기업 그리고 개개 시민의 생존을 위하여 귀하게 다루어져야 할 국가적 자원으로서 보존되고, 재사용되며, 보호되어야 한다는 인식이 높아지게 되었다.

현재 정부의 정보자원 관리에 관련한 여러 계획들은 1995년 8월에 제정된 「정보화촉진기본법」에 따른 1996년의 '제1차 정보화촉진 기본계획'과 1999년의 '전자정부 종합실천계획' 수립으로 전자정부에 따른 정부의 정보자원에 대한 본격적인 계획이 시작되었다. 이전에 행정전산화 사업이나 국가기간전산망사업 등 행정의 전산화를 통해 정보기술을 활용하는 정부차원의 노력이 있었지만, 이는 지금의 전자정부에 대한 개념보다는 진보된 기술을 활용하는 수준이었기 때문에 전산화를 통해 정보자원을 본격적으로 활용하고자 하는 의지를 담고 있다고 보기는 어렵다. 1995년 이후, 2001년 전자정부특별위원회는 11대 전자정부 과제를 선정하여 정보자원 관리에 대한 본격적인 계획을 진행해 왔으며, 2003년 8월 '전자정부로드맵[1]'을 발표하고 이후에도 'Broadband IT KOREA VISION 2007', 'u-KOREA 기본계획' 등을 통해 국가정보화에 대한 지속적 계획을 추진하였다. 2008년 정부조직 개편에 따라, 구 정보통신부와 구 행정자치부

1) 로드맵 과제는 4대 분야(일하는 방식 혁신, 대 국민 서비스 혁신, 정보자원 관리 혁신, 법·제도 정비), 10대 의제(전자적 업무처리 정착, 행정정보 공동이용 확대, 서비스중심 업무재설계, 대 국민 서비스 고도화, 대 기업 서비스 고도화, 전자적 국민 참여, 정보자원의 통합 및 표준화, 정보보호 체계강화, 정보화 인력·조직전문화, 전자정부 관련 법제 정비), 31대 단위과제 및 45개 세부사업으로 구성된 전자정부 로드맵을 체계적으로 관리하기 위하여 사업의 중요성과 내용 및 범위에 따라 위원회 핵심추진 과제(범부처 공통 과제로서 위원회가 핵심적으로 추진할 필요가 큰 과제), 위원회 중점관리 과제(부처요청 과제 중 위원회가 중점 관리할 필요가 있는 과제), 부처별 추진과제(부처가 위원회와 관계없이 자율적으로 추진하는 과제) 등 세 가지 유형으로 구분하여 관리한다(출처: 국가기록원 나라기록).

에서 개별 추진하던 지식정보자원관리사업과 행정정보DB구축사업의 주무부처를 행정안전부로 통합되고 2009년 8월에 「지식정보자원관리법」, 「전자정부법」으로 이원화된 근거법령을 「국가정보화기본법」으로 통합하여 사업추진의 법적기반을 일원화시켰다. 이를 기반으로 추진체계 일원화 및 예산통합 등을 위한 ‘국가DB통합관리 세부추진계획’(2008~2012년)을 수립하여 2009년도부터 국가DB구축사업으로 통합 추진하면서 정보자원에 대한 통합적 관리가 활성화되었다. 그리고 2009년 5월에는 향후 5년간 추진할 ‘국가DB구축 중기계획’(2009~2013년)을 수립하고 중요성과 시급성이 높은 지식정보 및 행정정보의 디지털화 완결성 위주로 지원하여 완성도 높은 서비스가 가능하도록 디지털화를 추진하고 있다(국가정보화백서, 2011). 최근 2011년 3월에는 ‘스마트 전자정부(Smart Gov)’ 추진계획안을 마련하여 언제 어디서나 매체에 관계없이 자유롭게 국민이 원하는 정부 서비스를 이용할 수 있도록 하여 정보자원에 대한 통합과 공개, 공유의 공간적 범위를 넓히고자 하는 계획을 진행 중이다.

국가DB구축과 관련하여 현재 정부에서는 2009년에 ‘국가DB구축 중기계획’(2009~2013년)에 따라 총 654억 원을 투입하여51종(56개 사업과제)의 주요 행정정보와 지식정보의 디지털화를 추진하고 있다. 지식정보DB구축 분야는 총 286억 원을 투입하여 북한 자연인문지리 DB구축, 한국고대사료집성 DB구축 등 31종(34개 사업과제)을 디지털화하고 있으며, 동북아해양위성관측자료 DB구축, 플라즈마 물성정보 DB구축, 국가생명정보 DB구축, 국방학술정보 DB구축, 대한뉴스 DB구축, 장애재활 및 보육지원정보 DB구축, 천문현상정보 DB구축, 학위논문 DB구축, 한국근현대사자료 DB구축 등 9종의 디지털화를 완료하였다. 그리고 행정정보DB구축 분야는 총 368억 원을 투입하여 병적증명서 인터넷발급을 위한 병적DB구축, 소방대상물 DB구축 등 20종(22개 사업과제)에 대한 디지털화를 추진하였으며, 2009년 행정정보DB구축 추진을 통해 주민등록표원장 DB구축, 체류외국인문서 DB구축, 병적증명서 인터넷발급을 위한 병적 DB구축, 과학수사지문 DB구축, 구토지대장DB구축, 역사기후 DB구축, 새주소기반 표준전자

지도 DB구축, 보훈행정 DB구축, 수사자료표 DB구축, 선거정당 관련 중요 기록물 DB구축 등 10종의 디지털화를 완료한 상황이다. 정보자원의 효율적 관리계획을 중앙 및 부처별로 수립하고 각종 정보통신기술시스템을 적극적으로 도입한 결과, 전자정부 인프라 구축과 정보자원 구축은 세계 어느 국가보다 선도적이 되었다.

또한 정부는 정보자원의 관리를 위한 법제를 마련함으로써 합리적 정보자원관리를 시도하였는데, 「공공기관의 개인정보보호에 관한 법률」과 「전자정부법」에서 주로 정보자원관리에 대해 규정하고 있으며 「주민등록법」, 「민원사무의 처리에 관한 법률」, 「국가공무원법」, 「공직자윤리법」 등 기타 법률에서도 부분적으로 규율하고 있다.

2) 정보자원관리의 새로운 측면: 정보인권

그러나 전자정부의 확립과 정보자원의 구축으로 시스템 측면에서는 세계적인 수준으로 발전한 반면, 다른 한편으로 정보자원관리를 둘러싼 새로운 사회적 갈등이 발생하였다. 정부의 전자주민카드 도입 무산, 교육행정정보시스템 도입 갈등, 형사사법통합정보체계 도입 갈등 등 정보화 과정에서 우리 사회에 발생한 뜻밖의 갈등들은 정부가 정보를 효율뿐만 아니라 국민의 자유와 권리로서 다뤄야 한다는 관점의 변화를 요구하기 시작하였다.

이러한 갈등사례들에서는 정보인권이라는 개념으로 정부 정보자원 관리상의 인권적 가치를 반영할 것을 주장하고 있는데, 이러한 갈등은 정보자원의 관리과정에서 새로운 기본권적 요구가 발생하고 있음을 알려주는 것들이다. 정보자원관리는 조직 내부적 범위에 그치지 않고 새로운 시민적 권리와 밀접하게 연결됨으로써 정부는 이러한 요구를 반영하여 정보자원을 어떻게 관리할 것인가를 고려해야 하는 시점이다. 즉 정보를 정부조직 목적의 달성을 위한 효율적 자원이자 보호해야할 권리임을 인식해야 하는 것이다. 따라서 조직 관리의 거시적 합리성 확보를 위해서도 정부

정보자원관리에의 사회적 반발을 자세히 검토하고 이를 기반으로 인권적 정보자원관리 체계를 구축해야할 때이다.

이제 정부는 상당량의 정보를 수집·관리하고 처리해야하는 합리적인 정보자원관리자가 되어야 하는 동시에 국민 개인정보의 보호자가 되도록 노력할 필요가 있다. 정부의 정보란 결국 국민의 개인정보이므로 국민의 자유와 권리의 대상으로서 정보를 인식해야 하며, 정부는 정보가 국가의 자원인 동시에 국민의 인권이라는 관점을 구축해야 한다.

3) 정부 정보자원의 인권적 관리 체계 필요

특히 정부가 상당량의 정보자원을 확보하면서도 빅브라더라는 우려와 경계를 불식하기 위해는 국가의 정보자원관리 과정을 관리적 시각과 인권적 시각에서 함께 다뤄야 할 필요가 있으며 정보인권의 보장을 위한 구체적인 체계를 구축해야 한다.

이를 위해 정보자원의 생산, 정보자원의 제도화 및 가공, 정보제품의 유통 등 생성 및 수집-저장-분배 및 공유-사용-폐기로 구성되는 국가 정보자원생애주기(information resources life cycle)를 정보인권의 시각에서 총체적으로 검토할 필요가 있는 것이다. 이에 국가의 정보자원관리가 어떤 측면, 어떤 단계에서 문제가 되고 있는지를 정보자원생애주기에 따라 총체적으로 검토하여 끊어지거나 약해진 단계를 발견하고 이를 강화시켜야할 것이다.

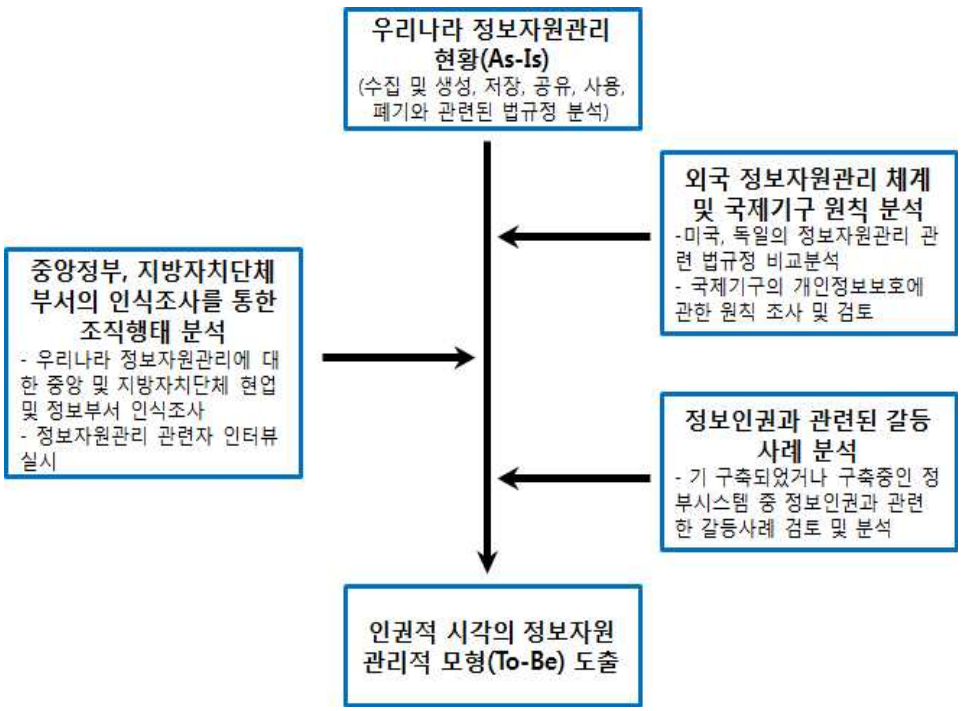
국가의 정보자원관리 과정을 관리적 시각과 인권적 시각에서 함께 다룬다는 것은 전략적 합리성을 강조하던 정부의 정보자원관리 측면에 대해 ‘인권적 관리’라는 새로운 차원의 접근을 반영한 구체적 프레임 구축함으로써 향후 정부 정보자원의 인권적 관리에 관한 기반을 제공할 것으로 기대할 수 있는 측면이 있으며, 인권적 요구가 상대적으로 증가한 요즘 사회상에 비추어 정보자원 관리에 있어 필수적인 시각인 것이다.

2. 연구설계

1) 본 연구의 분석 흐름

본 연구는 <그림 1-1>과 같이 정보자원생애주기의 흐름에 따라 분석을 실시하였다.

<그림 1-1> 본 연구의 분석 흐름



분석부문은 크게 네 부분으로 구성된다. 첫째, 현재 정보자원관리가 어떻게 되고 있는가? 위에서 제시한 분석 흐름 안에서 한국의 법체계 부문을 검토하여 정보자원생애주기별 정보자원관리 원칙과 현재 법체계의 괴리를 확인하여 우리의 현재적 수준을 진단한다. 아울러 미국, 독일의 정보인권과 관련된 법규정을 비교하면서 시사점 도출한다.

둘째, 전자정부 구축 과정에서 효율성 가치와 인권적 가치가 충돌했던 대표적 갈등사례(교육, 경찰, 보건 정보시스템)를 통해 정보생애주기 단계별로 어떤 문제가 발생하였는지, 발생한 갈등의 원인이 무엇이었는지를 구체적으로 분석한다.

셋째, 정부 정보자원의 실질적 관리자인 정부조직과 공무원들이 정보자원관리에 관해 어떤 인식을 하고 있는지 관리 실태를 조사(인터뷰, 설문조사)하여 실태와 관리 원칙과의 괴리를 확인하고 시사점을 도출한다.

넷째, 앞의 분석에 근거하여 정부 정보자원의 인권적 관리 프레임을 구성하고 관련 내용을 제안한다.

2) 구체적인 연구방법

(1) 문헌 분석

정보자원생애주기에 따른 법적 관리 체계와 정보인권 원칙의 검토를 위하여 선행연구 및 각종 법률, 공식문서 등 문헌들을 수집하고 분석할 것이다.

법적 체계 분석의 대상이 되는 법률은 전자정부법과 개인정보보호법이며 정보인권 원칙은 UN, OECD 등 국제기구와 미국, 독일 등 외국 정부의 정보자원관리 원칙 등을 대상으로 한다. 현재 우리 정부의 정보자원관리와 관련한 법제적 현실이 어떠한가를 확인함으로써 나날이 중요해지는 정보자원의 인권적 관리에 관한 현 주소를 확인할 수 있을 것이다.

(2) 사례조사 및 분석

지난 20여 년간 전자정부 추진과정에서 우리 사회가 겪은 갈등사례들이 정보자원관리의 어떤 측면에서 문제시 된 것인지 찾기 위해, 대표적 갈등사례들을 선정하여 분석하였다. 갈등사례는 전자정부 추진과정상에서

벌어진 사례들 중에서 사회적으로 이슈가 되었던 사례들 중에서 정보자원의 효율적 관리와 인권적 관리가 충돌하였던 대표적 사례들을 대상으로 하며, 수집된 사례는 정보자원생애주기라는 틀에서 갈등의 양상, 측면, 요인 등을 분석하였다.

선정된 갈등사례(형사사법통합망, 교육행정정보망, 보건의료정보망)를 정보자원생애주기의 단계별로 구분하여 인권차원에서 무엇이 문제되었던가를 분류하고 그 특징을 도출함으로써 정부의 정보인권 갈등의 현재적 특징을 파악하고 앞으로 어떤 문제가 도래할 것인지를 추론하도록 하였다. 예를 들어 현재까지 정보의 수집 및 생성단계의 갈등이 주를 이뤘다면 앞으로는 그동안 간과되었던 폐기 단계와 관련된 갈등이 등장할 수 있다는 점 등을 발견할 수 있는 것이다.

또한 갈등사례에 대한 분석을 통해 정보생애주기에 따르고 있는 우리나라 정보자원관리 순환과정에서 끊기거나 약한 고리를 찾아서 이를 강화하고 보강하는 근거를 제시하도록 하였으며, 이를 활용하여 향후 정부의 정보자원관리상 전략적 합리성을 넘어선 정보인권 차원의 관리를 가능하게 할 수 있는 자료를 제공할 수 있을 것으로 본다.

(3) 설문조사 및 분석

정보자원관리자인 공무원의 인식이 정보인권적 측면에서 어느 정도인지, 법적 원칙과는 어느 정도 괴리를 나타내고 있는지를 확인하고 이를 통한 정보자원의 인권적 관리 프레임을 도출하기 위해, 2011년 9월에서 10월 중순까지 설문조사를 실시하였다.

설문조사의 대상은 중앙정부 및 지방정부 소속 부처의 정보화책임관(Chief Information Officer: CIO) 및 정보관리담당 부서와 현업 부서 등으로, 해당 부처의 정보화업무를 책임지며 정보자원의 획득, 배분, 이용 등의 종합 조정 및 체계적 관리를 책임지는 부서를 대상으로 하였다. 설문내용은 정보자원의 관리에 대한 실태를 조사하였으며, 특히 인권적 정보

자원의 관리 측면에서 어느 정도의 수준을 보이는가에 초점을 두었다.

정부 조직의 정보자원 관리 실태 분석이 연구의 초점이므로 중앙 및 지방정부의 부서를 분석 단위로 하여, 부서 단위에서 이뤄지는 개인정보 관리 실태에 대하여 조사하였다. 중앙 및 지방 정부의 부서들 중에서 개인정보 목록을 구축 및 관리를 주로 담당하고 있는 부서 리스트를 작성한 후, 국가인권위원회를 통해 공문 협조를 구하여 총 346개 과를 대상으로 온라인 설문지를 발송하였다.

총 346개 부서의 정보관리 담당자 및 일반 현업부서 담당자에게 발송한 온라인 설문지는 2011년 9월 말부터 10월 둘째 주까지 3주 이상 진행되었으며, 총 126개 부서로부터 응답을 받았다. 약 35%대의 수거율이었으나, 중앙 및 지방자치단체 전체를 대상으로 정보자원관리 실태에 관한 설문조사를 진행하였다는 점에서 의의가 크다고 할 수 있을 것이다. 또한 특정 부처나 중앙정부 수준에서 진행되었던 기존 연구과는 달리, 중앙과 지방을 포괄한 정부 전 부서를 대상으로 하였다는 점에서 정부의 정보관리 실태를 보다 전반적으로 파악할 수 있을 것이라고 판단한다.

Ⅱ. 정보인권에 대한 선행연구 검토

정보인권(citizen's right to information)은 정보화 사회로의 시대변화에 따라 등장한 새로운 인권 개념으로 제4세대 인권으로도 일컬어진다. 정보의 생산자, 소비자, 유통자로서 국민을 상정하고 권리와 의미를 체계적으로 논의하기 시작한 현재에는, 사이버인권, 디지털인권 등 다양한 용어로도 불리지만 최근 정보인권이라는 표현으로 보편화되는 추세이다. 정보인권은 '정보사회에서 정보의 유통에 대한 개인의 통제권을 의미하는 것으로 개인의 존엄과 자유를 보장해주는 기본적인 인간의 권리이며 정보의 자유와 정보프라이버시권을 포함한 정보유통의 통제에 관한 권리들의 다발'(이인호, 2005)로 정의할 수 있다.

1. 정보인권에 대한 연구: 법적측면

정보관리와 관련한 여러 선행연구 가운데 가장 많은 비중을 차지하고 있는 것이 정보자원관리와 관련한 법적인 측면에 관한 연구들이다. 실제 정보인권의 문헌에 대해 분석한 최홍석(2010)의 연구에서는 정보인권과 관련한 그동안의 연구 가운데 약 절반 정도가 법/제도에 대한 부분들로 나타나고 있다.

특징적으로는 국외의 정보자원관리에 대한 법령을 소개하고 국내 적용에 대한 시사점을 제시하는 것이 주요한 연구의 흐름이었다. 특히 미국의 정보자원관리와 관련한 법체계를 분석한 연구(권태웅, 2009; 김성근 외, 2005; 백윤철, 2008; 오일석 외, 2010; 임혜경, 2005)들이 많았는데, 순차별 미국의 전자정부관련 법제를 통해 정보의 자원화, 정보보안, 정보의 디지털화 및 미국 전자정부의 포괄적 법인 전자정부법의 고찰을 통해, 미국전자정부의 목표 및 전자정부 추진의 성공요건인 리더십, 기관 간 협력, 지위와 역할의 인식이 전제되어야 함을 도출하고, 이를 통해 국내 정보자원관리의 제도적 기반을 마련하기 위한 법적 요소를 도출하고 기본적

구조를 제시하는 특징을 보여주고 있다.

미국의 정보자원관리 관련 법체계 분석에 있어 OMB-Circular의 내용을 분석하고 이를 중심으로 한 정보보안 개선과 관련한 내용을 구성함으로써 정보인권과 관련한 내용을 다룬 경우도 있다. 미국 뿐 아니라 영국의 개인정보보호법을 연구한 최경진(2009)의 연구에서는 영국의 개인정보보호법의 주요 내용 및 개인정보보호에 관한 7개의 일반원칙에 대해 살펴보고 있으며, 해외 행정정보공동이용 법제 분석과 관련한 김현경(2010)의 연구에서는 미국, 영국, 일본의 법제의 비교분석을 통해 정책적 시사점을 도출하고 행정정보공동이용의 필요 및 한계에 대해 논하면서 행정정보는 주요 정보자원으로 기능하므로 행정정보공동이용은 종합적 정보자원관리 측면에서의 고려가 필요하다는 주장을 내고 있다.

국내 법체계와 관련한 연구(백윤철, 2009; 윤상오, 2009; 이제희, 2009; 정충식, 2004; 정한기, 2009)들도 다수 있다. 이들 연구들은 국내 법체계만을 한정되어 연구하기 보다는 국내 법체계를 중심으로 국외 사례에서의 시사점을 국내 법체계에 적용하고자 하는 시도들인데, 공통적으로 정보자원의 인권적 관리에 대한 부분이 부족한 상황이고 한국에 있어 개인정보보호체계를 강화해야 한다는 시사점을 제시하고 있다.

정보자원관리와 관련한 선행연구들에서는 국외 법체계를 소개하는 경우가 대부분인데, 이를 국내 상황과 비교하고 이를 통해 국내에 적실성 있는 대안을 제시하거나 정보인권과 관련한 구체적인 방법을 주장한 경우는 거의 없다. 방향성을 제시하거나 현 한국의 법체계에 있어 인권적 측면에 대한 대응방식 등에 대해서 언급하고 다루고 있지만, 보다 실제적인 관점보다는 현재 정보자원의 인권적 측면에 있어서의 문제점 제기와 거시적 측면에서의 방향성만을 언급하는 것이 대부분이다.

또한 정보자원관리에 있어 관리의 기술적 측면과 인권적 측면이 통합적으로 다루어지지 않아 효율적 관리이자 기본권 보호의 두 측면을 통합하려는 시도가 미흡하다고 판단된다.

2. 정보인권에 대한 연구: 관리측면

정보자원관리를 큰 틀로 구분하면, 효율성에 강조점을 두느냐 아니면 정보인권에 중심을 두고 있느냐로 말할 수 있다. 최근에는 정보인권에 논의가 보다 활발해 지고 이에 대한 관심이 높아지면서 정보자원관리의 인권적 측면에 대해 논의하는 경우가 종종 나타나고 있다.

하지만 NEIS 사례로 인한 사회적 갈등이 발생하고 이에 대한 관심이 증가하기 이전에는 정보자원의 관리에 있어 보다 효율적인 관리방법에 대한 논의가 주를 이루었다. 정보자원관리의 효율성과 관련하여 윤정수(2005)과 최진명(2007)의 연구에서는 EA와 정보자원관리의 관계 등과 같이 정보자원의 외형적 관리체계에 대한 논의를 진행하였고, 황주성 · 임혜경(2006)의 연구에는 원활한 정보자원관리를 위해서는 리더십과 같은 조직관리체계와 관련된 것과 정보의 통합이 필요하다는 주장을 하고 있다.

황주성 외(2007)의 연구에서는 효과적인 정보자원관리를 위해서는 통합관리가 필요하다는 결론을 언급하고 있다. 이외의 다수의 논문에서도 정보자원관리와 관련하여 통합과 집적을 통한 효율성 추구를 중심으로 하는 논의를 전개하는 경우가 많이 나타나고 있다.

하지만, 정보자원관리에 있어 인권적 측면을 관리과정속에 담아내는 연구는 많이 부족한 상황이다. 그간의 연구에서는 정보자원관리의 인권과 관련하여 NEIS, 전자주민카드 등 사례나 단일 이슈에서 나타난 갈등을 중심으로 연구를 진행하고 있다.

거버넌스의 관점에서 NEIS 갈등 사례를 다룬 조화순(2004)의 연구나 정책인식프레이밍을 통해 NEIS 갈등을 설명하고 있는 나태준(2006)의 연구와 같이 정보인권과 관련한 단일의 갈등사례를 일정한 분석프레임을 통해서 바라보고 있는 경우가 많아서 정보자원의 관리과정에서의 인권적 가치 측면을 다루고 있는 연구는 소수에 불과하다.

또한 개인정보와 사생활보호의 가치의 중요성에 대한 공감대를 바탕으로 전자정부 추진시의 방향성을 제시한 윤상호(2009)의 연구나 자기정보

관리통제권을 중심으로 정부 정보자원의 인권적 측면을 강조하고 있는 정인숙(2010)의 연구에서처럼 정보자원의 인권적 측면을 다루고는 있으나 정부자원이 가지는 생애주기라는 특징을 반영하여 연구를 진행한 경우는 찾아보기 어렵다. 이는 효율성을 강조한 정보자원관리 연구에서도 마찬가지이다.

3. 선행 연구의 한계점 검토

전자정부 구축이 인권적 측면을 고려해야 한다는 주장은 2000년대 중반부터 본격화되었는데 전자주민카드, 교육행정정보시스템 등이 사회적으로 큰 갈등과 논란을 일으키며 정부의 효율성 중심의 사업추진에 대한 반성적 고찰이 시작되었다.

이에 따라 국가인권위원회(2006)의 연구는 정보인권의 관점에서 전자정부사업에 대한 치밀한 법적 검토가 필요하며 행정정보의 공동이용법률안의 내용 수정, 형사사법정보통합체계구축이 기본권을 침해할 우려 등을 주장하고 있는 것이다.

정부 정보자원관리의 인권적 가치를 주장해온 기존 연구들은 주로 전자정부의 개별 사업이 개인정보보호를 침해할 우려를 제기하거나 현재 정부의 개인정보관리를 위한 법제의 불완전성을 지적하고 개인정보보호를 위한 통합 법률의 마련 등을 주장하는 연구들이 주를 이루고 있다.

그리고 관리적 측면에서는 정보자원관리체계 구축이나 효율적 활용과 관련한 연구들이 다수를 차지하고 정보인권을 중심으로 하는 연구에서는 정보자원생애주기가 반영되지 않고 단일 갈등 이슈에 의해 인권관련내용을 풀어내고 있다.

이처럼, 정부의 정보자원 관리 과정에 따라 구체적으로 어떠한 인권적 요소들이 고려되어야 하는지, 실제로 어떻게 관리되고 있는지 등에 관한 분석적인 연구는 부족한 상황이다.

1) 정보자원관리와 정보인권 연구의 통합적 접근 미흡

선행연구의 정보자원관리에 관한 정의로부터 짐작할 수 있듯이, 정보자원관리에 관한 연구는 조직 효과성에 초점을 둔 기술적 조직관리 체계를 구축하고자 하는 접근방식이었다. 비록 정보자원관리가 조직의 기본적 임무를 수행하는 수단이라는 점을 부각시킴으로써 정보기술차원 이상의 포괄적 조직관리 차원임을 주장하였으나, 이것이 조직 외부의 시민들에게 기본권적 요소를 지님으로써 효율적 관리이자 기본권 보호의 두 측면을 통합하려는 시도는 미흡하였다.

국가의 정보자원관리는 정보의 생산, 가공, 유통, 폐기 등 정보자원생애주기 전반에 걸쳐 낭비와 중복의 방지 등 효율성을 강조하고 있을 뿐, 정보인권의 관점에서 어떤 관리적 노력을 해야 하는지에 대해서는 고려하지 않고 있다.

정보자원관리 과정이 정보인권이라는 새로운 기본권 침해 요소를 가진다는 많은 비판에도 불구하고 정보자원관리체계에 관한 연구와 정보인권에 관한 연구가 통합되지 못하고 각각 진행되면서 통합적 프레임 구축이 미흡한 측면이 많다.

따라서 선행연구를 보면, 정부의 효율적 정보자원관리를 위한 연구가 주류를 이루고 있으며 정보자원관리의 정보인권적 측면을 통합하려는 연구는 부족한 것을 알 수 있다.

정보인권에 관한 연구는 법학, 행정학, 사회학, 언론학 등 다양한 분야에서 많이 연구되어왔으나 정보자원생애주기별 정보인권의 원칙을 구축하고 관리하려는 관점은 상대적으로 부족한 측면이 많다.

특히 정보자원의 관리를 합리적 조직관리 측면으로 접근하다보니 정보자기결정권, 정보프라이버시 등 정보인권이라는 새로운 사회적 요구를 관리과정에 어떻게 반영해야하는가에 관한 행정적 접근이 부족하다.

2) 정보자원관리의 실제적 갈등과 공무원 인식에 관한 분석 미흡

정보자원의 개념 및 중요성, 체계에 관한 많은 선행의 연구에도 불구하고 정보자원의 실제적 관리과정에서 벌어졌던 갈등을 분석함으로써 한국적 정보자원의 관리 현상에 관한 고찰이 미흡하였다.

단일 갈등 사례에 대한 논의를 중심으로 하게 되면서 정보자원관리와 관련한 갈등의 실제적 양상과 정보자원생애주기에 따른 보다 세밀한 분석이 나타나고 있지는 않고 있다. 또한 정보자원관리로서 공무원들이 어떤 정보자원관리 행태를 보이는가에 관한 분석적 연구도 부족한 상황이다.

정보자원관리는 법제도와 같은 체제상의 관점에서 논의될 필요와 더불어 실제 정보를 수집하고 활용하는 공무원들이 정보자원에 대한 어떠한 인식을 가지고 있으며 이러한 인식이 정보자원관리에 있어 그들의 행태와 연관성을 가지는지에 대한 논의도 중요한 측면이다.

하지만 기존 연구들에서는 공무원의 인식과 행태보다는 정보인권과 관련한 법제도에 대한 연구가 상당부분을 차지하면서 행태수준에서의 정보자원의 인권적 관리에 대한 논의가 부족한 상황이다. 이에 법제도와 구성원의 행태를 포괄적으로 다룰 수 있는 연구가 필요한 것이다.

우리에게 적실한 정보자원의 인권적 관리 프레임을 도출하기 위해서는 정보자원의 관리의 실제적 모습을 파악하는 것이 우선이며 이를 위해서는 발생한 갈등사례의 분석과 공무원의 인식분석이 기반이 되어야 한다.

그러나 현재까지 이러한 분야에 관한 분석적 연구보다는 정보자원관리 체계의 효율적 구축이 주류적 연구가 되어왔다. 따라서 정보자원의 실제적 갈등과 공무원의 인식을 분석에 초점을 둔 연구가 필요하다고 판단되어 진다.

Ⅲ. 정보자원관리의 이론적 검토와 분석틀 구성

1. 공공조직의 정보자원관리에 관한 논의

1) 정보자원관리의 등장 및 의의

정보화를 통하여 환경 변화에 행정이 효과적으로 대응하고, 그 결과 혁신을 통한 조직성과의 향상을 도모하기 위해서는 무엇보다도 공공조직 내의 수많은 정보들을 효율적으로 관리하고 이를 적극적으로 활용할 수 있는 환경이 조성되어야 한다. 특히, 공공조직의 경우 제한된 재원과 비용 절감에 직면하고 있으며, 보다 효과적인 관리가 요구되는 상황에서 공공조직의 정보자원관리는 조직의 생존과도 직결된다고 해도 과언이 아니다[2].

정보자원관리(Information Resource Management: IRM)는 정보자원관리의 초기개념이 나타나게 된 시점에서 그 필요성이 강조되었는데(최흥석 · 서진완, 2006)[3], 1970년대 미국 의회는 정부가 보관하고 있는 문서가 급증하여 관리에 문제가 있을 뿐만 아니라 국민에게 반복 부과되는 문서작업의 부담이 과중한 점을 인식하고 1975년 연방문서작업위원회를 설치하여 정보수집 처리 제공 및 정보활동의 관리 통제와 관련한 연방정부의 법령, 정책, 규칙, 규제, 절차, 관행 등을 연구 조사하고 그 이유를 분석하도록 하였다[4].

그 결과 연방정부는 정부의 모든 정보와 정보자원을 효율적, 경제적으

---

2) Lutchen(2004)은 정보기술관리에 대한 역할과 책임은 CEO에게 있다는 점을 강조하면서 기존의 정보기술관리의 시각과는 다른 새로운 접근을 필요하다고 주장하였다. 그는 ① 정보기술을 조직의 중요 영역으로 설정하기, ② IT관련 조직을 별도의 독립된 사업단위로 할 것, ③ IT전략을 조직전략과 연계(alignment)시키기 등을 제시하고 있다.

3) 정보자원관리를 소개한 대표적인 초기의 문건으로 미국 의회의 연방문서작업위원회(Commission on Federal Paperwork, 1977)의 "A Report of the Committee on Federal Paperwork: Information Resource Management"를 들 수 있는데, 연방문서작업위원회의 보고서에 담긴 내용의 대부분은 문서감축법(Paperwork Reduction Act, 1980)에 반영되어 미국 연방정부에서 시행되어 오고 있다.

4) 위원회는 문제의 근본 이유가 정보가 관리될 필요가 있는 가치 있는 자원으로 고려되지 않고 대부분의 공무원들이 정보를 '자유재'로 인식하기 때문에 이미 작성된 관련 정보의 소재를 파악하지 못하여 발생되는 중복작업의 악순환 때문이라는 결론을 내린바 있다.

로 관리하기 위해서는 인적자원, 재정자원과 같은 다른 전통적 자원과 동일한 방법으로 관리해야 한다는 정보자원관리의 도입을 제안하였다(최홍석·구상회·이정준, 1999). 미국의 정보자원관리의 기본 철학과 개념은 2002년에 제정된 전자정부법에 계승되었는데, 전자정부법의 핵심중 하나가 바로 연방정부차원에서의 EA(Enterprise Architecture)의 도입이다.

연방문서작업위원회의 보고서와 문서작업감축법 등을 기반으로 OMB(Office of Management and Budget)는 "정보자원관리는 정부기관의 정보 부담, 수집, 창출, 사용 및 보급에 관련된 계획화, 예산화, 조직화, 지휘, 훈련, 그리고 통제를 뜻하며, 이 개념은 정보자체 및 이와 관련된 인력, 기구, 기금, 그리고 기술과 같은 자원들의 관리를 포함한다"고 제시하였다(OMB, Circular No. A-130, 1985: 1; Choi, 1993).

2) 정보자원관리의 개념 및 정보생애주기에 따른 관리

한 조직에 있어서 정보자원관리의 성숙도는 그 조직의 임무를 달성하기 위해 정보자원이 얼마나 효과적으로 통합되어 있는가를 통해 판단할 수 있기에 정부의 경우 국민의 자유와 권리, 복지의 향상 등 정부가 추구하는 다양한 공적 가치 달성하도록 정보자원이 원활히 관리되어야 한다.

최홍석 · 구상회 · 이정준(1999)은 정보자원관리란 "개별 중앙정부 부처 및 기관의 수준에서는 정보를 수집 및 생성, 보관, 분배 및 공유, 사용, 폐기하는 단계를 효과적·효율적으로 수행하기 위하여 H/W, S/W, N/W 등의 정보기술을 적절히 활용하고, 정보생애주기의 각 단계를 계획·조직·지휘·조정·통제하며, 예산관리, 인사관리, 민원사무처리 등의 행정업무를 수행함에 있어 정보기술을 활용한 행정관리기법을 도입·활용하는 것"으로 정의하면서 정보자원관리는 정보기술관리의 차원을 뛰어넘는 개념임을 지적하고 있다. 이처럼 정보자원관리는 정보를 유용한 요소로 파악하는 모든 관리적 기법들을 포함한다고 이해할 수 있으며, 조직목표의 달성을 위한 효과적 수단으로 조직에게 다양한 의미로 작용하고 있는 것이다(정충식, 2007).

정보자원관리의 개념에서는 정보의 수집 및 생성, 보관, 분배 및 공유, 그리고 폐기에 걸치는 정보생애주기 전반에 대한 체계적인 관리가 강조되어 진다. 정보생애주기(information life cycle)란 정보가 거치는 일반적 단계 즉, 생성 및 수집, 저장, 분배 및 공유, 사용, 그리고 폐기를 의미하는 것으로, 이를 통해 정보자원을 정보의 생애주기에 따른 흐름으로 관리함으로써 보다 체계적인 정보자원의 관리가 가능해 진다.

최흥석 외(1999)은 정보자원생애주기 단계별 적절한 정보자원관리의 목표를 검토하면서 관리계층과 생애주기의 결합을 주장하였다. 단계별 정보자원관리 목표를 보면, 먼저, 정보의 수집 혹은 기존 정보의 처리를 통해서 새로운 정보가 발생하는 '생성 및 수집' 단계로, 중요한 정보자원관리목표로 디지털 형태로의 기록화, 정보 이중수집의 방지, 그리고 유용한 정보의 수집을 들 수 있다. 두 번째는 새로이 발생한 정보를 '저장' 하는 단계인데, 저장의 안정성 확보는 가장 기본적인 고려사항이며 정보저장단계에서는 정보생애주기의 다음 단계들에 있어서 정보활용의 수월성을 제고하기 위한 정보자원관리 행위가 이루어져야 한다. 세 번째로, 정보가 조직구성원들 간에 '분배 및 공유' 되는 단계인데, 해당 주기단계는 정보자원관리의 중요 관심사는 정보의 분배 및 공유를 원활하게 할 수 있는 조직관리적, 기술적 환경의 마련이라 할 수 있다. 그리고 정당한 사용권한이 없는 자의 정보접근을 막기 위한 각종 제도적, 기술적 장치의 마련이 필요하게 된다. 조직구성원들에게 분배된 정보가 특정한 업무의 맥락에서 사용되는 단계에 있어서의 일차적 관심사는 정보이용을 통한 부가가치의 창조라 할 수 있고 비록 정당한 절차를 거쳐 취득한 정보라고 할지라도 조직구성원이 이를 그릇된 목적으로 사용할 수 없도록 해야만 할 것이다. 마지막으로 정보의 '폐기' 인데, 특정 정보가 업무수행의 맥락에서 정보로서의 유용성을 상실한 상태에서 폐기되거나 지속적이고 규칙적인 유지관리의 대상으로부터 제외되는 것을 뜻하며, 정보폐기단계에서의 중요한 정보자원관리목표는 불필요한 정보를 찾아내고 이를 적절한 절차를 거쳐 은퇴시키는 일이라는 점에서 중요성을 가진다.

2. 우리나라에서 공공조직 정보자원관리의 등장

정보자원관리의 필요성이 대두됨에 따라 우리 정부 역시 다양한 연구와 논의[5]를 기반으로 "행정기관의 업무수행 효율성 제고 및 대국민 행정서비스 품질제고 등 행정기관의 업무 목적달성을 위하여 필요한 행정정보자원(행정정보시스템, 행정정보, 정보기술, 정보화예산, 정보화인력 등)을 체계적이고, 효율적이며, 투명하게 계획, 구축, 운영 및 평가하는 활동"으로 정의내리고 이에 관련한 업무를 추진하고 있다.[6]

1) 정부의 정보자원관련 경과 및 계획

정부가 본격적으로 정보자원을 활용하고 자원으로써 관리하게 된 것은 행정정보 공동이용을 추진하기 시작하면서이다. 지난 2005년 10월 18일에 행정정보 공동이용의 효율적 추진을 위해 국무총리와 민간위원장을 공동위원장으로 하는 행정정보공유추진위원회를 대통령 자문기구로 출범, 위원회 운영을 지원하는 사조직으로 행정정보공유추진단을 설치하면서 정보자원과 관련한 정부의 계획은 본격적으로 진행되었다. 그리고 동년 12월에 '행정정보 공동이용 종합추진계획'을 확정하고 2008년 10월까지 3차에 걸쳐 행정정보 공동이용 확대 구축 사업을 추진하였다. 1차는 행정정보공유기반 구축사업(2005.12 ~ 2006.08)으로 총 34종 공동이용 대상정보를 모든 행정기관과 5개 공공기관이 이용하도록 하였고, 2차는 범정부 행정정보공유체계 구축사업(2006.09 ~ 2007.03)으로 총 42종 공동이용 대

---

5) 기존의 공공부문에서의 정보자원관리에 대한 연구는 정국환(1996), 서진완(1998), 문신용(1998), 황주성 · 권헌영(1998), 유시완·이연희(1999), 최홍석 외(1999), 황종성(2002), 김성근 외(2004), 황주성 외(2005), 최홍석·서진완(2006)을 참조하기 바라며, 정보자원관리가 정리되어 있는 교과서로는 김성태(2003), 이용규(2004), 정충식(2007) 등이 있다.

6) 아울러, 정부는 전자정부법 제2조 제8호에서 " '행정정보자원'이라 함은 전자정부 구현을 위하여 행정기관이 보유하고 있는 행정정보, 전자적 수단에 의하여 행정정보의 수집·가공·검색이 용이하게 구축된 정보시스템, 정보시스템의 구축에 적용되는 정보기술, 정보화예산 및 정보화 인력 등을 말한다"라고 정의내리고 있다.

상정보를 모든 행정기관, 43개 공공기관, 2개 은행이 이용하도록 확대하였다. 3차는 행정정보 공동이용 확대구축 사업(2007.12 ~ 2008.10)으로, 총 71종의 공동이용 대상정보를 모든 행정기관, 50개 공공기관, 16개 은행이 이용하도록 행정정보 공동이용 구축 사업을 진행하였다. 이후 2009년 부터는 수요자 맞춤형 공동이용체계 구축 사업을 추진(2009 ~ 2012)하면서, 2009년 8월부터 12월까지 공동이용 대상정보의 수와 이용 기관을 확대하고 행정정보중계시스템 개선 및 확충하였으며 617개 민원사무에 대해 전자민원서류관리 시스템을 시범 구축하였다. 2010년 4월부터 현재까지 총 92종의 정보가 모든 행정기관, 79개 공공기관, 17개 금융기관, 6개 교육기관에서 공동으로 이용되고 있다. 또한 전자민원서류관리 서비스를 확대 구축(1015개)하는 등 정보자원의 원활한 활용으로 위해 지속적인 노력을 기울여 왔다. 2011년 에는 제3차 수요자 맞춤형 공동이용 체계 확대구축사업(2011.4~)을 진행 중이며 공동이용 대상정보 28종을 추가적으로 확대하고, 22개 사무를 대상으로 맞춤형 정보조회서비스를 적용 및 확대 할 예정이다.

<그림 3-1> 행정정보공동이용 경과 및 계획

자료: 행정정보공동이용추진위원회(http://pr.share.go.kr/)

2) 정부의 정보자원관리 실태

2010년 4월부터 현재까지 총 92종의 정보가 총 415개 기관(53개 중앙행정기관, 260개 지방자치단체, 79개 공공기관, 17개 금융기관, 6개 교육기관) 들에 의해 공동으로 활용되고 있다.

<표 3-1> 행정정보 공동이용 현황

정보보유기관	공동이용 대상 행정정보(구비서류)
23개 기관	92종
외교통상부(2)	여권, 해외이주신고확인서
법무부(4)	출입국에관한사실증명, 외국인등록사실증명, 국내거소신고사실증명, 외국인의부동산등기등록증명서
행정안전부(6)	주민등록표 등·초본, 지방세납세증명서, 방세세목별과세(납세)증명서(자동차세), 지방세세목별과세(납세)증명서(재산세), 상훈수여증명서, 인감증명서
농림수산식품부(5)	선박국적증서(어선), 어선등록필증, 어업면허증, 선적증서, 축산업등록증
지식경제부(2)	공장등록증명서, 석유판매업등록증
보건복지부(7)	국민기초생활수급자증명서, 장애인증명서, 약사면허증, 영양사면허증, 의료기사면허증(안경사, 방사선사), 의료면허증(의사, 치과의사, 한의사, 간호사), 전문의자격증(의사, 치과의사, 한의사)
환경부(6)	사업장폐기물배출자신고증명서, 폐수배출시설설치(허가증/신고증명서), 폐기물수집운반업허가증, 폐기물(중간/최종/종합)처리업허가증, 폐기물처리시설설치승인서, 폐기물처리시설설치신고증명서
고용노동부(1)	국가기술자격취득사항확인서
여성가족부(1)	한부모가족증명서
국토해양부(27)	개별공시지가확인서, 건축물대장, 건축물사용승인서, 건설기계등록원부, 주택건설사업사용검사필증, 자동차등록원부, 이륜자동차사용신고필증, 건축허가서, 선박원부, 토지대장, 임야대장, 지적도, 임야도, 건설업등록증, 토지이용계획확인서, 건설기계등록증, 건설기계검사증, 건설기계사업등록증, 건축사업무신고필증, 자동차등록증, 부동산등기용등록번호증명서, 선박검사증서, 선박국적증서(상선), 토지거래계약허가증, 자동차말소등록사실증명서, 임대사업자등록증, 임시운행허가증
국가보훈처(2)	국가유공자(유족)확인원, 취업지원대상자증명서
국세청(6)	(국세)납세증명서, 소득금액증명, 납세사실증명, 휴업사실증명, 사업자등록증명, 폐업사실증명
관세청(2)	수출신고필증, 수입신고필증
병무청(1)	병적증명서

정보보유기관	공동이용 대상 행정정보(구비서류)
경찰청(1)	자동차운전면허증
소방방재청(1)	안전시설등완비증명서
특허청(4)	특허등록원부, 실용신안등록원부, 디자인등록원부, 상표등록원부
해양경찰청(1)	폐기물위탁·처리신고증명서
대법원(3)	건물등기부등본, 법인등기사항증명서, 토지등기부등본
국민건강보험공단(4)	건강보험증, 건강보험자격득실확인서, 건강보험료납부확인서(개인), 사업장 건강보험료납부확인서
국민연금공단(2)	연금산정용가입내역확인서, 사업장국민연금보험료월별납부증명
근로복지공단(3)	고용보험료완납증명원, 산재보험료완납증명원, 산재보험급여지급확인원
한국가스안전공사(1)	검사증명서발급확인서

자료: 행정정보공동이용추진위원회(http://pr.share.go.kr/)

정보자원과 관련한 국가DB구축과 관련해서는 현재 정부에서는 2009년에 '국가DB구축 중기계획'(2009~2013년)에 따라 총 654억 원을 투입하여 51종(56개 사업과제)의 주요 행정정보와 지식정보의 디지털화를 추진하고 있다. 지식정보DB구축 분야는 총 286억 원을 투입하여 북한 자연인문지리 DB구축, 한국고대사료집성 DB구축 등 31종(34개 사업과제)을 디지털화하고 있으며, 동북아해양위성관측자료 DB구축, 플라즈마 물성정보 DB구축, 국가생명정보 DB구축, 국방학술정보 DB구축, 대한뉴스 DB구축, 장애재활 및 보육지원정보 DB구축, 천문현상정보 DB구축, 학위논문 DB구축, 한국근현대사자료 DB구축 등 9종의 디지털화를 완료하였다.

그리고 행정정보DB구축 분야는 총 368억 원을 투입하여 병적증명서 인터넷발급을 위한 병적DB구축, 소방대상물 DB구축 등 20종(22개 사업과제)에 대한 디지털화를 추진하였으며, 2009년 행정정보DB구축 추진을 통해 주민등록표원장 DB구축, 체류외국인문서 DB구축, 병적증명서 인터넷발급을 위한 병적 DB구축, 과학수사지문 DB구축, 구토지대장DB구축, 역사기후 DB구축, 새주소기반 표준전자지도 DB구축, 보훈행정 DB구축, 수사자료표 DB구축, 선거정당 관련 중요기록물 DB구축 등 10종의 디지털화를 완료한 상황이다.

다수 구축된 국가DB와 점차 증가하는 행정정보 공동이용을 통해 2010년에는 일 평균 구비서류 감축건수가 183,105건으로 2005년에 비해 10만건 이상 줄어들었는데, 이는 약 2,392억원의 비용절감효과를 거둔 것이어서, 전자정부 이후 행정정보 공동이용의 효율성 측면에서는 상당부분 효과를 거두고 있다.

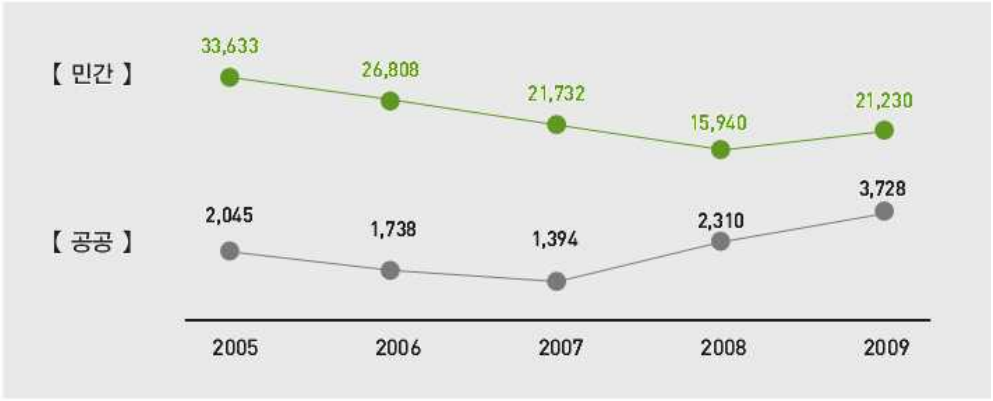
<표 3-2> 행정정보 공동이용 현황

구 분	2005	2006	2007	2008	2009	2010
일평균 구비서류 감축건수(건)	31,681	82,040	105,862	115,035	167,806	183,105
연간 구비서류 감축건수(천 건)	11,563	29,945	38,640	41,988	61,249	66,833

자료: 행정안전부(2011). “국가정보화 백서”.

하지만, 정보자원의 디지털화를 통해 얻어지는 편익 이외에 개인정보의 유출이나 해킹 등 정보자원의 공동이용이나 디지털화로 인해 발생할 수 있는 문제가 과거에 비해 증가하고 있으며, 행정정보 DB가 지속적으로 증가하고 있는 현재 추세로 봤을 때, 이로 인해 발생하는 피해 또한 증가할 것으로 예상된다.

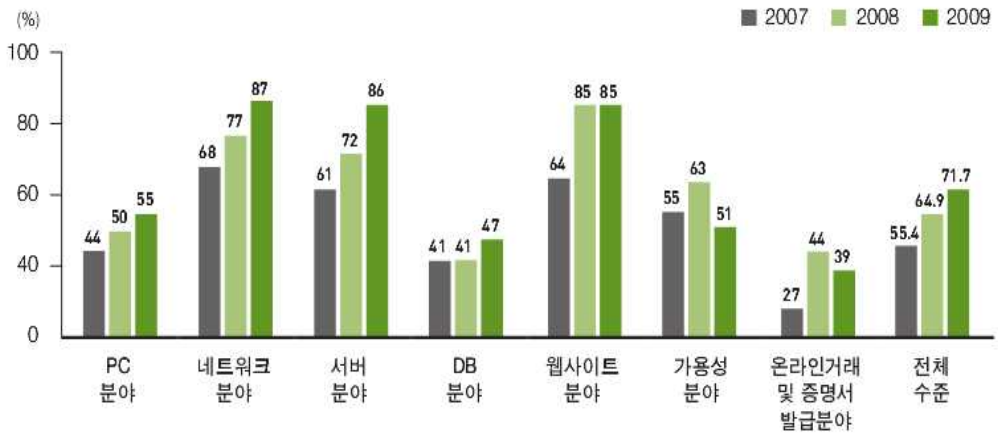
<그림 3-2> 연도별 해킹 등 사이버 침해 사고 발생건수



자료: 행정안전부(2010). “국가정보화에 관한 연차보고서”.

<그림 3-2>를 보면, 민간의 사이버 침해사고는 줄어들고 잇는 추세인데 반해 공공부문에 대한 사이버 침해사고 발생은 오히려 증가하고 있다. 특히 공공부문에 대한 보안 수준 가운데, 정보자원과 관련한 DB 분야가 다른 분야에 비해 낮게 나타나고 있는 등 정보자원의 관리가 상대적으로 취약한 것으로 나타나고 있다.

<그림 3-3> 전자정부 서비스 보안수준 실태조사 결과



자료: 행정안전부(2010). “국가정보화에 관한 연차보고서”.

<표 3-3> 공공분야 사이버침해사고 발생현황

연도별	합계	국가기관	지방자치단체	산하기관	교육기관	기타
2008	7,965(건)	1,187	3,067	1,490	1,867	354
2009	10,659(건)	1,734	4,398	1,287	2,653	587

자료: 행정안전부(2010). “국가정보화에 관한 연차보고서”.

외부에 의한 침해 사고 뿐 아니라 내부의 정보자원 관리에 있어 문제점을 보여주고 있다. 2008년 감사원의 ‘행정정보 공유 및 관리실태’에 따르면, 서울특별시의 모 구청의 경우, 민원사무처리를 위해 공동이용한 행정정보 5,682건 중 민원사무처리부에 기록되지 않은 것이 3,964건 이고,

그중 일반사무를 처리하면서 민원사무를 위해 정보를 열람한 것으로 기록하는 등 실제와 다르게 이용 목적을 기록한 것이 395건, 정보열람 목적을 확인할 수 없는 것이 3,569건으로 나타나 행정정보자원에 대한 공공기관의 관리가 허술한 것으로 나타나고 있다.

국정감사에서는 건강보험공단 내부자에 의한 개인 정보 유출 사례가 2008년 70건에서 2009년 143건으로 늘어나고 있음이 드러나는 등 정보자원을 관리하는 공공기관의 명확하지 못한 정보자원의 관리실태가 나타나고 있다. 외부로 부터의 사이버 침해와 내부자의 허술한 정보자원 관리는 정보유출에 의한 정보인권의 훼손으로 이어지게 되며, 정보자원의 인권적 관리라는 측면에서 문제점을 보여주고 있는 것이다.

3) 정보인권 관련 정부기구와 활동

(1) 정부기구

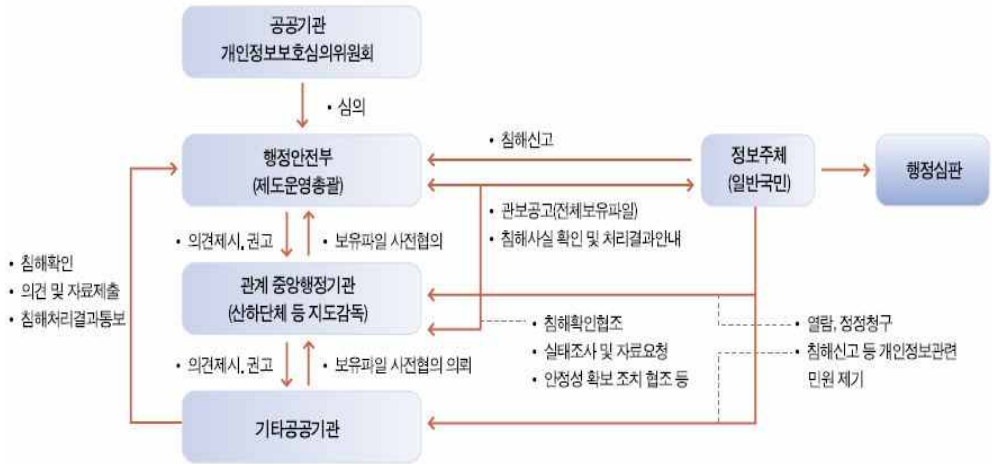
공공기관에서 수집·처리되는 개인정보보호를 위하여「공공기관의 개인정보보호에 관한 법률」에서는 공공부문의 개인정보보호체계를 규정하고 있다. 해당 법률을 기반으로 공공기관에서 다루어지는 정보자원에 대한 개인정보보호 등 인권적 관리를 담당하고 있는 기관은 공공기관 개인정보보호 심의위원회와 행정안전부가 있다.

국무총리 소속하에 행정안전부 차관을 위원장으로 하여 설치된 '공공기관 개인정보보호 심의위원회'는 개인정보보호에 관한 정책 및 제도 개선 처리정보의 이용 및 제공에 대한 공공기관 간의 의견조정 등 공공기관의 개인정보보호에 관한 전반적인 사항을 심의한다(방송통신위원회 외, 2011).

행정안전부는「국가정보화기본법」,「전자정부법」,「전자서명법」,「정보통신기반보호법」,「공공기관의 개인정보보호에 관한 법률」에 의해 해당 업무를 수행하고 있다. 행정안전부는 개인정보보호에 관한 의견

제시 및 권고 개인정보처리에 관한 자료제출을 요구 할 수 있으며 필요시 개인정보처리에 관한 실태점검 등을 실시한다. 또한 개인정보파일보유와 관련하여 공공기관과 사전협의 한 내용 등을 공고하고 인터넷상에서의 개인정보보호를 위하여 관련법령정비 계획수립 시설 및 시스템 구축 등 제반조치를 취한다. 공공기관은 관계 중앙행정기관을 통해 행정안전부와 사전협의를 거친 다음 개인정보파일을 보유할 수 있으며 개인정보보유에 따른 개인정보보호 방침을 수립·공고하고 개인정보파일을 보유목적 외로 이용하거나 제공하지 않아야 한다. 동시에 개인정보를 IT시스템을 통해 처리하거나 정보통신망을 이용해 개인정보를 송·수신할 경우 안전성 확보에 필요한 보호조치를 취하여야 한다. 개인정보주체는 처리정보에 대한 열람, 정정 및 삭제를 청구할 수 있으며 개인정보에 관한 권리 또는 이익을 침해받은 자가 행정안전부에 침해 사실을 신고할 경우 공공기관은 침해사실에 대한 처리결과를 행정안전부를 통해 신고인에게 통지하여야 한다(방송통신위원회 외, 2011; 국가정보보호백서 2011).

<그림 3-4> 공공기관의 개인정보관리 체계



자료: 행정안전부(2008), “공공기관 개인정보관리 업무매뉴얼”.

행정안전부는 최근 대량의 개인정보 유출로 각급 공공기관이 긴장하고 있는 가운데, 기관 스스로 개인정보보호 수준을 진단할 수 있는 프로그램을 운영하고 있다. 해당 진단 프로그램은 개인정보보호 여건, 개인정보 관리, 개인정보 사고대응 등 3개 분야 총 18개 지표로 구성되어, 각 기관의 담당자가 분야별 질문에 기관의 상태를 입력하면 자동으로 취약점을 알려주고 점수로도 환산하여 주고 있다. 개인정보보호 수준진단은 행정안전부가 2008년부터 공공기관을 대상으로 매년 실시해 오고 있으며, 진단 대상을 지속적으로 확대(2008년 286개 → 2009년 695개)하여 2010년에는 공사·공단과 대학을 포함해 1,100여 개 기관으로 대폭 확대하는 등 개인정보보호 수준진단의 대상을 지속적으로 확대하고 있는 추세이다. 중앙부처의 개인정보보호 수준은 진단 첫 해인 2008년 83.9점에서 2009년 92.7점으로 보호 수준이 상승하였으며 2010년에는 더 높은 수준을 예상하고 있다. 2009년 처음으로 실시한 지방자치단체는 87.7점의 수준을 기록한 반면, 공사·공단의 경우 66.4점으로 현저하게 낮은 수준을 나타내고 있다.

<표 3-4> 개인정보 관리실태 점검 항목

구분	중점 점검항목
공공기관	• 개인정보관리 책임관(CPO) 지정 등 개인정보보호 추진체계
	• 개인정보보호 추진계획 수립 등의 관리적 보호조치 사항 - 개인정보 Life-Cycle(수집→보유→이용·제공→파기)에 따른 법규 준수 현황 - 개인정보 이용·제공 및 개인정보 처리의 위탁 관리 사항
	• 개인정보 암호화, 접근권한 등의 기술적 보호조치 사항 - 개인정보 송·수신 시 안전성 확보 여부 - 전산실 보안관리, 입출력자료 보안관리, 단말기 보안조치 등
	• CCTV 설치 · 운영 시 CCTV 보호조치 사항 - CCTV 설치 시 사전 협의, 사전 의견수렴 및 안내판 설치 여부 - 개인화상정보 이용·제공, 파기, 위탁 사항 등
민간기관	• 개인정보 수집 시 정보주체 동의 여부
	• 개인정보 이용 및 제공 시 정보주체 동의 여부
	• 개인정보 위탁 시 정보주체 동의 여부
	• 영업의 양수 등에 따른 개인정보 이전 시 정보주체 동의 여부
	• 개인정보 관리적·기술적 조치
	• 개인정보 파기 및 이용자 권리

자료: 행정안전부(2010). “국가정보화에 관한 연차보고서”.

(2) 활동

행정안전부는 공공 및 민간 사업자 개인정보보호 교육 강화하여 정보자원에 대한 인권적 관리 측면에 대한 인식제고를 위한 활동을 진행하고 있다. 2008년 공공기관을 대상으로 개인정보보호 등 정보인권과 관련한 인식제고 및 전문능력 향상을 위해 '공공기관 개인정보보호 교육 기본계획'을 통보하고 개인정보보호 담당자를 대상으로 동영상 및 각종 교육자료 등을 개발·보급하고 있다. 그리고 2009년 부터는 각급 기관 담당자가 개인정보보호 제도·기술·관리 등에 필요한 전문 능력을 갖추도록 중앙행정기관 및 지방자치단체 등 행정·공공기관 개인정보보호담당자들을 대상으로 개인정보보호 전문교육을 실시하는 등의 노력을 기울이고 있으며, 개인정보 처리단계별 기술적 보호조치 가이드라인을 개발하여 공공기관에 보급하고 있다. 실제 정부중앙청사·대전청사·광주광역시청·부산강서구청·경기도청에서 공공기관 개인정보보호 담당자를 대상으로 순회교육을 실시하고 공공기관의 강의요청에 따라 30여 개 기관 5,000여 명을 대상으로 기관의 특성을 반영한 맞춤형 방문교육을 실시하는 등 정보인권과 관련한 교육을 통해 정보자원의 인권적 측면에 대한 인식제고를 확산시키려 하고 있다.

가이드라인 개발과 교육 뿐 아니라 공공기관의 개인정보보호 중요성에 대한 인식제고 및 개인정보보호 담당자의 업무능력 향상을 위하여 공공기관 워크숍 및 개인정보보호 컨퍼런스를 매년 개최하고 있는데, 2009년 2회(5.21, 10.14)에 걸쳐서 실시한 공공기관 워크숍 및 개인정보보호 컨퍼런스에서는 개인정보관리책임관(CPO : Chief Privacy Officer)을 위한 개인정보보호 관리 정책 및 담당자들에게 개인정보보호 등 정보인권의 중요성에 대한 인식확산을 유도하고 각종 정보보호 신기술을 습득하는 기회를 제공하였다.

정보인권의 중요성에 대한 인식을 확산시키기 위한 교육이나 컨퍼런스 등 공무원의 자율성에 바탕을 둔 활동과 더불어 정보인권 침해 시의 처벌규정과 징계기준을 마련하기도 하였다. 「공공기관의 개인정보보호에 관

한 법률」(제23~24조), 「주민등록법」(제37~ 40조) 등에서 규정하고 있는 처벌규정은 민간분야에 비해 경미한 실정으로, 개인정보를 의도적으로 유출할 경우 등에 대응한 강력한 처벌규정을 마련할 필요가 있는 것으로 보인다. 현재의 징계기준에는 개인정보의 침해유형을 '침해대상'과 '침해자'로 구분하여 침해대상에는 개인정보의 성격(민감정보, 일반정보), 피해규모 등을, 침해자는 침해행위의 유형, 행위자의 고의성(고의, 과실 등) 및 상습성 등을 종합적으로 고려하여 징계수준을 정하도록 하고 있다. 하지만, 최근 공공기관이 보유하고 있는 개인정보 유출 등의 침해사고는 증가하고 있으나, 그에 따른 처벌규정과 징계기준이 미흡하여 적절한 조치가 이루어지지 못하고 있는 상황이다.

3. 정보자원관리의 인권적 모델 도출을 위한 분석틀 구성

<표 3-5>는 본 연구가 제시하고 있는 공공정보자원관리의 인권적 모델을 도출하기 위하여 구성한 모형을 도식적으로 표현한 것이다.[7] 해당 모형의 특징은 정보자원관리의 관리단계로서 정보생애주기와 정보자원의 관리 측면에서 제도, 관리, 기술, 행태 차원을 종합하여 다룰 수 있게 해 준다는 점이다.[8]

정보자원의 관리 측면에서 제도 차원은 정부 전반적인 차원에서 다루어야 할 제도적 이슈를 말하며, 관리 차원은 중앙, 지방자치단체 단위 정보화 담당관 차원에서 다루어야 할 관리적 이슈, 기술 차원은 중앙, 지방자치단체 단위 정보화 부서 차원에서 다루어야 할 기술적 이슈, 행태 차원은 중앙, 지방자치단체 단위 현업 및 정보부서 차원에서 다루어야 할 인식적 이슈를 말한다.

정보의 생애주기 단계 측면에서 수집 및 생성 단계의 중요한 정보자원관리 목표는 정보 시스템에서 사용할 수 있는 형태로의 기록화, 정보의 이중수집에 따른 정부와 민간부문의 불필요한 비용발생 억제, 조직에 유용한 정보의 수집 및 생성이며, 이와 관련된 정보인권 이슈는 명확한 목적과 법적 근거, 정보주체의 동의, 정보주체의 선택권 등을 들 수 있다.

저장 단계의 중요한 정보자원관리 목표는 정보의 분배와 공유를 용이하게 하는 저장, 효율적인 정보재생, 저장의 안정성 확보이며, 이와 관련

---

7) 정보자원관리 모형의 대표적인 예로 Synnott(1987)과 Zachman(1987)의 모형을 들 수 있다. 하지만 범 정부수준의 제도적인 지원부분(법, 규정, 업무지침 등)이 포함되어야 함에도 불구하고 하나의 조직을 대상으로 하여 꾸며진 기존의 모형들은 공공부문의 특수성을 반영하지 못하고 있다.

8) 최근 우리나라가 최근 우리나라 정부가 정보자원관리의 상위적 목표를 달성하기 위해 추진하고 있는 것도 적극적인 Enterprise Architecture(이하 EA)의 도입이다. EA의 구축과 활용시 참조되거나 기준으로 사용되는 내용으로 미국의 연방정부 참조모델 노력을 들 수 있는데 이중에서 성과참조모델(performance Reference Model)을 들 수 있다. 또한 성과참조모델을 기반으로 평가의 내용을 보완하고 새로운 평가모형을 시도한 대표적인 연구로 KISDI(2005~2007), 최홍석 외(2006)을 들 수 있다. 그러나 이러한 모형 역시 정보생애주기와 정보인권적 측면이 반영되지 않아 정보자원관리의 인권적 모델을 도출하기에는 부족한 면이 있다.

된 정보인권 이슈는 안전한 관리를 위한 물리적, 조직적, 기술적 조치 의무, 행정기관의 관리책임 등이다.

분배 및 공유단계의 중요한 정보자원관리 목표는 정보의 원활한 공유를 통한 정보요구 충족, 정보의 효율적 공유를 위한 기술적 환경의 마련, 부적격자의 정보접근 금지 등이며, 이와 관련된 정보인권 이슈는 목적외 이용 금지, 정보주체의 동의, 자기정보 접근 등이다.

사용 단계의 중요한 정보자원관리 목표는 정보 사용을 통한 조직 내외적 가치 창조, 정보오용 및 남용의 방지 등이다. 이와 관련된 정보인권 이슈는 제3자 제공 규제, 목적외 활용 금지, 정보이용에 관한 정보 주체 알 권리, 법적 근거에 따른 이용 등을 들 수 있다.

폐기 단계의 중요한 정보자원관리 목표는 불필요한 정보의 보존에 따른 비용절감, 과도한 정보보안에 따른 사회적 비용의 축소 등이며, 이와 관련된 정보인권 이슈는 불필요한 정보폐기, 복구/재생 불가처리 등을 들 수 있다.

〈표 3-5〉 정부 정보자원관리 현황(As-Is) 파악과 정보자원의 인권적 관리 프레임(To-Be) 도출을 위한 분석틀

	생성 및 수집	저장	분배 및 공유	사용	폐기
IRM 중요 목표	- 정보 시스템에서 사용할 수 있는 형태로의 기록화 - 정보의 이중수집에 따른 정부와 민간부문의 불필요한 비용발생 억제 - 조직에 유용한 정보의 수집 및 생성	- 정보의 분배와 공유를 용이하게 하는 저장 - 효율적인 정보재생 - 저장의 안정성 확보	- 정보의 원활한 공유를 통한 정보요구 충족 - 정보의 효율적 공유를 위한 기술적 환경의 마련 - 부적격자의 정보 접근 금지	- 정보사용을 통한 조직 내외적 가치 창조 - 정보오용 및 남용의 방지	- 불필요한 정보의 보존에 따른 비용절감 - 과도한 정보보안에 따른 사회적 비용의 축소
정보인권 중요 이슈	- 명확한 목적과 법적 근거 - 정보주체의 동의 - 정보주체의 선택권	- 안전한 관리를 위한 물리적, 조직적, 기술적 조치의무 - 행정기관의 관리 책임	- 목적외 이용 금지 - 정보주체의 동의 - 자기정보 접근	- 제3자 제공 규제 - 목적외 활용 금지 - 정보이용에 관한 정보 주체 알권리 - 법적 근거에 따른 이용	- 불필요한 정보폐기 - 복구/재생 불가처리
제도 layer 분석지표	- 중앙관리기구(존재여부, 담당 범위, 권한 정도) - 외적 통제절차(존재여부, 수집동의 과정, 수집 기획 참여 과정)	- 보안관리(지침 존재, 관리 정도, 시스템 상 기록관리) - 외부적 통제 절차(유출 피해 감시)	- 시스템 연계(공공부문/민간부문 연계범위) - 표준관리지침(존재여부) - 중앙관리기구(기구, 권한, 관리) - 정보공유의 범위(기관수, 업무수, 가치창조, 비용부담) - 공유제한(열람권, 공유절차 및 기록)	- 정보의 질 관리(최신성, 정확성) - 오남용 관리(오남용 감시 절차, 보고 체계) - 목적외 사용통제(통제규정 존재, 자율적 규제 관행) - 외부적 통제절차(접근대상, 접근편의, 통제권한 정도)	- 관리체계(기구존재여부, 관련규정 존재여부, 폐기정보 목록관리, 폐기 보고 체계 존재) - 재생 및 재사용가능성 평가(보존비용의 부담, 재생, 재사용여부 평가)
관리 layer 분석지표	- 단위별 관리지침(책임자 권한, 강제성 정도, 공개정도)	- 보안관리(지침 존재, 관리 정도, 시스템 상 기록관리) - 외부적 통제 절차(유출 피해 감시)	- 공유제한(열람권, 공유절차 및 기록) - 외적 통제절차(아웃소싱 감독) - 외적 통제절차(공유범위 및 과정 참여)	- 정보의 질 관리(최신성, 정확성) - 오남용 관리(오남용 감시 절차, 보고 체계) - 목적외 사용통제(통제규정 존재, 자율적 규제 관행) - 외부적 통제절차(접근대상, 접근편의, 통제권한 정도)	- 관리체계(기구존재여부, 관련규정 존재여부, 폐기정보 목록관리, 폐기 보고 체계 존재) - 재생 및 재사용가능성 평가(보존비용의 부담, 재생, 재사용여부 평가)
기술 layer 분석지표	- 메타DB(존재 여부, 관리 주체, 포함 범위, 공개정도)	- 보안관리(지침 존재, 관리 정도, 시스템 상 기록관리) - 외부적 통제 절차(유출 피해 감시)	- 공유제한(열람권, 공유절차 및 기록) - 외적 통제절차(아웃소싱 감독) - 외적 통제절차(공유범위 및 과정 참여)	- 정보의 질 관리(최신성, 정확성) - 오남용 관리(오남용 감시 절차, 보고 체계) - 목적외 사용통제(통제규정 존재, 자율적 규제 관행) - 외부적 통제절차(접근대상, 접근편의, 통제권한 정도)	- 관리체계(기구존재여부, 관련규정 존재여부, 폐기정보 목록관리, 폐기 보고 체계 존재) - 재생 및 재사용가능성 평가(보존비용의 부담, 재생, 재사용여부 평가)
행태 layer 분석지표	- 제도, 관리, 기술 layer와 관련된 설문문항[9]	- 제도, 관리, 기술 layer와 관련된 설문문항	- 제도, 관리, 기술 layer와 관련된 설문문항	- 제도, 관리, 기술 layer와 관련된 설문문항	- 제도, 관리, 기술 layer와 관련된 설문문항

9) 구체적인 내용은 본 연구보고서의 7장을 참조하고, 설문지 전문은 부록 1을 참조하도록 한다.

Ⅳ. 우리나라 정보자원관리의 법규정 분석

정보화시대의 정부는 방대한 양의 정보를 수집, 보관, 처리하는 정보집약적 행위자이며, 정보의 관리는 정부 생산성과 국민 신뢰 향상을 위해 이미 그 중요성이 부각되었다. 우리나라도 정부개혁으로 정보자원의 효율적 관리를 위한 국가행정전산망사업 뿐 아니라 이에 따라 정보자원 관리를 위한 각종 법제를 마련함으로써 합리적인 정보자원관리를 시도하였다.

공공기관의 개인정보보호에 관한 법률과 전자정부법에서 주로 정보자원관리에 대해 규정하고 있으며, 주민등록법, 민원사무처리에 관한 법률, 국가공무원법, 공직자윤리법 등 기타 부분적으로 규율하고 있다. 그 중에서도 행정업무의 전자적 처리를 위한 기본원칙 및 추진방법 등을 포괄적으로 규정하고 있는 전자정부법, 2011년 9월 30일부터 시행되는 개인정보보호법, 공공기관이 준수해야 할 개인정보파일 관리에 관한 세부사항을 규정한 행정안전부 개인정보보호를 위한 기본지침에 대해 살펴보겠다.

1. 전자정부법

1990년대 말 전자정부가 국가의 주요 정책 아젠다로 등장하면서 학계, 정부 등 각계에서 전자정부법 제정 필요성을 제기함에 따라 정부와 입법부를 중심으로 한 전자정부법의 지속적 입법 추진 시도가 있었다. 이에 따라 2001년 행정기관의 생산성 및 투명성, 민주성을 높여 지식정보화시대 국민 삶의 질을 향상시키는 것을 목적으로 전자정부법을 제정하였으며, 내부적으로는 정보화관련 법률의 간소화 및 통·폐합, 외부적으로는 IT 정책 환경의 변화에 적극적인 대응이라는 배경에서 2010년 제 3차 전부개정에 이어 2011년 법률의 일부개정이 있었다.

정보사회로의 변화에 대응하여 정보기술을 적극적으로 반영한 전자정부를 구현하기 위한 전자정부법 시행령(전부개정)의 주요내용은 민원업무처리에 전자 문서의 활용, 전자민원창구의 운영, 전자정부서비스의 통폐

합 등 효율적 관리, 행정정보 공동이용 등에 관해 다루고 있다. 그 구체적인 내용을 살펴보면 첫째, 민원의 신청·처리에 전자화문서 활용(제5조, 제6조)는 민원업무 처리에 있어 각종 종이서류를 전자문서로 변환하여 신청하게 하거나 통지할 수 있도록 하여 모든 민원을 온라인으로 처리할 수 있도록 한 것이다. 둘째, 전자민원창구의 운영(제9조, 제10조)에서는 행정기관의 장은 소관 민원을 전자적으로 처리할 수 있도록 전자민원창구를 설치 운영하고, 이는 통합전자민원창구와 효율적으로 연계되도록 해야 한다는 것이다. 셋째, 전자정부서비스의 통폐합 등 효율적 관리(제18조, 제19조)에서는 전자정부서비스 제공 및 이용실태를 조사·분석하여 서비스의 중복·유사성, 접근 편의성, 이용률 등을 고려하여 통합 또는 폐기 방안을 권고할 수 있도록 한다.

넷째, 행정정보 공동이용 대상기관의 확대(제39조)에서는 행정정보를 공동 이용할 수 있는 기관을 명기하며, 개인정보의 유출 및 오용·남용을 예방하기 위해 행정안전부장관이 사전 및 사후에 개인정보 보호조치 등을 확인하도록 한다. 다섯째, 행정정보 공동이용의 방법 및 절차(제44조, 제45조, 제47조)는 행정정보의 안전성·신뢰성을 확보할 수 있도록 하기 위해, 행정정보의 공동이용기관은 그 목적 및 업무를 기입한 신청서를 제출해야 하며, 행정안전부장관은 해당 행정정보의 내용 및 열람자의 범위 제한 등을 조건으로 이를 승인하고, 승인받지 않은 목적으로 행정정보를 이용한 경우 이를 철회할 수 있도록 하고 있다. 여섯째, 정보주체의 사전동의 및 열람신청(제49조, 제50조)에서는 정보주체에게 이익이 되는 것이 명백한 경우 등 행정기관 등이 정보주체의 사전동의를 받지 않고 행정정보를 공동 이용할 수 있는 경우를 규정하고, 정보주체의 사전동의 없이 공동 이용할 수 있는 소관 업무와 행정정보의 목록을 인터넷에 게시하도록 하였다.

일곱째, 정보기술아키텍처 및 정보시스템 감리(제53~56조, 제71~77조)에서는 정보기술아키텍처(정보화설계도) 도입·운영 및 정보시스템에 대한 감리제도의 운영 등에 관한 주요 내용을 통합적으로 규정하였다. 여덟째,

각종 정보자원의 효율적 관리(제60조, 제61조, 제66조)는 법률에서 여러 행정기관 등이 사용할 수 있는 시스템 및 소프트웨어 등의 정보자원을 공유서비스로 지정·변경하거나 취소할 수 있도록 함에 따라 공유서비스 지정·변경신청서에 포함되어야 할 사항과 지정취소기준 등을 정하고, 정보자원을 통합 관리하기위한 기준에 포함될 사항으로 정보시스템의 규모, 용량 및 활용도 등을 규정하였다.

전자정부법의 제 36조 행정정보의 효율적 관리 및 이용에 관해 이미 보유하고 있는 행정정보를 다른 행정기관이 공동으로 이용하고, 이와 같은 내용의 정보를 따로 수집할 수 없도록 하여, 행정기관 간 정보 이용의 효율성을 강조하였으며 개인정보의 무분별한 중복수집으로 인한 개인정보 침해를 지양하고 있다. 정보자원생애주기의 저장단계와 관련하여 제 35조 금지행위, 제 54조 통합관리, 56조 정보통신망 종합대책이 규정하고 있다. 이 조항에서 행정기관이 승인받지 않은 방식의 저장장치에의 행정정보를 저장하는 행위를 금지하고, 관련 행정기관은 행정정보의 안전성, 신뢰성 확보를 위한 보안대책을 마련해야 하며, 행정정보를 보유한 각 행정기관의 장은 보유정보를 체계적으로 작성 및 관리하고, 정보자원을 통합적으로 구축하여 관리하도록 하고 있다. 제 32조 전자적 업무수행, 제 34조 업무담당자의 신원 및 접근권한, 36조 행정정보의 효율적 관리 및 이용, 39조 행정정보 공동이용의 신청 및 승인, 제 51조 공유서비스의 지정 및 활용 부분은 정보의 분배/공유와 관련한 내용을 규정한다.

행정기관의 장은 업무담당자가 온라인 접속을 통해 행정정보를 다루게 될 경우, 정보에의 불법적인 접근을 막기 위한 보안대책을 수립하도록 하고 있으며, 업무담당자의 신원 및 접근권한을 법률로서 관리하도록 하고 있다. 또한 2010년 개정된 제 36조에 따르면 행정정보를 수집・보유하고 있는 행정기관의 장은 다른 행정기관 및 은행 그리고 법인 단체나 기관으로 하여금 행정정보를 공동으로 이용할 수 있게 하여, 행정정보 공동이용 기관의 범위를 넓혔다. 또한 공동이용센터를 통해 행정정보를 이용하려는 기관은 그 목적, 범위 및 이용 방식을 알리고 행정안전부 장관의 공동이

용 승인을 받아야 한다. 이로서 기관별 중복수집 및 관리로 인해 낭비되는 예산을 절감할 수 있고, 불필요한 개인정보 누출을 줄일 수 있게 되었으며, 공동 이용의 범위를 민간으로까지 넓혀 기존의 정보로 인한 부가가치를 창출할 수 있게 되었다. 이로 인해 발생할 수 있는 정보보안문제에 대해 행정기관 간 공동이용의 승인조건을 법률로 규정하도록 하고 있고, 적절한 절차를 통해 행정안전부 장관의 승인을 요구하고 있다.

정보의 사용에 관해서는 제 36조, 제 42조, 제 43조, 제 51조에 해당한다. 이를 통해 이용기관이 행정정보공동이용센터를 통해 개인정보가 포함된 행정정보를 이용할 때에는 정보주체가 이를 알 수 있도록 사전에 정보주체의 동의가 있어야 하며, 정당한 이유 없이 행정정보가 누설, 행정정보를 권한 없이 처리하거나 권한 범위를 넘어서는 처리, 권한 없이 다른 사람으로 하여금 이용하게 하는 행위 또는 거짓이나 부정한 방법으로 행정기관 등으로부터 행정정보를 제공받거나 열람하는 행위 등을 금지하고 있다. 이러한 조항은 정보주체의 개인정보자기결정권을 인정한 것으로 판단되며, 개인정보가 공동으로 이용되더라도 부당한 개인정보의 접근 및 처리, 활용을 금지함으로써 정보관리의 능률성을 강조하면서도 개인의 정보인권을 보장하는 조항으로 볼 수 있다.

전자정부법에 정보의 폐기에 관한 구체적인 조항은 보이지 않으나 제 23조 전자정부서비스의 효율적 관리에서 서로 유사하거나 중복되는 경우 또는 운영가치가 낮은 경우에 국가정보화전략위원회의 심의를 거쳐 서비스를 통합 또는 폐기 등의 개선방안을 권고할 수 있도록 하고 있다. 이는 행정정보의 폐기에 관한 구체적 규정은 아니지만 서비스의 통합 및 폐기 방안에는 정보의 이관 또는 보존의 내용이 포함되어야 함을 규정하고 있다.

한국의 전자정부법의 주요내용을 정보자원생애주기별로 분류하여 정리하면 다음과 같다.

<표 4-1> 전자정부법의 정보자원생애주기에 따른 분류

정보자원 생애주기	전자정부법	
수집/생성	행정기관 등의 장은 수집·보유하고 있는 행정정보를 다른 행정기관과 공동으로 이용하고, 신뢰할 수 있는 정보를 제공받을 경우, 같은 내용의 정보를 따로 수집할 수 없음	36조 행정정보의 효율적 관리 및 이용
저장	행정기관이 승인받지 않은 방식으로 정보시스템 또는 저장장치에 행정정보의 내용을 저장하는 행위를 금지	제35조 금지행위
	행정기관 등의 장은 해당 기관이 보유하고 있는 정보자원의 현황 및 통계자료를 체계적으로 작성·관리하여야 하고, 정보자원을 통합적으로 구축·관리	제54조 정보자원 통합관리
	국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부 및 행정기관의 장은 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련	제56조 정보통신망 보안대책 수립·시행
분배/공유	행정기관의 장은 소속 직원이 정보통신망을 이용한 온라인 원격근무를 하게 될 경우, 정보통신망에 대한 불법적인 접근의 방지와 그 밖의 보호대책을 마련	제32조 전자적 업무수행
	행정기관 등의 장은 전자적 업무의 수행을 위하여 정보시스템 또는 행정정보를 이용하려는 업무담당자 등의 본인 여부 및 접근권한 등을 법률이 정하는 방법으로 관리 및 확인	제34조 업무담당자의 신원 및 접근권한
	행정정보를 수집·보유하고 있는 행정기관 등의 장은 다른 행정기관등과 인가 받은 은행 및 법인·단체 또는 기관으로 하여금 행정정보보유기관의 행정정보를 공동으로 이용하게 할 수 있음<개정 2010.5.17>	제36조 행정정보의 효율적 관리 및 이용
	공동이용센터를 통하여 행정정보를 이용하려는 기관은 공동이용 대상 행정정보와 그 범위, 공동이용의 목적·방식, 행정정보보유기관 등을 특정하여 행정안전부장관에게 공동이용을 신청하여야 하며, 행정안전부장관은 신청을 받으면 공동이용의 조건 등을 정하여 행정정보 공동이용을 승인(행정정보가 다른 법률 또는 다른 법률에서 위임한 명령에서 비밀 또는 비공개 사항으로 규정된 경우 등은 제외)	제39조 행정정보 공동이용의 신청·승인

	행정정보가 개인정보파일인 경우에는 개인정보 보호위원회의 심의·의결을 거쳐 제2항에 따른 공동이용 승인	
	중앙사무관장기관의 장은 보유한 정보자원 중 여러 행정기관 등 또는 민간에서 활용할 수 있는 표준화된 정보자원을 관계 행정기관 등의 장과 협의하여 지정, 변경 또는 취소할 수 있고, 그 중 우수한 정보자원을 발굴·선정하여 다른 행정기관 등에 보급	제51조 공유서비스의 지정 및 활용
사용	행정기관 등의 장은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관등과 공동으로 이용	제35조 금지행위
	이용기관이 공동이용센터를 통하여 개인정보가 포함된 행정정보를 공동이용 할 때에는 정보주체의 사항을 알 수 있도록 정보주체의 사전동의를 받아야 함	제36조 행정정보의 효율적 관리 및 이용
	공개되어서는 안 되는 행정정보를 정당한 이유 없이 누설, 행정정보를 권한 없이 처리하거나 권한 범위를 넘어서 처리, 행정정보를 권한 없이 다른 사람으로 하여금 이용하게 하는 행위, 거짓이나 부정한 방법으로 행정기관 등으로부터 행정정보를 제공받거나 열람하는 행위 등을 금지	제42조 정보주체의 사전동의
	공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 이용기관, 공동이용의 목적 등에 대한 열람을 행정안전부장관 또는 해당 이용기관의 장에게 신청	제43조 정보주체의 열람청구권
	중앙사무관장기관의 장은 우수한 정보자원을 발굴·선정하여 다른 행정기관 등에 보급	제51조 공유서비스의 지정 및 활용
폐기	-	

2. 개인정보보호법

2009년부터 입법논의가 시작된 한국의 개인정보보호법은 모든 공공과 민간에 통합 규율로 법 적용 대상을 확대하였으며, 개별법간 상이한 처리기준에 대해 개인정보 수집, 이용, 처리, 파기의 각 단계별 공통된 보호기준과 원칙을 규율하게 된다. 또한 개인정보 열람・정정・삭제 및 처리정지권 보장, 개인정보 유출시 통지・신고제도, 집단분쟁조정제도, 권리침해 중지를 구하는 단체소송을 도입하여 국민 피해구제가 강화될 것이다.

또한 주민등록번호 등 고유식별번호의 처리를 엄격히 제한하고, 공공기관의 개인정보 영향평가를 의무화하는 등의 개인정보 침해사고 예방과 국가의 개인정보보호 수준이 강화될 전망이다. 한편 대통령소속으로 '개인정보 보호위원회'를 구성하여 주요 정책사안을 심의・의결 하도록 하고, 헌법기관, 중앙행정기관, 지자체의 법규위반 사항에 대해 시정조치 권고권, 국회 연차보고서 제출권과 자료제출 요구권을 부여하였다. 또한 '개인정보 분쟁조정위원회'를 확대 설치하여 정책과 의사결정의 독립성을 크게 강화했다. 이 법의 제정으로 현행 '공공기관의 개인정보보호에 관한 법률' 전부와 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'의 일부 조항이 흡수되어 폐지된다.

개인정보보호법 주요내용은 다음과 같다. 첫째, 개인정보 보호법안의 적용대상을 공공・민간부문의 모든 개인정보처리자로 함(안 제2조)에서는 개인정보를 처리하는 자는 동법에 따른 개인정보 보호규정을 준수하도록 하고, 전자적으로 처리되는 개인정보 외에 수기(手記) 문서까지 개인정보의 보호범위에 포함하도록 하여 그동안 개인정보보호 법률의 사각지대에 있었던 사회 전반의 개인정보보호를 다루도록 하였다.

둘째, 개인정보 보호위원회 설치안(제7조・제8조)는 개인정보 보호와 관련한 중요 사항에 대하여 의사결정의 신중성・전문성・객관성을 확보 개인정보 보호위원회를 두고, 개인정보 보호위원회에 사무국을 설치하는 내용을 규정한다. 셋째, 개인정보의 수집, 이용, 제공 등 단계별 보호기준

마련 (안 제15조부터 제22조까지)에서는 개인정보를 수집, 이용하거나 제3자에게 제공할 경우에는 정보주체의 동의 등을 얻도록 하고, 개인정보의 수집 · 이용 목적의 달성 등으로 불필요하게 된 때에는 지체 없이 개인정보를 파기하도록 하며, 개인정보의 수집, 이용, 제공, 파기에 이르는 각 단계별로 개인정보처리자가 준수하여야 할 처리기준을 구체적으로 규정하였다.

넷째, 고유식별정보의 처리제한 강화(안 제24조)은 주민등록번호 등 법령에 의해 개인을 고유하게 구별하기 위해 부여된 고유식별번호는 원칙적으로 처리를 금지하고 별도의 동의를 얻거나 법령에 의한 경우 등에 한해 제한적으로 예외를 인정하도록 하고 있다. 즉, 주민등록번호의 광범위한 사용 관행을 제한함으로써 주민등록번호의 오·남용을 방지하도록 하고 있다. 다섯째, 영상정보처리기기의 설치제한 근거마련(안 제25조)에서는 영상정보처리기기 운영자는 일반적으로 공개된 장소에 범죄 예방 등 특정 목적으로만 영상정보처리기기를 설치하도록 하고, 영상정보처리기기의 설치 · 운영 근거를 구체화함으로써, 폐쇄 회로 텔레비전 등 영상정보처리기기의 무분별한 설치를 방지하도록 하였다.

여섯째, 개인정보 영향평가제도 도입(안 제33조)은 개인정보처리자는 개인정보파일의 구축 · 확대 등이 개인정보 보호에 영향을 미칠 우려가 크다고 판단될 경우 자율적으로 영향평가를 수행할 수 있도록 하되, 공공기관은 정보주체의 권리침해 우려가 큰 일정한 사유에 해당될 때에는 영향평가 수행을 의무화한다. 이 내용은 개인정보 침해로 인한 피해의 원상회복과 같은 사후구제가 어려우므로 영향평가를 통해 위험요인을 분석하고 이를 조기에 제거하여 개인정보 유출 및 오 · 남용 등의 피해를 효과적으로 예방하기 위한 목적이다.

일곱째, 개인정보 유출사실의 통지 신고제도 도입(안 제34조)은 개인정보처리자는 개인정보 유출 사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지하고, 일정 규모 이상의 개인정보가 유출된 때에는 전문기관에 신고하도록 하는 한편, 피해의 최소화를 위해 필요한 조

치를 취하도록 하는 내용을 규정한다. 이러한 내용은 개인정보 유출로 인한 피해의 확산을 방지하며, 신속한 조치 및 정보주체의 효과적 권리 구제를 위한 시행 규정이라고 할 수 있다.

여덟째, 정보주체의 권리 보장(안 제35조부터 제39조까지)에서는 정보주체에게 개인정보의 열람청구권, 정정·삭제 청구권, 처리정지 요구권 등을 부여하고, 그 권리행사 방법 등을 규정함으로써 정보주체가 개인정보에 대한 자기통제권을 실현할 수 있도록 하였다. 아홉째, 개인정보 분쟁조정위원회 설치 및 집단분쟁조정제도의 도입(안 제40조부터 제50조까지)에서는 개인정보 관련 분쟁의 공정하고 조속한 해결 및 침해의 신속한 구제를 위해 개인정보 분쟁조정위원회의 설치와 집단분쟁조정제도를 도입의 내용을 규정한다.

열 번째, 동법은 개인정보 침해사실의 신고(안 제62조)를 통해, 개인정보처리자로부터 권리 또는 이익을 침해받은 자는 행정안전부장관에게 그 침해사실을 신고할 수 있으며, 행정안전부장관은 신고 접수 및 업무처리 지원을 위해 개인정보 침해신고센터를 설치·운영하도록 하는 내용을 규정하고 있다. 개인정보보호법 제 3조, 제 15조, 제 16조에서는 개인정보이 수집 시 그 목적을 명확히 하고, 목적에 부합하는 범위에서 최소한의 개인정보만을 정당한 절차를 통해 수집하도록 하며, 정보주체의 동의가 있어야 함을 규정하고 있다.

또한 정보주체가 개인정보 수집에 동의하지 않는다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부할 수 없도록 한다. 정보의 저장과 관련해서 제 3조, 제 29조, 제 33조에서 정보주체의 권리가 침해되지 않도록 개인정보를 안전하게 관리할 것을 규정하고, 공공기관은 정보주체의 권리침해 우려가 클 경우 개인정보영향평가의 수행을 의무화하도록 하고 있다. 제 17조는 정보주체의 동의가 있거나 법령상 의무 준수를 위해 불가피한 경우, 개인정보를 제 3자에게 제공할 수 있으며, 정보주체에게 정보수령자와 개인정보 이용 목적 등을 알리도록 하고 있다.

정보의 사용과 관련해 제 3조 개인정보보호원칙에서는 개인의 사생활

침해를 최소화하는 범위 내, 개인정보의 처리 목적에 필요한 범위 내에서 적합하게 개인정보를 처리하여야 하며, 목적외의 용도로 활용될 수 없도록 규정하고 있다. 또 전술한 17조는 정보의 사용에도 관련된다. 제 5조 국가의 책무에서 국가와 지방자치단체는 개인정보의 목적 외 수집, 오·남용, 무분별한 감시 및 추적 등에 따른 폐해를 방지할 의무를 지니고 있음을 명시하고 있다. 한국의 개인정보보호법의 특징적인 부분은 정보자원 생애주기의 폐기에 관한 규정이 보다 구체적으로 보여진다는 점이다. 제 21조에 정보의 파기에 관한 사항을 규정하고 있는데, 그 내용을 살펴보면, 보유기관이 경과 하거나 개인정보의 처리목적을 달성한 경우와 같이 개인정보가 불필요하게 되었을 때 그 정보를 파기하도록 하고 있다. 개인정보의 파기방법 및 절차 등 필요한 사항은 법률로 정하도록 하며, 개인정보처리자가 개인정보를 보존하여야 할 경우 해당 개인정보파일을 다른 정보와 분리하여 저장 및 관리하도록 한다. 한국의 개인정보보호법의 주요내용을 정보자원생애주기별로 분류하여 정리하면 다음과 같다.

〈표 4-2〉 개인정보보호법의 정보자원생애주기에 따른 분류

정보자원 생애주기	개인정보보호법	
수집/생성	개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 함	제3조 개인정보 보호 원칙
	정보주체의 동의를 받은 경우, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 등 법률이 정하는 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있음	제15조 개인정보의 수집·이용
	개인정보를 수집하는 경우, 그 목적에 필요한 최소한의 개인정보를 수집하여야 함	제16조 개인정보의 수집 제한
	정보주체가 개인정보 수집에 동의하지 않는다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부해서는 안 됨	
저장	개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 함	제3조 개인정보 보호 원칙
	개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 법률이 정하는 대로 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 함	제29조 안전조치 의무
	공공기관은 정보주체의 권리침해 우려가 큰 일정한 사유에 해당될 때에는 영향평가 수행을 의무화 함	제33조 개인정보영향평가제도 도입
분배/공유	법률이 정하는 경우에 정보주체의 개인정보를 제3자에게 제공할 수 있음(정보주체의 동의를 받은 경우, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 등)	제17조 개인정보의 제공
	동의를 받을 때에는 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적 등의 사항을 정보주체에게 알려야 함	

사용	개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적외의 용도로 활용해서는 안 됨	제3조 개인정보 보호 원칙
	정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 함	
	국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여야 함	제5조 국가 등의 책무
	정보주체의 동의를 받은 경우, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 등의 경우 정보주체의 개인정보를 제3자에게 제공할 수 있음	제17조 개인정보의 제공
	개인정보사용 동의를 받을 때에는 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적 등의 사항을 정보주체에게 알려야 함	
폐기	보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때 그 개인정보를 파기하여야 함	제21조 개인정보의 파기
	개인정보를 파기할 때에는 복구 또는 재생되지 않도록 조치 함	
	개인정보처리자가 개인정보를 보존하여야 하는 경우, 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하여야 함	
	개인정보의 파기방법 및 절차 등에 필요한 사항은 법률로 정함	

3. 개인정보 보호를 위한 기본 지침

행정안전부는 공공기관의 개인정보파일 관리수준을 제고하고자 개인정보 파일 관리기준 및 방법에 대한 지침을 2008년 3월부터 제정하여 시행하고 있다. 이 지침은 공공기관이 준수해야 할 개인정보파일의 관리에 관한 세부사항을 규정하고 있으며, 적용대상은 정부조직법에 따른 중앙행정기관 및 그 소속기관, 지방자치단체, 교육기관, 법률에 따른 각 급 학교, 공공단체 중 대통령령으로 정하는 기관이다(금융실명거래 및 비밀보장에 관한 법률에 따른 금융기관은 제외).

개인정보보호법을 적용받는 공공기관에서 업무처리를 목적으로 보유 및 처리하고 있는 전자적 형태의 개인정보파일에 대하여 적용하고 있으나, 통계법에 의해 수집되는 개인정보 및 국가안전보장과 관련된 정보분석을 목적으로 수집되는 개인정보를 제외한다.

행정안전부의 개인정보보호 기본 지침은 개인정보처리에 관한 기관의 내부지침으로서 전자정부법과 개인정보보호법의 조항보다 구체적인 관리 규율이 수행되고 있다. 정보자원생애주기에 따라 살펴보면, 정보의 수집/생성에 있어 새롭게 수집하는 개인정보에 대해 변경 사항이 발생할 경우, 사전협의서를 작성하여 행정안전부와 협의하도록 하고 있다.

정보의 저장과 관련해서 정보의 보유기간 및 개인정보 파일 현황 관리, 열람제한과 정보의 정정 및 삭제에 관한 내용을 담고 있다. 보유기간은 보유목적에 부합된 최소기간으로 하며, 특별한 경우를 제외하고는 2주년을 주기로 정보주체의 재동의(再同意) 절차를 거쳐 정보주체의 동의가 있은 후에만 정보를 계속 보유할 수 있다.

또한 보유 공공기관이 소관업무 수행을 위해 보유하는 개인정보파일에 대한 종합적인 사항을 일정한 양식에 따라 취급자별로 개인정보파일대장을 작성하여 보관하며, 개인정보 총괄부서는 정보의 보유 및 파기 현황을 주기적으로 조사하여 그 결과를 기관 홈페이지 개인정보보호방침에 포함하여 관리하도록 하고 있다. 또 중앙행정기관 및 최상위 기관은 하위기관의

개인정보 보유 및 파기 현황을 주기적으로 조사 및 관리하여 행정안전부에 보고하며, 행정안전부는 매년 전 공공기관의 개인정보파일 보유현황을 조사하여 관보에 공고하여야 한다. 정보주체의 개인정보자기결정권과 관련하여 공공기관이 보유하고 있는 개인정보 파일의 경우 정보주체(대리인 포함)에게 열람을 제한할 수 없으며, 개인정보를 열람한 주체가 본인의 처리정보에 대해 정정 및 삭제를 청구한 경우 즉시 조치를 취하도록 하고 있다. 동 지침의 파일 이용 및 제공 관리 부분은 정보의 분배/공유에 관한 내용을 담고 있다. 다른 기관이 보유정보에 대해 정보의 제공을 요청할 경우 문서를 통해 보유 목적 범위 등을 제출 받아 적정 여부를 확인해야 한다.

한편 보유기관은 정보를 다른 기관에 정보를 제공하고자 할 때, 최소한의 범위로 제한하여 제공하고, 보유기관의 동의 없이 제 3자에게 제공할 수 없도록 한다. 그러나 개인정보보호법 제 10조 3항에 해당하는 사항(정보주체의 동의가 있거나, 조약, 국제협정의 이행을 위해 외국정부 또는 국제기구에 제공하는 경우, 범죄수사에 필요한 경우 등)은 예외적으로 이용·제공할 수 있으며, 이는 '처리정보이용·제공 대장'에 기록하여 관리해야 한다. 정보의 사용단계는 분배/공유 단계와 내용상의 중복이 있다.

개인정보파일을 생성하여 처리하는 부서의 장은 개인정보관리대장에 기록 하여 관리하고, 다른 기관이 이용 및 제공을 요청할 경우 문서를 통해 보유 목적과 범위 등을 제출받아 적정 여부를 확인하고, 보유정보를 제공하고자 하는 경우 최소한의 범위 내에서 제공하도록 한다. 정보자원 생애주기의 마지막단계의 폐기에 관해 지침은 구체적인 내용을 제시하고 있다. 개별 개인정보에 대한 변경 또는 수정, 보유기간 만료 등 보유 불필요, 삭제 청구가 발생되었을 때 이를 반영하여 관리하며, 개별 개인정보를 삭제할 경우에는 재사용이 불가능하도록 영구 삭제하도록 한다. 파기는 복구할 수 없는 기술적 방법을 통해 원본 및 백업본을 파기하도록 하고 있다.

또한 파기 부서장은 파기사항에 대해 '입출력관리자료대장'에 기록하며, 중앙기관, 광영자치단체, 시도교육청 등 최상위 기관은 하위기관의 개인정보 보유·파기 현황을 주기적으로 조사 및 관리하고, 행정안전부는 이

에 대한 사항을 조사하여 관보에 공고해야 한다. 그러나 정보주체의 삭제 청구가 있어도 다른 법률에 따라 정보를 보유해야 할 경우, 해당 개인정보 항목에 대한 삭제를 거부할 수 있는데, 이러한 제한 사유에 대해 결정의 내용 및 사유와 당해 결정에 대한 불복절차에 관한 사항을 기재한 '정정·삭제거부 등 결정 통지서'를 청구인에게 송부해야 한다.

공공기관의 개인정보보호 지침의 주요내용을 정보자원생애주기별로 분류하여 정리하면 다음과 같다.

<표 4-3> 공공기관 개인정보보호 지침의 정보자원생애주기에 따른 분류

정보자원 생애주기	행정안전부 개인정보보호 지침	
수집/생성	개인정보를 새로이 수집하거나 보유 개인정보파일에 관한 사항 변경 시, 사전협의서를 작성하여 행정안전부와 협의	파일사전 협의
저장	보유기간은 보유목적에 부합된 최소기간으로 산정	보유기간
	정책고객, 홈페이지 회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속 보유	
	공공기관이 소관업무 수행을위해 보유하는 개인정보파일에 대한 종합적인 사항을 일정한 양식에 따라 개인정보 취급자별로 개인정보파일대장을 작성하여 보관	개인정보 파일대장
	개인정보 총괄부서는 보유·파기 현황을 주기적으로 조사하여 그 결과를 기관 홈페이지 개인정보보호방침에 포함하여 관리	파일현황 관리
	중앙행정기관, 광역자치단체, 시도교육청 등 최상위기관은 하위기관의 보유·파기현황을 주기적으로 조사 및 관리	
	행정안전부는 매년 전 공공기관의 개인정보파일 보유현황을 조사하여 관보에 공고하며, 최상위기관은 하위, 산하기관에 대한 보유 및 파기현황 제출에 협조해야 함	파일현황 제출
	공공기관이 보유하고 있는 개인정보 파일의 경우 처리정보의 당사자인 정보주체(대리인 포함)에게 열람을 제한할 수 없음	열람제한
	개인정보를 열람한 정보주체가 본인의 처리정보에 대해 정정 및 삭제를 청구한 경우 즉시 조치	정정및 삭제
분배/공유	다른 기관이 보유정보에 대해 이용·제공을 요청할 경우 문서를 통해 보유 목적 범위 등을 제출받아 적정 여부를 확인해야 함	파일 이용 및 제공 관리
	보유정보를 다른 기관에 제공하고자 할 때, 최소한의 범위로 제한하여 제공하고, 보유기관의 동의 없이 제 3자에게 이용·제공할 수 없도록 함	
	개인정보보호법 제 10조 제 3항에 해당하는 사항(정보주체의 동의가 있거나, 조약, 국제협정의 이행을 위해 외국정부 또는 국제기구에 제공하는 경우, 범죄수사에 필요한 경우 등)은 예외적으로 이용 제공할 수 있으며, 이를 '처리정보 이용제공대장'에 기록 하여 관리	

사용	개인정보파일을 생성하여 처리하고 있는 부서의 장은 개인정보 입출력 사항에 대해 '입출력자료관리대장'에 기록하여 관리	파일 입·출력관리
	다른 기관이 보유정보에 대해 이용·제공을 요청할 경우 문서를 통해 보유 목적 범위 등을 제출받아 적정 여부를 확인해야 함	파일 이용 및 제공 관리
	보유정보를 다른 기관에 제공하고자 할 때, 최소한의 범위로 제한하여 제공하고, 보유기관의 동의 없이 제 3자에게 이용·제공할 수 없도록 함	
폐기	개인정보 총괄부서는 보유·파기 현황을 주기적으로 조사하여 그 결과를 기관 홈페이지 개인정보보호방침에 포함하여 관리	파일현황 관리
	중앙행정기관, 광역자치단체, 시도교육청 등 최상위기관은 하위기관의 보유·파기현황을 주기적으로 조사 및 관리	
	행정안전부는 매년 전 공공기관의 개인정보파일 보유현황을 조사하여 관보에 공고하며, 최상위기관은 하위, 산하기관에 대한 보유 및 파기현황 제출에 협조해야 함	파일현황 제출
	개인정보를 열람한 정보주체가 본인의 처리정보에 대해 정정 및 삭제를 청구한 경우 즉시 조치	정정및 삭제
	개별 개인정보에 대한 변경 또는 수정, 보유기간 만료 등 보유 불필요, 삭제 청구가 발생되었을 때 이를 반영하여 관리	
	개별 개인정보를 삭제할 경우 재사용이 불가능하도록 영구 삭제	
	정보주체의 청구가 있어도 다른 법률에 따라 보유해야 할 경우해당 개인정보 항목에 대한 삭제를 거부할 수 있으며, 제한 사유가 발생한 경우 결정의 내용 및 사유와당해 결정에 대한 불복절차에 관한 사항을 기재한 '정정·삭제거부 등 결정통지서'를 청구인에게 송부	삭제제한
	개인정보파일의 보유목적 달성 등 해당 개인정보파일의 보유가 불필요하게 된 경우 해당 개인정보파일을 지체없이 파기 및 파기부서장은 파기사항에 대해 '입출력관리자료대장'에 기록	파일파기
	보존이 필요한 경우 파기하지 않을 수 있음	
	개인정보파일을 파기할 경우 복구할 수 없는 기술적 방법을 통해 원본 및 백업본을 파기해야 함	파기방법

4. 우리나라 정보자원관리 법규정 분석의 시사점

전자정부법의 제 11조에서는 행정정보공동이용의 원칙을 규정하고 있다. 또한 전자정부법 제 12조에서 개인정보보호의 원칙을 명시하고 있다. 그 구체적 내용은 다음과 같다. “행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다.” 이 원칙은 행정정보공동이용에도 불구하고 개인정보보호의 취지를 명시하고 있음을 보여준다.

그러나 제 21조 및 22조에서는 공동이용의 의무 및 행정정보공동이용에 관한 내용을 상세하게 설정하고 있으며(국가인권위원회, 2006), 전자정부법의 법규 조항의 행정정보공동이용에 관한 내용상 비중을 통해 판단해 보건데, 개인정보보호 보다는 행정정보 공동이용으로 인한 행정 및 전자문서 업무의 효율성에 보다 큰 비중을 둔 것으로 판단된다. 전자정부법에 따르면 정보공유를 통해 예산의 절감 및 행정의 효율성, 정보자원 이용에의 편리성 등을 통한 국민에 대한 정부의 신뢰성 제고에 목적을 둔 것으로 보인다.

그러나 정부효율성과 국민편리성 뿐 아니라 인권적 측면에서 개인정보 침해 및 개인의 사생활 보호도 그에 못지않게 중요한 요소이다. 그 동안 파편적으로 적용되어 왔던 공공기관의 개인정보보호가 공공과 민간에 통합 규율로서 법 적용 대상이 확대된 개인정보보호법은 그 동안 개별법 간의 상이한 처리기준에 대해 정보의 생애주기 각 단계별로 공통된 보호기준과 원칙을 적용한다. 또한 개인정보 열람·정정·삭제 및 처리정지권 보장, 개인정보 유출시 통지·신고제도, 집단분쟁조정제도, 권리침해 중지를 구하는 단체소송을 도입하여 국민 피해구제가 강화될 것이다.

그러나 법 적용의 실효성 확보를 위한 구체적인 세부 지침이 마련되어 있지 않다. 예컨대 제 21조 3항은 “개인정보처리자가 개인정보를 파기하지 아니하고 보존해야 하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장 및 관리해야 한다”고 규정되어 있으나 어떠

한 방식으로 분리 저장해야 하는 것인지 불분명하다.

전자정부법과 개인정보보호법은 상충하는 측면이 존재한다. 전자정부법의 행정정보 공동이용의 대상 및 범위가 확대는 결국 개인정보보호법의 적용이 배제되는 법률의 사각지대가 확대되는 결과가 될 수 있다.

개인정보보호지침은 기관 내부의 규율로서 보다 구체화된 내용을 명시하고 있다. 파일보유기간의 최소화, 파일 이용 및 제공에 관한 원칙적 금지(예외 경우 인정), 정보주체의 정정 및 삭제요구권 인정 등은 후술할 국제기구의 개인정보보호 가이드라인을 따르고 있는 것이라 볼 수 있다.

국제기구에서 다루고 있는 정보의 최신성 및 정확성에 관련해 정보의 변경으로 인한 수정 및 최신성·정확성 확보에 관한 규정은 보이지 않는다. 행정안전부 정보보호 지침은 정보관리에 있어 담당자들의 관리절차를 보다 상세하게 규율했다. 또 타 법률이 폐기에 관한 간단한 언급 수준에서 그친 것과는 달리 완전한 폐기에 관한 규정 및 폐기 정보관리에 관한 내용을 다루었다. 그러나 이러한 정보의 수집에서 저장, 사용 및 폐기에 관한 정보관리가 철저하게 이루어지고 있는지를 평가할 수 있는 관리지침은 보이지 않는다.

Ⅴ. 정보자원생애주기에 따른 국가별 법적 체계 비교 분석

정부가 수집 및 관리하는 국민의 개인정보량이 방대할수록 전제적 통치가능성이 높아질 것이라는 우려로 인해 정부의 정보관리를 규제하는 효과적 원칙을 도출하려는 노력이 진행되어 왔다. 여러 학술적 연구와 함께 OECD와 UN을 비롯한 국제기구들은 국제적인 개인정보보호 규범을 발표하였으며 개인정보보호를 위한 정부 차원의 법률이 여러 국가에서 마련되어지고 있다. 이러한 맥락에서 본 장에서는 국가별 정보자원관리 법을 규정할 때 기준이 되는 국제기구에서 추진한 개인정보보호 원칙에 대해서 먼저 검토하고, 미국과 독일에 대한 법규정을 파악한 후 우리나라와의 비교를 통하여 정보인권과 관련된 시사점을 도출해 보고자 한다.

1. 국제기구의 개인정보보호 원칙

먼저 개인정보 유출과 관련해서 1970년 이후부터 OECD 가입국가들을 중심으로 국내법 차원에서 규제하기 시작했고, 1990년 UN에서 '컴퓨터화된 개인정보 파일의 규율에 관한 가이드라인'을 발표하면서 개인정보의 중요성이 더욱 부각되고 있다. 현재 대부분 국가의 개인정보보호와 관련한 법제는 OECD가 제정한 8가지 원칙에 기초하고 있는데 전자상거래가 국제적인 관심사로 부각되면서 개인정보유출 우려가 전자상거래의 발전에 장애가 될 것을 우려한 OECD는 각 나라가 합의하는 통일된 개인정보보호지침을 채택하였는데 이것이 '프라이버시 보호와 개인데이터의 국제유통에 대한 가이드라인에 관한 이사회 권고안(1980)이다.

개인정보보호에 관한 기본원칙은 정보의 주체인 한 개인이 사생활의 비밀과 자유를 가지고, 자기정보에 관한 자기결정권[10]을 가진다는 것을 기본으로 한다. 개인정보자기결정권을 보장하기 위해서는 정보수집 및 활

10) 개인정보자기결정권은 자신에 관한 정보가 이용되는 것에 관해 그 정보주체가 스스로 결정할 수 있는 권리를 말한다.

용의 적합성, 정보의 정확성, 정보관리의 보안성 및 정보처리의 충설성(integrity)이 보장되어야 한다. 이러한 정보수집 및 활용의 적합성, 정보의 정확성, 정보처리의 충실성 및 정보관리의 보안성을 확보하기 위해 각국 정부와 국제기구는 다양한 개인정보보호원칙을 제정하여 시행하고 있다. 그 중 UN의 개인정보보호를 위한 가이드라인, OECD의 프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인, APEC의 개인정보보호원칙에 대해 살펴보기로 한다.

1) UN 개인정보보호원칙

UN은 1990년 총회의 결의로 전자화된 개인정보파일의 규율에 관한 원칙을 규정하였다. 동 가이드라인은 회원국에의 권고적 성격을 가지고 있으며, 그 주요내용은 다음과 같다. 첫째, 합법성과 공정성의 원칙은 개인정보는 합법적인 절차와 방법으로 수집되고 처리되어야 하며 UN헌장에 명시된 목적과 원칙에 위배 되서는 안 된다는 것을 말한다. 둘째, 정확성의 원칙은 정보의 수집과 저장에 관여하는 정보담당자는 개인정보를 정기적으로 검사하여 정보가 정확한 정보인지를 검토해야 함을 규정하고 있다.

셋째, 목적 구체성의 원칙은 개인정보를 수집하고 처리하는 목적이 구체적이고 정당해야 함을 말한다. 이러한 개인정보는 구체화된 목적과 관련된 것이어야 하고, 정보주체의 동의가 없는 한 다른 목적으로 사용 및 공개되어서는 안 되며, 수집된 개인정보는 구체화도니 목적 달성에 필요한 기간을 준수해야 한다는 것이다.

넷째, 개인에 의한 접근 원칙은 정보가 수집한 정보와 관련된 개인은 그 정보의 처리 및 사용에 대해 알 권리가 있으며, 잘못되거나 정확하지 않은 정보의 삭제를 요구할 수 있는 정보주체의 권리를 명시한 조항이다. 다섯째, 보안의 원칙은 자연재해, 컴퓨터 바이러스 또는 권한 없는 접근 등으로부터 개인정보파일을 보호하기 적절한 조치를 취해야 함을 명시하고 있다. 공정하고 합법적인 방법으로 정보를 수집, 정보의 최신성 및 정

확성 확보를 규정한 합법성과 공정성의 원칙 정보자원생애주기 중 정보의 수집 및 생성과 정보의 사용에 관한 원칙을 명시한 조항이라 볼 수 있다.

<표 5-1> UN 개인정보보호원칙의 정보자원생애주기에 따른 분류

정보자원 생애주기	UN 개인정보보호에 관한 원칙	
수집/생성	공정하고 합법적인 방법에 의한 개인정보 수집·처리	합법성과 공정성 원칙
	정확성과 관련성 확보를 위한 정기적 확인 절차	정확성원칙
	정보의 완전성과 최신성 확보를 위한 노력	
저장	사고로 인한 정보의 손실이나 파괴 또는 정보의 남용, 권한없는 접근, 컴퓨터 바이러스 오염 등으로부터 정보를 안전하게 보호하기 위한 적절한 조치 필요	안정성원칙
	정확성과 관련성 확보를 위한 정기적 확인 절차	정확성원칙
분배/공유	동의가 있는 경우를 제외한 목적외 이용 및 공개금지	목적구체화 원칙
	부정확한 정보에 대한 정정 또는 삭제 요구권	개인접근의 원칙
사용	UN헌장 목적과 원칙에 합치되는 개인정보처리	합법성과 공정성에 관한 원칙
	정보의 이용 또는 처리 방법에 대한 정보주체의 알권리	개인접근의 원칙
폐기	-	

또한 정확성의 원칙은 정보의 수집/생성과 저장에 해당한다. 정보의 손실이나 파괴 또는 정보의 남용이나 권한 없는 접근으로부터의 정보 보호를 규정한 안정성의 원칙은 정보보안과 관련해 정보 저장 과정에 관한 원칙을 나타낸 것으로 볼 수 있다. 목적 외 이용 및 공개를 명시한 목적구체화원칙은 정보의 분배/공유 과정에서의 개인정보보호를 명시하였다. 마지막으로 정보주체의 부정확한 정보에 대한 정정 및 삭제요구권, 정보주체의 알권리를 나타낸 개인접근원칙은 정보의 분배/공유와 사용에 있어 정보주체의 권리를 보장한 조항으로 볼 수 있다.

2) OECD 개인정보보호원칙

OECD의 개인정보보호원칙은 수집제한의 원칙, 목적구체성의 원칙, 이용제한의 원칙, 안전성확보의 원칙, 공개의 원칙, 책임의 원칙 등을 규정하고 있다. 그 내용에 대해 구체적으로 살펴보면 다음과 같다. 첫째, 수집제한의 원칙은 개인정보의 수집은 제한이 있어야 하며, 합법적이고 공정한 절차를 통해 데이터 주체에게 그 수집에 대한 동의가 있은 후 수집되어야 한다는 것이다.

둘째, 목적구체성의 원리는 개인정보의 수집목적이 명확해야 하며, 수집 후 개인정보의 이용은 수집목적의 실현할 수 있는 것으로 제한되어야 한다는 것이다. 셋째, 이용제한의 원칙은 개인정보는 명확한 목적이외의 목적을 위해서는 개시, 이용, 타 목적으로 사용되어서는 안 된다는 것이다. 그러나 정보주체의 동의가 있거나 법률의 규정에 의한 사용은 예외로 한다. 넷째, 안전성확보의 원칙은 개인정보의 분실, 불법적인 접근, 파괴 및 사용, 수정 등의 위험에 대해 합리적인 안전조치를 취하여 정보를 보호하여야 한다는 것을 내용으로 한다.

다섯째, 공개의 원칙은 개인정보와 관련한 정책에 대해 일반적인 공개정책을 취하는 것과 개인정보의 존재사실 및 그 정보담당자에 관한 정보에의 접근의 용이성을 말한다. 개인정보의 존재, 그 성질 및 이용 목적 및 정보관리자의 식별, 주소를 명확히 하여야 한다는 것이다. 여섯째, 책임의 원칙은 정보관리자는 전술한 제 원칙의 실현을 위해 정보관리의 책임이 있다는 것이다. 공정한 개인정보의 수집 및 민감한 정보의 수집을 제한을 명시한 수집제한의 원칙과 이용목적상 필요한 범위 내에서 개인정보의 정확성, 완전성 최신성 확보에 대한 내용은 정확성확보의 원칙, 수집이전 또는 당시의 개인정보수집의 구체화를 담은 목적명시의 원칙은 정보자원 생애주기의 수집/생성에 관한 내용을 담고 있다.

또한 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적·조직적·기술적 안전조치의 확보를 담고 있는 안정성확보의 원칙, 개인정보처

리 및 보호를 위한 정책공개, 정보관리자의 신원 및 개인정보의 존재 사실, 그 이용목적 등에 대한 접근의 용이성을 구술한 공개의 원칙과 개인정보관리자의 책임의 원칙은 정보자원생애주기 중 저장에 관한 내용을 명시한 것으로 판단된다. 정보의 분배와 공유에 있어 정보주체의 동의가 있거나 법규정이 있는 경우를 제외하고 목적 외 이용 및 공개를 금지한 이용제한의 원칙은 정보의 분배 및 공유의 개인정보보호를 규정한다. OECD 가이드라인의 정확성확보의 원칙, 목적명시의 원칙, 이용제한의 원칙은 정보의 수집/생성 뿐 아니라 그 사용에 관한 규정으로도 볼 수 있다. 그러나 동 가이드라인의 규정에서는 개인정보의 폐기에 관한 구체적인 원칙은 규정하지 않고 있다.

<표 5-2> OECD 개인정보보호 8원칙의 정보자원생애주기에 따른 분류

정보자원 생애주기	OECD 개인정보보호에 관한 원칙	
수집/생성	적법하고 공정한 방법을 통한 개인정보의 수집	수집제한의 원칙
	정보주체의 동의를 얻어 개인정보수집	
	민감한 개인정보의 수집 제한	
	이용 목적과의 관련성 요구	정확성확보의 원칙
	이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성 확보	
	수집이전 또는 당시의 개인정보 수집 목적 명시	목적명시의 원칙
저장	개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적, 조직적, 기술적 안전조치확보	안전성 확보의 원칙
	개인정보의 처리 및 보호를 위한 정책의 공개	공개의 원칙
	개인정보 관리자의 신원 및 연락처, 개인정보의 존재사실, 이용목적 등에 대한 접근용이성 확보	
	개인정보관리자에게 원칙 준수의무 및 책임 부과	책임의 원칙
분배/공유	정보주체의 동의가 있거나 법규정이 있는 경우를 제외하고는 목적외 이용 및 공개 금지	이용제한의 원칙
사용	이용 목적과의 관련성 요구	정확성확보의 원칙
	명시된 목적에 적합한 개인정보의 이용	목적명시의 원칙
	정보주체의 동의가 있거나 법규정이 있는 경우를 제외하고는 목적외 이용 및 공개 금지	이용제한의 원칙
폐기	-	

3) APEC 개인정보보호원칙

APEC(Asia-Pacific Economic Cooperation)은 개인정보보호에 관한 기본 원칙을 제정하여 회원국으로 하여금 회원국의 법령에 반영하도록 권고하고 있다. APEC의 개인정보보호 가이드라인의 주요 내용은 다음과 같다. 첫째, 침해방지의 원칙은 회원국에 개인정보가 오용된 경우 야기될 수 있는 피해를 인지하고 그 심각성을 감안하여 그 위험을 피할 수 있는 조치를 취해야 한다고 하고 있다. 둘째, 수집제한의 원칙은 개인정보의 수집은 합법적이고 공정한 수단으로 이루어져야 하고, 개인의 동의가 있어야 하며, 개인정보는 수집목적에 반하여 사용되어서는 안 된다는 내용을 규정하고 있다.

셋째, 고지의 원칙은 정보관리자가 개인정보의 수집 시, 정보의 수집사실, 수집목적, 정보관리자의 신원 주소, 연락처, 정보주체가 개인정보 유출 시 행사할 수 있는 권리, 정보열람권 및 정보정정권 등을 고지하여야 한다고 하고 있다. 이러한 정보는 개인정보가 수집되는 순간 혹은 그 이전에 제공되어야 한다. 넷째, 개인정보는 정확하고, 완전하며, 최신성을 유지해야 한다는 정확성의 원칙이 있다.

다섯째, 안정성의 원칙은 정보관리자는 보유 정보의 손실, 불법적 접근 및 파괴, 수정 등을 방지하기 위해 적절한 보안수단을 마련해야 함을 말한다. 이러한 보안 수단은 발생 가능한 위협의 정도와 비례하여 이루어져야 하며, 정기적 검토와 평가가 요구된다. 여섯째, 정보접근의 원칙은 정보제공자는 본인의 정보를 열람할 수 있고, 정보관리자는 부정확한 정보를 수정하거나 삭제해야 함을 명시하고 있다.

일곱째, 선택의 원칙은 정보의 수집, 이용, 공개와 관련하여 정보주체가 선택권을 행사할 수 있도록 하며, 정보주체의 선택권 행사를 위한 적절하고 명확한 접근방법이 정보주체에게 주어져야 함을 규정하고 있다. 마지막으로 책임의 원칙은 관리자는 전술한 제 원칙을 준수해야 하며, 개인정보가 제 3자에게 이전될 경우 정보의 수령자는 제 원칙에 따라 개인

정보를 보호하기 위해 필요한 조치 및 의무를 다해야 한다는 것을 내용으로 한다. 정보의 수집제한 및 선택의 원칙은 정보의 수집/생성에 관한 내용을 담고 있다. 선택의 원칙, 정확성의 원칙, 안정성의 원칙, 책임의 원칙은 저장에 있어서의 개인정보보호 원리를 규정하였다.

또한 개인정보가 오용될 경우 야기될 피해에 대한 조치 강구하고, 개인정보와 관련한 정책을 개인에게 고지하며, 정보주체의 선택권, 정보접근의 원칙과 책임의 원칙은 정보자원생애주기의 정보 공유/분배에 해당하는 내용을 담고 있다. 정보의 사용에 관해서는 침해방지의 원칙, 이용의 원칙, 고지의 원칙, 선택의 원칙, 정보접근의 원칙이 개인정보의 적절한 사용에 관해 명시하고 있다. 각 원칙이 정보자원생애주기의 개별적으로 한 단계에 해당하는 것이 아니라 선택의 원칙이 수집 단계와 저장, 분배/공유와 사용단계 전체에 해당하는 것과 같이 각 원칙이 여러 단계에 해당되는 내용을 담고 있기도 하다.

<표 5-3> APEC 개인정보보호원칙의 정보자원생애주기에 따른 분류

정보자원 생애주기	APEC 개인정보보호에 관한 원칙	
수집/생성	개인정보의 수집 제한 및 합법적이고 공정한 수단으로 수집된 정보라도 개인의 동의가 요구되며, 목적에 부합해야 함	수집제한의 원칙
	정보의 수집, 이용, 공개와 관련하여 정보주체가 선택권을 행사할 수 있도록 해야 함 정보주체가 선택권을 행사할 수 있도록 적절하고, 명확하며, 접근가능한 방법이 정보주체에게 주어져야 함	선택의 원칙
저장	정보의 수집, 이용, 공개와 관련하여 정보주체가 선택권을 행사할 수 있도록 해야 함 정보주체가 선택권을 행사할 수 있도록 적절하고, 명확하며, 접근가능한 방법이 정보주체에게 주어져야 함	선택의 원칙
	개인정보는 정확하고, 완전하고, 최신성을 유지	정확성의 원칙
	개인정보관리자는 보유하고 있는 개인정보의 손실, 허가받지 않은 접근, 파괴, 수정 혹은 오용을 방지하기 위해 적절한 보안수단을 제공해야함 보유하고 있는 내용은 정기적인 검토와 평가를 받아야 함.	안정성의 원칙
	정보관리자의 원칙적인 책임 준수 개인정보가 조직에 이전되었을 경우, 정보관리자는 정보보호 보장을 위한 조치 및 의무를 이행하여야 함	책임의 원칙
분배/공유	개인정보의 오용 될 경우, 야기될 피해인지 및 이를 막기 위한 조치 필요	침해방지의 원칙
	개인정보와 관련된 관행 및 정책을 해당 개인에게 명료하고 알기 쉽게 설명해야 함	고지의 원칙
	정보의 수집, 이용, 공개와 관련하여 정보주체가 선택권을 행사할 수 있도록 해야 함 정보주체가 선택권을 행사할 수 있도록 적절하고, 명확하며, 접근가능한 방법이 정보주체에게 주어져야 함	선택의 원칙
	정보주체는 적정한 방식 및 비용으로 본인의 정보 이용 여부 및 자신의 정보에 접근할 수 있음	정보접근의 원칙

	정보주체는 자신의 정보의 정확성에 의문을 제기할 수 있으며 잘못된 정보에 대하여 수정·삭제를 요청할 수 있음. 정보주체의 권리가 거부되었을 경우 정보주체에게 그 이유가 고지되어야 함	
	정보관리자의 원칙적인 책임 준수 개인정보가 조직에 이전되었을 경우, 정보관리자는 정보보호 보장을 위한 조치 및 의무를 이행하여야 함	책임의 원칙
사용	개인정보의 오용 될 경우, 야기될 피해인지 및 이를 막기 위한 조치 필요	침해방지의 원칙
	수집된 개인정보는 법률의 규정에 의한 경우를 제외하고는 목적에 반하여 사용되어져서는 안됨	이용의 원칙
	개인정보와 관련된 관행 및 정책을 해당 개인에게 명료하고 알기 쉽게 설명해야 함	고지의 원칙
	정보의 수집, 이용, 공개와 관련하여 정보주체가 선택권을 행사할 수 있도록 해야 함 정보주체가 선택권을 행사할 수 있도록 적절하고, 명확하며, 접근가능한 방법이 정보주체에게 주어져야 함	선택의 원칙
	정보주체는 적정한 방식 및 비용으로 본인의 정보 이용 여부 및 자신의 정보에 접근할 수 있음 정보주체는 자신의 정보의 정확성에 의문을 제기할 수 있으며 잘못된 정보에 대하여 수정·삭제를 요청할 수 있음 정보주체의 권리가 거부되었을 경우 정보주체에게 그 이유가 고지되어야 함	정보접근의 원칙
폐기	-	

2. 미국의 정보자원관리의 법규정 분석

1) 정보자원관리 법체계 개요

여기서는 정보자원관리(IRM) 개념을 최초로 도입하고 법률에 체계적으로 반영한 미국의 사례를 토대로 미국의 인권적 정보자원 관리 법·제도를 분석하고 소개하고자 한다. 미국 정보자원관리(IRM)에 대한 초기 문건은 A Report of the Committee on Federal Paperwork: Information Resources Management이다(행자부, 2004). 이후 문서감축법(Paperwork Reduction Act)에 반영되어 정보기술관리혁신법(ITMRA)과 OMB-Circular를 통해 그 절차와 업무가 정리되고 관리되고 있다(행자부, 2004).

미국의 인권적 정보관리 관련 법률과 이와 관련된 정부의 활동 및 행정명령 등을 정보자원관리의 인권적 관점에서 분석한다. 미국은 개인정보보호에 대한 통일적 일반적인 법체계를 가지지 않고 연방의회 및 주의회에서 특정분야에만 한정적으로 적용되는 개별입법을 제정하고 있다.

2) 프라이버시법(Privacy Act)

미국은 1974년 프라이버시법(Privacy Act)을 제정하여 연방차원에서개인정보보호를 위한 제도적 장치를 마련하였다. 이 법은 행정절차법(Administrative Procedure) 편에 속하는데, 행정기관의 개인정보이용에 대한 제한으로서 사적 정보의 공개요건 및 방법을 규정하고 있다.

또한 행정기관이 보유하는 정보에 대한 개인의 통제권을 인정할 뿐 아니라 정보가 다른 목적으로 이용되는 것을 방지하며, 자기정보에 대한 접근, 복사, 정정 및 수정을 보장하고, 식별 가능한 인적 정보의 수집 및 이용 등의 합법성, 개인정보의 현재성 및 정확성, 정보오용에 관한 예방책을 강구하여 권리침해에 대한 민사적 구제방법을 명기하고 있다.

또한 이 법은 연방 행정기관에 의한 개인정보의 취급에 있어 제 분야

를 망라한 최초의 종합입법으로 여겨지고 있다. 이 법의 적용대상은 행정기관, 연방정부의 규제를 받는 법인 및 행정기관의 수탁업자이며, 보호대상은 상기 기관에서 보유하고 있는 개인의 기록 및 기록시스템[11]이다. 이 법의 적용대상은 연방기관이 보유하고 있는 기록(record)이다.

여기서 기록이란 "개인의 교육, 재정, 병력, 전과나 이력 등을 포함하고, 정부 기관이 보유하는 이름, 개인 확인번호, 상징, 지문, 사진과 같이 개인을 구체적으로 확인할 수 있는 것을 포함한 개인에 관한 정보, 정보의 수집이나 분류"를 말한다. 개인에 관한 어떤 기록이 행정기관에 의해 수집, 보유, 이용, 배포되는 것은 개인의 서면청구나 서면동의를 받는 경우가 아니면 원칙적으로 금지되는데, 개인의 입장에 서는 정보통제권으로 해석될 수 있다. 다만 공무수행원의 직무수행을 위한 개시, 정보공개법의 규정에 의한 개시, 저장·검색 등 정규적 이용, 통계국의 통계조사, 역사적 가치가 있는 기록의 개시, 민사법 또는 형사법의 집행, 급박한 상황에서의 개시, 연방의회 활동을 위한 개시, 회계검사원(General Accounting Office, GAO)의 직무수행을 위한 개시, 법원의 명령 등에 의한 개시는 예외이다.

〈표 5-4〉 프라이시법의 정보자원생애주기에 따른 분류

정보자원 생애주기	**미국 개인정보보호법(Privacy Act, 1974)**
수집/생성	행정기관은 법률상의 활동목적을 달성하는데 필요하고 관련있는 개인정보만을 수집하여야 함
	개인정보가 연방프로그램 하에서 그 개인의 권리나 특권에 불이익한 결정을 낳을 수 있을 때에는 개인정보를 가능한 한 직접적 경로를 통하여 수집하여야 하며, 개인 각각에게 그 정보의 수집형태를 알려야 함
저장	본인은 자신의 기록을 검사하고, 정확하지 않는 부분에 대해 정정 요구할 수 있음
	기록시스템의 설치 및 변경 시 당해 시스템의 명칭 및 위치, 관리책임 공무원의 직위 및 주소 등을 연 1회 이상 연방관보에 게재

11) 기록시스템은 행정기관이 관리하는 기록의 집합으로 정보가 개인의 성명, 식별번호, 기호 그밖의 개인에게 배정된 신분의 식별을 위한 특기사항에 의해 검색되는 것이다.

	행정기관은 개인자료의 보안과 비밀을 유지하는데 적합한 관리, 기술·물리적 보안장치를 마련해야 함
분배/공유	개인의 서면청구 또는 사전서면동의의 경우를 제외하고는 타인 또는 다른 행정기관에 기록된 내용을 어떤 통신수단으로도 개시해서는 안됨.
	본인은 자신의 기록을 검사하고, 정확하지 않는 부분에 대해 정정 요구할 수 있음(개인기록접근권)
사용	개인의 서면청구 또는 사전서면동의의 경우를 제외하고는 타인 또는 다른 행정기관에 기록된 내용을 어떤 통신수단으로도 개시해서는 안됨
	본인은 자신의 기록을 검사하고, 정확하지 않는 부분에 대해 정정 요구할 수 있음(개인기록접근권)
	행정기관이 고의 또는 과실로 개인정보를 공개했을 경우, 손해배상책임 부담
폐기	-

3) 문서감축법과 Circular A-130

1977년 의회의 연방문서작업위원회 보고서의 권고에 따라 문서감축법이 1980년 법으로 통과되었다. 주 내용은 OMB를 정부 문서작업에 관한 주요정책 입안과 감독 부서로 지정하며, 특히 OMB내에 정보규제국(Office of Information and Regulatory Affairs, OIRA)을 신설하고 문서작업에 관련된 여러 기능을 수행하도록 하는 것이다.

정보수집과 관련한 주 기능은 행정기관의 정보수집요청서의 검토 및 승인, 정보수집과 관련된 절차상의 요구사항 충족여부의 확인, 두 기관 이상에서 필요한 정보일 경우 특정기관을 지명하여 대표로 수집하도록 지명, 정보 수집요청 축소의 목표를 설정, 의회 연방문서작업위원회 권고사항에 대한 조치의 감독, 연방정보검색시스템(Federal Information Locator System, FILS)의 개발 및 운영 등이다.

문서 감축법에 의해 OMB에 부과된 역할과 책임은 정보수집의 감독 및 조정을 넘어 연방 정보정책, 원칙, 표준, 지침 등의 개발 및 구현, 통계활동, 자료관리, 프라이버시, 기관 간의 정보공유, 자료처리의 자동화 도구나 기술의 획득 및 활용의 정보관리(Information Management) 전반으로 확대되었다.

미국 백악관의 관리예산국(OMB)은 기관의 보안프로그램을 감독하는데 필요한 정보를 얻고 연례보고서를 작성하기 위해 매년 각 기관에 보고 지침을 내린다. 또, 정보자원관리의 실제적 구현에 필요한 구체적 내용을 OMB Circular(회람) A-130으로 작성하여 이를 각 행정기관에 제시하고 있다.

본래 A-130은 1980년 최초로 입법화된 문서감축법의 구현을 위한 행정명령으로 1985년에 작성되었지만 이후 2000년까지 수차례에 걸친 개정을 통해 정보자원관리의 실질적 구현을 위한 정보자원관리정책을 규정하는 행정명령의 내용까지 다루었다. OMB Circular A-130은 정보관리, 정보시스템 및 정보기술로 구성되어 있고, 정보관리는 생명주기에 따라 정보관리 계획, 정보수집 가이드라인, 전자정보집 가이드라인, 기록관리 방안, 기관의 정보제공의무, 보안규칙수행 등을 명시하고 있다.

주 내용은 정보관리 정책과 정보기술의 관리정책을 포함한다. OMB Circular A-130은 정보보호와 관련하여 정부기관의 정보시스템의 보안을 보장하는 방법을 규정하고 있다. 정부기관은 반드시 정보와 시스템의 아키텍처에 사업 운영 전반을 지원할 수 있도록 보안대책을 수립하고, 예산계획 및 보안관리 생명주기와 정보시스템을 일치시켜야 한다. OMB A-130 부록3은 연방 정보보안제도에 포함된 보안대책을 설명하고, 정보보안과 관련된 개별 연방정부기관의 책임을 명시한다(김성근 외, 2010).

그 구체적인 내용을 살펴보면 다음과 같다. 첫째, 정보관리계획수행에 있어 정보자원생애주기 전반에 걸쳐 통합적 방법으로 계획을 세우며, 계획단계에서 국민, 주와 지방정부와의 협의를 고려할 것을 명시하고 있다. 각 단계별, 특히 정보배포에 관해 그 실행에의 영향을 고려하고 정보의 손실, 오·남용, 허가받지 않은 정보에의 접근과 정보의 수정으로 인한

정보의 위험으로부터 보호하는 계획을 세우고, 개인사생활에 대한 수행에의 결과를 생각하여 적절한 법·기술적 안전이 보장되도록 할 것을 명기하고 있다. 예산, 정보기술과 같은 정보자원 분배와 사용 계획을 위한 정보시스템 계획을 통합하도록 하고 있다. 또, 계획 수립 시, 개인의 사생활에 대한 권리에 영향을 고려하고, 적절한 법·기술적 안전장치를 수행하도록 하고 있다. 특징적인 점은 정보관리에 있어 OMB Circular(회람) A-130에서도 다른 법률과 같이 국민의 알권리를 강조하고 있다.

<표 5-5> OMB Circular(회람) A-130의 정보자원생애주기에 따른 분류

정보자원 생애주기	미국 OMB Circular(회람) A-130	
수집/생성	새로운 정보를 창출하거나 수집하기 전에 관계부처간 또는 범정부간 정보 공유를 통해 새로운 정보 니즈(needs)를 만족시킴	정보관리 계획
	기관의 적절한 기능 수행 및 실용적 활용에 필요한 정보만을 수집 및 생성	정보수집 가이드라인
	개인정보의 수집은 법률이 정하고, 목적에 부합하는 것으로만 수집 제한	정보보안
저장	허가받지 않은 정보에의 접근, 정보의 손실 및 오용으로 인한 위험에서 정부의 정보 보호	정보관리 계획
	모든 기관의 직원 및 도급업자에게 연방 기록물 관리 책임에 관한 훈련 및 가이드라인을 제공	기록관리
	다른 기관이나 하도급업체, 또는 그 기관을 대신한 다른 조직이 제공 또는 관리하는 것을 포함하여 기관의 운영과 자산을 지원하는 정보 및 정보 시스템에 대한 정보보안 제공	정보배포 관리시스템
	정보주체가 본인의 정보에 접근할 수 있도록 하며, 개인정보를 열람한 정보주체의 잘못 기재된 정보에 대해 정정을 허가	정보보안
분배/공유	새로운 정보를 창출하거나 수집하기 전에 관계부처 간 또는 범정부간 정보 공유를 통해 새로운 정보 니즈(needs)를 만족시킬 것	정보관리 계획
	기록에의 적절한 국민의 접근 규정	
	기관은 국민에게 정보제공 할 책임이 있으며, 법률에 요하는 바에 따라 기관 조직, 활동 프로그램, 미팅, 기록 시스템 및 기타 정보 보유와 국민이 어떻게 기관의 정보자원에 접근했는지 기록하고 정보를 제공	국민에 정보 제공
	기관은 정보배포물에의 접근권이 있음을 장애인에게 알릴 책임	정보배포 관리시스템
	중요 정보 배포물의 시작, 유지, 수정, 종결에 관해 공지	
	정보의 공유는 법률이 정하는 경우(지속적인 비밀 준수의 의무를 유지하는 조건)로 제한	정보보안

사용	정보생애주기 각 단계에서, 특히 정보 배포에 관해 계획수립 시 결정 및 조치의 효과를 고려하고, 국민, 주, 지방 정부와 협의	정보관리 계획
	허가 받지 않은 정보에의 접근, 정보의 손실 및 오용으로 인한 위험에서 정부의 정보 보호	
	기록에의 절적한 국민의 접근 규정	
	정보의 형태에 관계없이 기록에의 접근 보장	기록관리
	국민에게 정보의 제공 결정에 있어, 기관은 정보의 유용성을 극대화하고, 정부와 국민의 비용을 최소화 할 수 있는 균형을 이룰 수 있는 방법으로 정보를 배포	국민에 정보제공
	공정하고 시의적절한 조건으로 정보배포물을 제공	
	국민이 정부 정보의 저장 위치를 찾는 것을 도울 것	
	정부의 정보배포물의 가용성을 저해하는 다른 배포체계를 허가하지 않음	제한관행의 방지
	기관은 예산의 범위 내에서 국민에 정부의 정보가 국민에게 더 쉽게 접근가능하고 유용하도록 적절한 전자 포맷 사용	전자정보 배포
폐기	-	

4) 전자정부법(e-Government Act)

2002년에 제정된 전자정부법은 미 행정부의 국정수행목표인 인적 자원의 전략적 활용, 예산과 수행성과의 통합, 경쟁적 구매체 확보, 행정서비스에 인터넷의 활용 등을 보다 효과적으로 달성하기 위해 전자정부 서비스를 촉진하려는 의도와 국민이 인터넷을 통해 정부가 보유하는 정보에의 접근을 활성화하기 하기 위한 기반을 구축하기 위해 만들어졌다.

특히 범기관(Cross-agency)의 노력을 강조하고 있다. 법안에서는 Federal CIO의 역할을 다음과 같이 명기하였다. FCIO는 각 기관의 정보시스템을 연방차

원에서 통합하는 것에 대한 가능성 검토, 정부기금으로 연구·개발된 정보의 수집 및 배포의 기준을 정하는 부처 간 Task Force 운영, 정부기관의 웹사이트에서 프라이버시에 관한 통지의 가이드라인 설정, 정부기관 웹사이트에 관한 각종 기준 및 표준 제시 등을 담당한다.

이 법안의 범 기관적 차원의 예로 OMB 내에 신설된 Federal CIO 및 부처별 CIO로 구성된 CIO 위원회를 설치하는 것이 있다. 연방정보화책임관위원회는 정부 정보자원의 개발, 사용, 운영, 실행 등과 관련한 제반 업무를 개선하기 위한 역할을 담당한다는 내용을 담고 있다.

연방기관에 대해서는 기관의 전략적 목적에 부합하는 전자정부 및 정보기술의 이용을 위한 고객·생산성 관련 업무수행의 측정기법 개발, 관리예산처(OMB)가 발한 전자정부가이드의 준수, 직원대상 정보기술 교육훈련 프로그램(IT training programs)의 수립 및 운영, 새로운 정보기술 투자와 온라인 정보수집을 위한 프라이버시 영향평가(Privacy Impact Assessments)의 수행 등의 의무를 명기하였다. 이 법안은 2002년 3월 1일 미국 정무위원회를 통과하였으나, 이후 OMB와 의회는 법안에 대해 협상을 계속하였다.

이 과정에서 부시행정부의 반대에 따른 협상과정이 지속되었고, 결국 미국 상원은 2002년 7월 1일 FCIO의 직제 대신 전자정부국(Office of Electronic Government, OEG)을 신설하는 것을 골자로 하는 '전자정부법' 개정안(E-Government Act of 2002)을 통과시켰다. 2002년 11월 15일 의회에서 최종확정 되었고, 대통령의 서명으로 발효되었다. 이 법에서 새롭게 요구된 내용으로는 연방기금 R&D(Federally funded R&D)를 탐지하는 데이터베이스 및 웹사이트의 개발, 정부 정보 및 서비스에의 접근을 위한 온라인 지침서의 개발 등이 있다.

또한 인터넷 정보를 포함하여 정부정보를 분류, 보존, 일반인의 접근성을 향상시키기 위한 목적으로 관리예산처장이 기관간정부정보위원회(the Inter-agency Committee on Government Information)을 설치하도록 한다. 이 위원회를 통해 일반국민과 협의하고, 정부정보의 효과적인 접근, 배포, 보존사례를 공유하며, 정부정보체계의 정의 및 그 체계화에 관한 표준의

채택에 대한 권고안을 OMB의 장에게 제시한다. 이 법안의 내용 중 주목할 만한 것은 프라이버시영향평가(Privacy Impact Assessments)이다.

이 법은 국민 중심의 전자정부를 구현함에 있어 개인정보가 충분히 보호되도록 하기 위해 전자정부의 세부사업이 프라이버시에 미치는 영향을 사전에 조사하도록 하는 것이다. 프라이버시 영향평가는 수집대상정보, 수집이유, 정보의 용도, 정보공유기관, 정보공유에 관한 개인의 동의, 정보보안방안, 기록체계의 합법성 등을 다루게 된다. 연방기관은 프라이버시 영향평가의 결과를 웹사이트나 연방관보 그 밖의 수단으로 공개하여야 한다(Section 208).

미국 전자정부법[12]의 주요내용은 다음과 같다. 첫째, 전자정부국(OEG)

---

12) 전자정부법의 세부 내용을 조문으로 살펴보면 다음과 같다.

Section 2. Findings and purposes
정보기술이 사회를 급격히 변모시켰으나 정부에의 적용은 불충분하다. 정보기술이 정부에 성공적으로 도입되기 위해서는 새로운 리더십, 보다 나은 조직, 향상된 부처간의 협조 등이 요구된다. 이에 따라 이 법은 관리예산처(OMB) 내에 전자정부국(OEG)를 두어 전자정부 구현에 있어 연방정부의 보다 효과적인 리더십을 지원하고자 한다.

Secion 202. Federal agency responsibilities
성공적인 전자정부 구현을 위해 기관들이 관리예산처와 협조하여 단순히 업무 자동화가 아닌 전략적 관점에서 기관의 목표와 합치시켜야 함을 강조하고 있다.

Section 204. Federal Internet portal
인터넷에 기반한 통합된 정부포털사이트의 발전을 명문화하였다. 특히 총무청에 의해 관리되고 있는 First Gov.gov와 관련해, 향후 전자정부국의 국장이 총무처의 작업을 감독할 수 있는 권한을 부여하였다. 구체적으로 2003년의 회계연도에 정부포털사이트의 유지 및 보수에 $1.5 million를 사용할 수 있도록 승인하였으며, 매 회계연도마다 필요한 만큼의 액수를 지출할 권한이 있음을 명기하였다.

Section 206. Regulatory agencies
여러 규제기관들도 정보기술을 활용하여 국민들로부터 의견을 수렴하고 규제분야에서 책임성과 투명성을 확보하는 방안을 제시하고 있다.

Section 207. Accssibility, usability and preservation of government information
정부가 생성, 보유, 전파하는 정보의 관리, 접근, 활용 및 보존 등에 대한 내용을 담고 있다. 국립기록물보관청(National Archives and Records Administration)과 부처 CIO로 구성된 정부의 정보에 대한 범부처위원회를 설립하였고 관리예산처장이 위원장을 맡았다. 이 위원회는 정보의 분류, 전자적 정보의 확산 등에 대해 국민의 자문을 거친 이후 정책방안을 마련하는 임무를 지닌다.

의 설치를 규정하여 각 기관간의 정보의 중복제공을 피하고, 일반인의 정보이용을 용이하게 하며, 웹사이트 간 표준화작업을 통해 개인정보보호를 위한 각 인프라 간의 유기적 연계를 도모하도록 하였다.

둘째, 정보보안 및 개인정보보호와 관련한 사항의 총괄하기 위해 전자정부국은 정부기관과 법원 등 미 정부 내 웹사이트를 효율적으로 관리·운용함으로써 국민이 정부가 구축한 사이트에 쉽게 접속할 수 있도록 할 뿐 아니라 미 정부의 IT 투자를 감시하고 정부 내 웹사이트 관련 플랫폼을 동질화하도록 한다.

셋째, 전자정부국은 정부문서업무제거법과 정보기술관리혁신법(Clinger-cohen Act 또는 ITMRA)의 E절, 정부정보보안개혁법 그리고 프라이버시법(Privacy)법 등 미국 내 전자정부와 관련한 법을 총괄하도록 한다(전자정부국의 역할).

넷째, 전자정부국장은 ① 정보기술에 대한 자본계획 및 투자통제, ②엔터프라이즈 아키텍처(enterprise architectures)의 개발,③ 정보보안, ④ 프라이버시, ⑤ 정부정보에의 접근, 배포와 보존, ⑥ 장애인을 위한 정보기술의 이용가능성 등에 관해 정보규제사무국장 및 관리 예산처의 다른 부서와 협력하여야 함을 규정한다.

Section 208. Privacy provisions

프라이버시와 보안은 전자정부 서비스에서 신뢰성을 제공하는데 가장 중요하다. 따라서 전자정부서비스에서 각 기관들은 개인적인 프라이버시가 보호되었는지 확인하여야 한다. 이 조문에서는 두 가지 측면에서 프라이버시 보호를 기술하고 있다. 첫째, 만일 정부가 시스템 디자인의 초기 단계에서부터 프라이버시에 대한 관심을 가진다면, 개인에 대해 정부서비스가 맞춤화된다고 해서 개인의 프라이버시를 침해하는 것은 아니다. 둘째, 프라이버시 보호의 통지는 분명하고, 간결하고 정확해야 한다. 이 조문은 각 연방기관이 프라이버시 영향 선언문(Privacy Impact Statement: PIAs)을 제정하도록 하고 있다.

Section 301. Information Security

본래 한시적 효력을 지닌 정부정보보안개혁법[1](Government Information Security Reform Act, GISRA)를 영구존속하는 것으로 개정하였다.

〈표 5-6〉 미국 전자정부법의 정보자원생애주기에 따른 분류

정보자원 생애주기	**전자정부법(E-Government Act, 2002)**
수집/생성	연방기관은 신원확인이 가능한 형태로 정보를 수집, 관리, 배포하는 정보기술의 개발 및 조달
	통합연구보고 및 시범사업에 관한 규정을 통해 연방정보시스템상의 상호운용성을 제고하고, 정보의 중복수집을 감소
	비통계적 목적으로 수집되는 정보의 경우에는 비통계적 이용가능성을 정보수집이전에 국민에게 알려야 함(section 512)
저장	사이버 보안에 대한 기준 마련 및 확산
	통계자료에 있어 프라이버시 보호를 위한 기준 마련
	연방기관은 신원확인이 가능한 형태로 정보를 수집, 관리, 배포하는 정보기술의 개발이나 조달(section 212)
	연방정보보안관리법(Information Seurity Management Act)을 통해 정보의 보안을 위한 범정부적 관리·감독을 실시하고, 연방정보시스템의 보호에 필요한 통제수단(정보보안프로그램)을 개발·유지
분배/공유	국민이 인터넷을 통해 정부가 보유하는 정보에의 접근을 활성화
	국민이 연방정보 및 서비스를 보다 편리하게 이용할 수 있도록 전자정부기금 설치의 규정
	전자정부기금의 지급대상사업 선정 시, 적절한 보안의 보장 및 프라이버시 보호방안 등의 기준 고려
	행정규칙 제정에 있어 일반국민이 제출한 내용을 수령하고(국민참여 보장), 행정규칙제정에 관한 자료 및 처리경과 등을 전자 일지 형식으로 웹사이트에 공개
	정부정보의 효과적인 접근, 배포, 보존사례를 공유
	연방기관은 신원확인이 가능한 형태로 정보를 수집, 관리, 배포하는 정보기술의 개발이나 조달
	통합연구보고 및 시범사업에 관한 규정을 통해 누구든지 프라이버시를 침해받지 않고 1인 이상의 기관이 보유한 유사한 정보를 통합하여 수집할 수 있게 함
	인터넷 이용격차에 관한 연구[13]를 통해 인터넷 이용격차를 해소하고자 함(section 215)

사용	국민이 인터넷을 통해 정부가 보유하는 정보에의 접근을 활성화
	인터넷을 통한 정부정보 및 서비스의 제공과 관련해 컴퓨터 비보유자나 인터넷을 사용할 수 없는 개인에 대해서도 이용에 불편이 없도록 조치하고, 장애인의 이용권 보장
	연방법원의 정보는 봉인문서 등의 특정 예외를 제외하고 전자적으로 보존된 문서는 일반인에게 모두 공개됨이 원칙
	대법원은 전자처리 된 문서에 대한 이용가능성과 관련해 프라이버시보호 및 보안을 위한 규칙을 제정해야 함(section 205)
	연방기관은 신원확인이 가능한 형태로 정보를 수집, 관리, 배포하는 정보기술의 개발이나 조달
	비밀유지서약에 따라 기관이 획득한 자료 또는 정보는 통계적 목적으로만 당해 기정보는 응답자의 사전동의 없이 통계적 목적 이외의 어떤 이용을 위해서도 신원확인이 가능한 형태로 공개되어서는 안 됨(section 503)관의 담당자에 의해 이용되어야 함.
폐기	-

13) 이 연구는 인터넷 이용격차의 속성, 인터넷 서비스의 금전적 부담, 집단간 인터넷 이용격차의 정도, 인터넷 접속 성격의 변화 등을 포함하여 온라인 정부와 인터넷 이용격차 사이의 상호영향관계를 그 내용으로 한다.

3. 독일의 정보자원관리의 법규정 분석

1) 개인정보보호에 관한 1995년 제46호 EU지침(Directive 95/46/EC)

EU지침(directive)은 유럽연합 가맹국을 법적으로 구속하는 법규범으로서 가맹국인 독일은 '개인정보보호에 관한 1995년 제46호 지침(95/46/EC)'[14]에서 요구하고 있는 내용을 반영하여 연방정보보호법(Bundesdatenschutzgesetz)을 개정하였다. 이 지침은 입법목적을 '사적 영역의 보호'로 설정하고 있다. 그 근거는 유럽인권협약(European Convention on Human Rights) 제8조로 이 조항은 개인생활과 가족생활 및 주거와 통신에서 비밀(privacy)의 존중을 요구하고 있다. 또한 1995년 제46호 EU지침은 이미 1980년에 OECD가 권고한 '개인정보보호에 관한 지침(Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)'이 포함하고 있는 중요한 원칙을 그대로 담고 있다.

이 지침에는 개인정보보호와 관련하여 ① 고지(notice)의 원칙(개인정보를 수집당하는 본인에게 수집 사실을 고지해야 하는 원칙), ② 목적(purpose) 외 사용금지의 원칙(수집되는 개인정보는 제시된 목적을 위해서만 사용되어야 하고, 그 외의 목적을 위해서는 사용될 수 없다는 원칙: 제9조 및 제10조), ③ 동의(consent)의 원칙(수집된 개인정보는 본인의 동의가 없으면 제3자에게 공개되거나 제공될 수 없다는 원칙), ④ 보안(security)의 원칙(수집된 개인정보는 안전하게 보호되어야 하고, 손상이나 파괴, 공개되지 않도록 보안조치가 취해져야 하는 원칙: 제11조), ⑤ 수집주체 공개(disclosure)의 원칙(개인정보를 수집당하는 본인은 수집하는 주체가 누구인지에 관하여 알아야 하는 원칙), ⑥ 접근(access)의 원칙(개인정보를 수집당하는 본인은 자신의 개인정보에 접근하여 부정확한 정보를 수정할 수 있어야 하는 원칙), ⑦ 책임(accountability)의 원칙(개인정보를

14) 개인정보보호에 관한 유럽연합의 지침에 대해서는 임규철, 각 국의 개인정보보호법제 비교연구 - 미국과 유럽연합의 개인정보보호법제를 주심으로, <공법연구>(한국공법학회), 제31집 제5호(2003), 82면 참조하도록 한다.

수집당하는 본인은 수집하는 주체에게 개인정보보호에 관한 원칙의 준수에 대하여 책임을 물을 수 있는 원칙: 제14조)이 포함되어 있다.

이 지침에서 개인정보는 특정한 또는 특정될 수 있는 자연인에 관한 정보로 정의되고, 특정될 수 있다는 것은 신체적, 정신적, 심리적, 경제적, 문화적, 사회적 신원(identity)을 표현하는 숫자나 하나 또는 다수의 특별한 요소를 부여함으로써 직접 또는 간접적으로 개인의 신원이 확인될 수 있는 경우로 정의된다(EU지침 제2조 a항).

그리고 EU지침은 가맹국에 대해서 개인정보보호를 감시하는 업무를 수행하는 감독기관의 설치와 개인정보보호 관련 법령의 제정 및 해당 법령 위반 시의 구제나 제재 절차의 보장을 권고하고 있다. 또한 EU지침은 개인정보를 수집하는 모든 기관에 대하여 개인정보처리절차를 시행하기 전에 행정관청에 그에 관한 내용(해당 수집기관의 명칭과 주소, 개인정보처리절차의 목적, 정보수집주체의 범주와 수집되는 정보의 범주, 수집된 정보가 공개되는 수령자, 개인정보의 외국이전 계획, 개인정보와 그 처리절차에 대한 보안조치에 관한 개괄적 설명)을 상세하게 보고해야 하는 의무를 요구하고 있다.

2) 연방정보보호법(Bundesdatenschutzgesetz: BDSG)

연방정보보호법의 헌법적 근거는 정보에 관한 자기결정권(Das Recht auf informationelle Selbstbestimmung)에 있다. 독일 연방헌법재판소(Bundesverfassungsgericht)는 1983년 12월 15일에 선고된 인구조사결정(Volkszählungsurteil)에서 자신과 관련된 개인정보의 수집과 이용에 관하여 스스로 결정할 수 있는 "정보에 관한 자기결정권(das Rechts auf informationelle Selbstbestimmung)"을 헌법상 보장된 기본권으로 인정하였다.[15] 연방헌법재판소는 이 기본권의 헌법적 근거를 독일 헌법(기본법, Grundgesetz: GG) 제1조 제1항의 인간존엄[16]과 제2조 제1항의 인격의 자

15) BVerfGE(연방헌법재판소결정집) 제65권, 1면 이하를 참조하도록 한다.

유로운 발현권[17]에서 찾았다. 그리고 이 기본권의 보장내용을 "자신의 개인정보의 제공과 이용에 관하여 원칙적으로 스스로 결정할 수 있는 권리(Befugnis)"로 규정한다. 연방정보보호법에서 정의하는 개인정보(personenbezogenen Daten)는 특정한 자연인 또는 특정할 수 있는 자연인의 인격적 또는 사항적 상태에 관한 개별적 정보를 의미한다(BDSG 제3조 제1항).

연방헌법재판소의 결정을 존중하여 의회는 개인정보에 대한 접근을 통해 인격권이 침해되는 것을 예방하기 위한 입법목적에서 연방정보보호법(Bundesdatenschuzgesetz: 이하 'BDSG'로 약칭)을 제정하여 1990년 12월 29일 공포하였다.[18] 이 법률은 2001년 5월 18일과 2003년 1월 14일에 개정되었고, 최근에는 2009년 8월 14일에 다시 개정되었다.

연방정보보호법은 원칙적으로 공공기관과 민간기관에 모두 적용된다. 동 법이 적용되는 공공기관은 연방의 행정관청, 사법기관, 공법상의 연방시설 및 단체 및 주의 행정관청, 사법기관, 지방자치단체, 주의 감독을 받는 공법상의 법인 등을 포함한다. 또, 공행정의 과제를 수행하는 연방 또는 주의 공공기관에 속한 사법상의 단체로 2개 이상의 주 영역에서 활동하거나 과반수 구성원, 과반수의 표결권이 연방에 속하는 단체도 이에 해당한다.

연방정보보호법은 다음과 같은 개인정보처리의 기본원칙을 규정하고

---

16) GG 제1조 제1항: 인간존엄은 불가침이다. 국가권력은 이를 존중하고 보호할 의무가 있다(Die Würde des Menschen ist unantastbar. Sie zu achten und zu schüzen ist die Verpflichtung aller staatlichen Gewalt).

17) GG 제2조 제1항: 모든 인간은 타인의 권리를 침해하지 않고, 헌법질서 또는 도덕률에 위반되지 않는 한에서 자신의 인격을 자유롭게 발현할 수 있는 권리를 가진다(Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt).

18) 연방헌법재판소의 인구조사결정과 연방정보호호법의 관계에 대해서는 임규철, 정보화사회에서의 개인정보자기결정권에 대한 연구 - 독일에서의 논의를 중심으로, <헌법학연구> (한국헌법학회), 제8권 제3호(2002), 245면 이하 참조. 독일의 연방정보보호법에 대한 개략적인 설명으로 김상겸/김성준, 정보국가에 있어서 개인정보보호에 관한 연구 - 공공부문을 중심으로 독일의 법제와 비교하여, <세계헌법연구> (국제헌법학회 한국학회), 제14권 제3호(2008), 107면 이하 참조하도록 한다.

있다. ① 최소화원칙(Datenvermeidung und Datensparsamkeit)으로, 개인정보의 수집, 처리, 이용 및 정보처리시스템의 선택과 구성에서 가능하면 목적달성에 필요한 최소한의 개인정보만 요구하도록 요청하는 원칙(제3a조) 이다. ② 익명화원칙(Anoymisierung und Pseudonymisierung)으로, 행정목적에 비추어 가능하고, 달성하려는 목적과의 관계에서 과도한 부담이 되지 않는다면 개인정보는 익명화 또는 가명화하도록 요청하는 원칙(제3a조) 이다.

③ 본인동의원칙으로, 개인정보의 수집은 연방정보보호법이나 다른 법규에서 허용하거나 강제하는 경우 또는 본인의 동의가 있는 경우에만 허용된다는 원칙을 말한다(제4조 제1항). 이때 동의는 본인의 자유로운 의사결정에 따라 이루어져야 하고, 원칙적으로 문서(Schriftform)로 행해져야 한다(제4a조 제1항). ④ 본인수집원칙으로, 개인정보는 원칙적으로 본인으로부터만 수집될 수 있고, 법규에서 규정하고 있거나 논리필연적으로 전제하고 있는 경우 또는 실현하려는 행정과제의 유형이나 목적에 비추어 타인이나 기관으로부터 수집될 필요가 있거나 본인으로부터 수집하는 것이 과도한 부담이 되면서 본인의 중대한 이익을 침해한다는 근거가 없는 경우에는 본인의 참여 없이도 개인정보가 수집될 수 있다는 원칙(제4조 제2항)을 말한다. ⑤ 고지원칙은 본인으로부터 개인정보를 수집하는 경우에 정보수집기관의 신원, 정보수집의 목적 등에 관하여 고지받을 권리가 있다는 원칙(제4조 제3항)이다.

연방정보보호법에 따르면 공공기관이든 민간기관이든 반드시 '정보보호담당관(Beauftragter für Datenschutz 또는 Datenschutzbeauftragter: BfD 또는 DSB로 약칭)' 을 임명해야 한다(BDSG 제4f조 제1항). 이로써 공공기관이나 민간기관의 조직상의 자유가 제한되기는 하지만 헌법상 보장된 '정보에 관한 자기결정권' 을 보호(특히 권리침해에 대한 예방)하기 위한 입법자의 정당한 입법적 조치(강제)로 이해된다. 한편 정보보호담당관 제도는 개인정보보호에 관한 기관내부의 "자기통제(Selbstkontrolle"를 본질로 하기 때문에 국가의 경우에는 통제기관을 따로 만드는 비용을 절

감할 수 있고, 기업의 경우에는 국가적 간섭으로부터 자유롭게 되는 효과가 있다.[19] EU지침은 정보보호담당관제도를 필수적으로 요구하고 있지는 않지만 정보보호담당관과 같은 통제기관에 대해서 '완벽한 독립성'의 보장을 요구하고 있다(EU지침 제18조 제2항). 이러한 독립성은 원칙적으로 신분(임기)의 보장을 통해서 가능하기 때문에 고용기간 내의 해고는 원칙적으로 금지된다(제4f조 제3항 제4문). 또한 해고 이외의 불이익한 처우도 금지되는 것으로 해석된다.[20] 해당 기관은 정보보호담당관의 업무수행을 지원해야 할 의무가 있고, 특히 업무수행에 필수적인 경우에는 보조인력, 공간, 시설, 설비 등을 제공해야만 한다(제4f조 제5항).

정보보호담당관의 주된 업무는 연방정보보호법과 정보보호에 관한 다른 법령이 준수되도록 하는 것이고, 정보보호에 관한 통제과정에서 의문이 있는 경우에는 '관할 행정기관'에 문의해야 한다(제4g조 제1항). 특히 개인정보를 처리하는 프로그램이 법령을 준수하여 운영될 수 있는지 감독하고, 이를 위하여 적절한 시기에 보고를 받을 수 있어야 한다. 또한 개인정보처리를 담당하는 인력들이 연방정보보호법과 정보보호에 관한 다른 법령 및 정보보호의 필요성에 대하여 숙지할 수 있도록 적절한 조치를 취해야만 한다.

자동화처리절차는 운영 전에 민간기관의 경우에는 감독관청에 연방기관 및 우편 · 통신기업은 연방정보보호 · 정보자유담당관에게 보고해야 하는 의무가 부여된다(제4d조 제1항). 이러한 보고의무는 정보보호담당관이 수행한다. 자동화처리절차가 당사자의 자유와 권리에 대한 특별한 위험이 되는 경우에는 처리절차가 시작되기 전에 사전심사(Vorabkontrolle)를 받아야 한다(제4d조 제5항). 사전심사의 권한은 정보보호담당관이 갖는다.

정보보호담당관은 직무상 알게 된 개인의 신원에 관하여 비밀엄수의 의무(Verschwiegenheitpflicht)를 진다(제4f조 제4항). 이러한 의무는 정보보호담당관이 독립적으로 업무를 수행하기 위하여 필수적이기 때문에 권리

19) Golla/Schomerus, BDSG Kommentar §4f Rn(단락번호). 1.

20) Golla/Schomerus, BDSG Kommentar §4f Rn(단락번호). 53.

로 이해될 수도 있다.[21] 같은 맥락에서 정보보호담당관은 직무상 알게 된 정보에 관하여 증언을 거부할 수 있는 권리(Zeugnisverweigerungsrecht)를 보장받는다(동조 제4a항).

연방정보보호법에 따라 정보보호담당관은 자동화처리절차를 운영하기 전에 감독관청(민간기관의 경우)이나 연방정보보호·정보자유담당관(공공기관의 경우)에게 보고해야 하는 의무(Meldepflicht)가 있다(제4e조). 보고해야 할 내용은 해당기관의 명칭, 법률상 정보처리 책임자, 정보수집, 처리, 이용의 목적, 정보폐기 기한, 제3국가에 대한 정보제공 계획, 정보처리의 보안이 적절한지 여부를 판단할 수 있는 개괄적인 설명 등이 있다. 또한 독일의 연방정보보호법은 감리제도에 대해 규정한다. 개인정보를 처리하는 기관은 인가받은 독립적인 평가기관에 의해 감리(audit)를 받아야 하는데(BDSG 제9a조), 감리제도에 대해서는 정보보호담당관제도를 통해 실현되고 있는 '자기통제의 원칙'과 모순되고, 정보보호담당관제도를 통한 내부적 통제와 관할 행정관청의 감독권에 의한 외부적 통제 이외에 새로운 형태의 외부적 통제는 불필요한 비용을 추가로 지불해야 하는 관료기관의 도입이라는 비판이 제기되기도 한다.[22]

연방정보보호법은 개인정보를 수집당하는 당사자에게 설명, 수정, 삭제, 차단을 요구할 수 있는 권리를 보장하고 있다(제6조). 당사자 권리로는 먼저, 설명요구권(Auskunfrecht)과 설명의무(Benachrichtingspflicht)가 있다. 설명요구권은 "누가, 무엇을, 언제, 그리고 어떤 여건에서 자신에 대해서 알게 되었는지"[23]에 관하여 알 권리를 말한다(제19조 및 제33조). 이에 상응하여 해당 기관은 설명의무를 부담한다(제19a조 및 제34조).

다음으로, 수정요구권은 당사자에게 보장되는 이의제기권(Widerspruchsrecht) 가운데 하나로 본인에 관한 개인정보 가운데 부정확하거나 불완전한 내용을 수정해주도록 요구하는 권리를 말한다(제20조 제1항 및 제35조 제1항).

---

21) Golla/Schomerus, BDSG Kommentar §4f Rn(단락번호). 51.

22) Golla/Schomerus, BDSG Kommentar §9a Rn(단락번호). 5.

23) BVerfGE 65권, 1(43)면.

수정요구권은 법률행위를 통해서 배제되거나 제한될 수 없다(제6조 제1항).

마찬가지로 이의제기권 가운데 하나인 삭제요구권은 본이과 관련된 개인정보를 더 이상 사용할 수 없게 데이터베이스에서 제거하도록 요구하는 권리를 말한다(제20조 제2항 및 제35조 제2항). 삭제요구권도 법률행위를 통해서 배제되거나 제한될 수 없다(제6조 제1항).

차단요구권도 이의제기권 가운데 하나로 본인과 관련된 개인정보가 적절한 조치를 통해 배포되거나 사용되지 못하게 차단해주도록 요구하는 권리를 말한다(제20조 제3항 및 제35조 제3항). 차단요구권도 법률행위를 통해서 배제되거나 제한될 수 없다(제6조 제1항).

행정관청이 수정, 삭제, 차단을 거부하면 연방정보보호·정보자유담당관(BfDI)에게 신고하거나 관할법원(행정법원 또는 사회법원)에 소송(의무이행소송 또는 부작위위법확인소송)을 제기할 수 있다.

연방정보보호법은 개인정보침해에 대한 손해배상제도를 규정하고 있다. 이에 따라 개인정보를 수집하는 기관이 연방정보보호법이나 정보보호에 관한 다른 법규에서 허용하지 않거나 부당한 방식으로 개인정보를 수집·처리·이용하여 손해를 입힌 경우에는 기관 또는 그 직원은 당사자에게 손해배상을 해야 할 의무가 있다(제7조). 개인정보를 수집하는 기관이 연방정보보호법이나 정보보호에 관한 다른 법규에서 허용하지 않거나 부당한 방식으로 자동화된 개인정보수집·처리·이용을 하여 손해를 입힌 경우에는 기관의 책임과 독립적으로 해당 기관의 직원은 당사자에게 손해배상을 해야 할 의무가 있다. 개인정보를 수집·처리·이용하는 기관은 과도한 부담이 되지 않는 한도 내에서 연방정보보호법을 집행하는 데 필요한 조치를 기술적, 조직적 조치를 취해야 할 의무가 있다(제9조).

연방정보보호법은 연방정보보호·정보자유담당관(Bundesbeauftragter für Datenschutz und Informationsfreiheit: 이하 'BfDI'로 약칭)제도를 규정한다. 이에 따라 연방의회는 연방정부의 추천으로 연방정보보호·정보자유담당관을 재적과반수의 의결로 선출하고, 연방대통령이 임명한다

(BDSG 제22조 제1항). 연방정보보호 · 정보자유담당관의 임기는 5년이고, 1차에 한하여 중임할 수 있다(동조 제3항). 연방정보보호 · 정보자유담당관은 조직상 연방내무부장관에 소속되지만 직무수행에서 독립적이고 오직 법률에만 구속되며 연방정부의 법적 감독을 받는다(동조 제4항).

연방정보보호 · 정보자유담당관은 연방공공기관이 연방정보보호법 및 정보보호에 관한 법률을 준수하는지 여부를 감독하는 권한을 가진다(BDSG 제24조 제1항). 연방정보보호 · 정보자유담당관은 연방정보보호법이나 정보보호 관련법률에 대한 위반이나 개인정보의 처리나 이용에서 결함을 확인한 경우에는 해당 기관에 이의제기(Beanstandung)를 할 수 있는 권한을 가진다(BDSG 제25조 제1항). 연방정보보호 · 정보자유담당관은 2년마다 연방의회에 활동보고서를 제출해야 한다(BDSG 제26조 제1항).

민간기관과 공기업이 개인정보를 수집, 이용하는 경우에는 감독관청(Aufsichtsbehörde)이 감독할 수 있는 권한을 가진다. 감독관청은 연방정보보호법과 정보보호 관련법률의 준수 여부를 통제한다(BDSG 제38조 제1항). 또한 정보보호담당관의 해당 기관에게 자문을 제공하고 지원한다. 감독관청은 감독의 목적을 위해서만 저장된 정보를 처리, 이용할 수 있고, 특히 다른 감독관청에 정보를 전달하는 것은 감독의 목적을 위해서만 허용된다.

감독관청은 해당 기관이 보고한 정보를 기록하는 장부(Register)를 비치하여 누구나 열람할 수 있도록 조치해야 한다(BDSG 제38조 제2항). 연방정보보호법과 정보보호 관련법률의 보장을 위하여 감독관청은 개인정보의 수집, 처리, 이용에서 법률위반이나 기술적 조치나 조직상의 조치의 결함을 확인했을 때 이에 대한 시정을 명령할 수 있다(BDSG 제38조 제5항). 특히 개인의 인격권에 대한 특별한 위험을 초래하는 법률위반이나 결함이 있는 경우에는 시정명령에 불구하고, 그리고 이행강제금의 부과에도 불구하고 적절한 시간 안에 시정되지 않으면 개인정보의 수집, 처리, 이용 및 이에 관한 절차의 허용을 취소할 수 있다.

〈표 5-7〉 독일 연방정보보호법(BDSG)의 정보자원생애주기에 따른 분류

정보자원 생애주기	**독일 연방정보보호법(BDSG)**	
수집/생성	개인정보의 수집과 이용에 관하여 스스로 결정할 수 있음.	정보에 관한 자기결정권
	개인정보의 수집, 처리, 이용 및 정보처리시스템의 선택과 구성에서 그 목적을 지향해야 하고, 가능하면 목적달성에 필요한 최소한의 개인정보만 요구하도록 요청	최소화원칙
	행정목적에 비추어 가능하고, 과도한 부담이 되지 않는다면 개인정보는 익명화 또는 가명화하도록 요청하는 원칙	익명화원칙
	개인정보의 수집은 연방정보보호법이나 다른 법규에서 허용하거나 강제하는 경우 또는 본인의 동의가 있는 경우에만 허용	본인동의원칙
	개인정보는 원칙적으로 본인으로부터만 수집할 수 있음 예외적으로 본인의 참여 없이도 개인정보가 수집될 수 있는 경우(법규에서 규정하고 있거나 논리필연적으로 전제하고 있는 경우 또는 실현하려는 행정과제의 유형이나 목적에 비추어 타인이나 기관으로부터 수집될 필요가 있거나 본인으로부터 수집하는 것이 과도한 부담이 되면서 본인의 중대한 이익을 침해한다는 근거가 없는 경우)	본인수집원칙
	개인정보를 수집하는 경우에 정보수집기관의 신원, 정보수집의 목적, 정보수령자의 범위 및 정보제공 여부 결정권과 정보제공을 거부했을 경우의 효과에 관하여 본인은 고지받을 권리가 있음	고지원칙
	'특수한(민감한) 개인정보'(BDSG 제3조 제9항)를 공공기관이 수집하는 행위는 법규에서 규정하거나 중대한 공익상의 이유 등, 대단히 중대한 이유가 존재하는 경우에만 허용	특수한 개인정보에 대한 특별한 보호의 원칙
	개인정보를 수집당하는 당사자에게 자신의 개인정보에 관한 정보제공, 수정, 삭제, 차단을 요구할 수 있는 권리를 보장	이의제기권
저장	개인정보의 수집, 처리, 이용 및 정보처리시스템의 선택과 구성에서 그 목적을 지향해야 하고, 가능하면 목적달성에 필요한 최소한의 개인정보만 요구하도록 요청	최소화원칙
	행정목적에 비추어 가능하고, 달성하려는 목적과의 관계에서 과도한 부담이 되지 않는다면 개인정보는 익명화 또는 가명화하도록 요청하는 원칙	익명화원칙
	개인정보를 처리하는 프로그램이 법규를 준수하여 운영될 수 있는지 여부를 감독하고, 이를 위하여 적절한 시기에 보고를 받을 수 있어야 함	정보보호 책임자의 권한 및 의무

	이의제기권 중 수정요구권은 본인에 관한 개인정보 가운데 부정확하거나 불완전한 내용을 수정(Berichtigung)해주도록 요구하는 권리	이의제기권
분배/공유	개인정보의 수집과 이용에 관하여 스스로 결정할 수 있음	정보에 관한 자기결정권
	개인정보의 수집, 처리, 이용 및 정보처리시스템의 선택과 구성에서 그 목적을 지향해야 하고, 가능하면 목적달성에 필요한 최소한의 개인정보만 요구하도록 요청	최소화원칙
	행정목적에 비추어 가능하고, 달성하려는 목적과의 관계에서 과도한 부담이 되지 않는다면 개인정보는 익명화 또는 가명화하도록 요청하는 원칙	익명화원칙
	이의제기권 중 차단요구권은 본인과 관련된 개인정보가 적절한 조치를 통해 배포되거나 사용되지 못하게 차단(Sperrung)해주도록 요구하는 권리 예외인정(학문적 목적, 증거부족의 해결 또는 해당 기관이나 제3자의 이익이 우월하다는 근거가 있는 경우 등)	이의제기권
사용	개인정보의 수집, 처리, 이용 및 정보처리시스템의 선택과 구성에서 그 목적을 지향해야 하고, 가능하면 목적달성에 필요한 최소한의 개인정보만 요구하도록 요청	최소화원칙
	행정목적에 비추어 가능하고, 달성하려는 목적과의 관계에서 과도한 부담이 되지 않는다면 개인정보는 익명화 또는 가명화하도록 요청하는 원칙	익명화원칙
	이의제기권 중 차단요구권은 본인과 관련된 개인정보가 적절한 조치를 통해 배포되거나 사용되지 못하게 차단(Sperrung)해주도록 요구하는 권리 예외인정(학문적 목적, 증거부족의 해결 또는 해당 기관이나 제3자의 이익이 우월하다는 근거가 있는 경우 등)	이의제기권
폐기	민간기관이 수집한 특수한 개인정보는 원칙적으로 폐기(삭제)되어야 함	특수한 개인정보에 대한 특별한 보호의 원칙
	정보폐기의 기한 존재	보고의무제도
	이의제기권 중 삭제요구권은 저장이 허용되지 않거나 권한에 속한 직무의 수행에 더 이상 불필요한 경우(공공기관) 및 저장이 허용되지 않는 경우, 그 정확성이 수집기관에 의해 증명되지 않은 경우(민간기관) 등 본인과 관련된 개인정보를 더 이상 사용할 수 없게 데이터베이스에서 삭제(Löschung)해주도록 요구하는 권리	이의제기권

3) 통신법(Telekommunkationsgesetz: TKG)과 전자매체법(Telemediengesetz: TMG)

2004년 6월 22일 공포된 통신법은 2010년 2월 17일에 개정되었고, 최근에는 2011년 3월 24일에 개정되었다. 통신법에서 규율하는 통신(Telekommunikation)은 "통신설비를 이용하여 신호를 송출, 전달, 수신하는 기술적 과정"으로 정의된다(TKG 제3조 제22호).

여기서 통신설비(Telekommunikationsanlage)는 "뉴스로 볼 수 있는 전자신호 또는 영상신호를 송출, 전달, 매개, 수신, 조종, 통제할 수 있는 기술적 시설이나 시스템"을 의미한다(동조 제23호). 통신과 관련된 정보보호는 통신법 제7장 제2절에서 규정하고 있다. TKG 제 88조는 통신비밀을 보장하고 있고, 감청금지의 원칙(TKG 제89조)을 통해 모든 사람 또는 불특정 다수에게 제공되는 정보 외에는 감청이 금지된다. 또한 통신서비스 제공자는 통신서비스이용자에게 계약체결 시에 개인정보의 수집과 이용의 유형, 범위, 장소, 목적에 대해 설명할 의무가 있고(TKG 제 93조), 이와 관련된 연방정보보호법(BDSG)상의 설명요구권이 그대로 적용된다.

통신서비스제공자는 이용자의 개설정보(Bestanddaten) 및 접속정보(Verkersdaten)를 수집, 이용할 수 있다. 개설정보의 경우 계약관계가 종료되면 종료일이 속한 연도의 다음 연도가 지나면 폐기해야 한다(TKG 제95조 제3항). 위치정보는 통신망에서 수집, 이용된 정보 및 통신서비스의 최종이용자가 사용한 기기의 위치를 공중에게 제시하는 정보를 말하고(TKG 제3조 제19호), 익명화되거나 이용자의 동의가 있는 경우에만 처리될 수 있다(TKG 제98조).

전자매체법은 2007년 2월 26일 제정되어 최근에 2010년 5월 31일에 개정되었다. 이 법률은 정보기업의 서비스, 특히 전자상거래에 관한 법적 측면을 규율하는 2000년 제31호 EU지침(Directive 2000/31/EC)을 반영하고 있다. 이 법률은 통신법(TKG)에 따라 규율되는 통신서비스, 즉 순전히 통신망을 통한 신호의 전달만을 본질로 하는 서비스를 제외한 전자정보 · 통신서비스 영역, 다시 말해 통신에 기반한 서비스 및 방송에 적용된다

(TMG 제1조 제1항). 동법에서는 전자매체법이나 전자매체와 직접 관련이 있는 법률에서 허용하거나 당사자의 동의가 있는 경우에만 서비스제공자는 전자매체의 개설을 위하여 개인정보를 수집, 이용할 수 있음을(TMG 제12조 제1항) 규정한다.

동법에서 서비스 제공자는 설명의무(Unterrichtungspflicht)와 설명요구권(Auskunftrecht), 서비스이용자가 언제나 서비스를 종료할 수 있고, 접속이나 그밖의 이용에 관한 개인정보를 종료 후에 즉각적으로 폐기하거나 저장할 수 있으며 제3자의 인식으로부터 보호되고, 동일한 이용자가 이용한 상이한 전자매체의 이용에 관한 개인정보가 분리되어 사용되는 등 서비스 제공자는 기술적, 조직상의 예방조치를 취해야 할 의무가 있다(TMG 제13조 제4항). 동법에서는 서비스제공자가 수집, 이용할 수 있는 개인정보로 개설정보(Bestanddaten)[24]와 사용정보(Nutzungsdaten)[25]를 명기하고 있다.

〈표 5-8〉 독일 통신법(TKG) 및 전자매체법(TMG)의 정보자원생애주기에 따른 분류

정보자원 생애주기	독일 전자매체법(TMG)	
수집/생성	전자매체법이나 전자매체와 직접 관련이 있는 법률에서 허용하거나 당사자의 동의가 있는 경우에만 서비스제공자는 전자매체의 개설을 위하여 개인정보를 수집, 이용할 수 있음	정보보호원칙 제12조 1항
	개인정보의 수집과 이용의 유형, 범위, 목적에 대해서 설명해야 할 의무	TMG 제13조 제1항
	연방정보보호법(BDDG)상의 설명요구권(제34조)에 따라 당사자가 요구하면 개인정보에 대하여 설명	TMG 제13조 제7항
	통신서비스제공자는 통신서비스이용자에게 계약체결 시에 개인정보의 수집과 이용의 유형, 범위, 장소, 목적에 대해서 설명해야 할 의무	TKG 제93조

24) 원격매체의 사용에 관한 서비스제공자와 사용자 간의 계약관계의 창설, 내용적 구체화, 변경에 필요한 경우에만 개인정보의 수집과 이용이 허용된다(TMG 제14조).

25) 원격매체의 청구를 가능하게 하거나 중단하는 데 필요한 경우에만 개인정보의 수집과 이용이 허용된다. 사용정보에는 사용자의 신원확인을 위한 표식, 개별적인 사용의 시작, 종료, 범위에 관한 정보, 사용자가 청구한 원격매체에 관한 정보(TMG 제15조).

저장	서비스제공자는 기술적, 조직상의 예방조치를 취해야 할 의무	TMG 제13조 제4항
분배/공유	법률에서 허용하거나 당사자의 동의가 있는 경우에만 서비스제공자는 전자매체의 개설을 위하여 수집한 개인정보를 다른 목적에 이용할 수 있음.	정보보호 원칙 제12조 2항
사용	법률에서 허용하거나 당사자의 동의가 있는 경우에만 서비스제공자는 전자매체의 개설을 위하여 수집한 개인정보를 다른 목적에 이용할 수 있음.	정보보호 원칙 제12조 2항
	통신망의 위치정보는 익명화되거나 이용자의 동의가 있는 경우에만 처리될 수 있음.	TKG 제98조
폐기	-	

4. 종합분석: 한국과 미국, 독일의 정보자원관리 법규정 비교

세계 여러 나라 가운데 단일한 전자정부법의 제정은 2001년 우리나라가 최초이며, 뒤이어 미국이 2002년 11월에 제정하였다(정충식, 2006) 우선 미국의 정보관리에 관한 법률은 우리나라의 법과 비교해 볼 때, 비교적 포괄적인 내용을 담고 있다. 우리나라의 전자정부법이 전자적인 문서처리를 기본관점으로 하여 기존의 사무관리 규정 조항들을 법령으로 승격시킨 것에 비해, 미국의 법은 전자정부 구현 및 개인정보보호에 있어, 관리예산처(OMB)의 역할을 규정하고, 연방정부의 조정력 강화에 초점을 맞추고 있다.

그러나 2011년 9월 시행되는 한국의 개인정보보호법 및 행정안전부의 공공기관 개인정보보호 지침에서 볼 수 있듯이 한국의 경우도 미국의 관리예산처(OMB)와 같이 행정안전부를 주축으로 각 부처에서 개별적으로 관리되고 있는 정보자원을 통합적으로 조정하고 통제하려는 노력을 보여주고 있다. 독일의 경우, 연방정보보호법은 독일 헌법의 “정보에 관한 자기 결정권”을 근거로 1990년 12월에 공포하여, 두 차례의 개정을 거쳐 현재에 이르고 있다. 이 법은 공공기관과 민간기관 모두에 적용되는 특징이 있다. 한국과 미국, 독일의 법률은 정보자원의 관리에 있어 정보의 수집, 생성, 이용, 파기에 이르는 정보자원생애주기의 각 단계별 처리기준을 구체적으로 제시하고 있다.

1) 수집/생성

정보의 수집/생성에 있어서 한국과 미국, 독일 모두 중앙관리기구가 존재한다. 미국은 1980년에 제정된 정부문서업무제거법에 따라 관리예산처(OMB)를 중심으로 각 기관의 문서감축에 대한 중앙집권적 리더십의 발휘와 범정부적인 정보자원관리의 효율성을 도모하고 있다. 이후 여러 차례 개정된 정부문서업무제거법을 통해 종합적인 정보관리정책을 개발하고 유

지하며, 각 기관에 대해 정보자원관리에의 책임을 지도록 하는 등 OMB는 연방정부의 정보자원관리를 총괄하며, 관리예산처장이 연방정보자원관리를 위한 정책과 지침을 개발하고 조정하는 중앙관리기구로서의 자리를 확고히 하였다. 한국의 경우 2011년 9월 30일 시행되는 개인정보보호법을 통해 행정안전부는 정부의 정보관리에 있어 중앙 관리기구로서의 일부 역할을 맡고 있으며, 행정기관에서 이용되는 대부분의 정보는 각 기관 소관으로 되어 있다.

행정안전부의 정보관리에 있어 역할은 개인정보를 새롭게 수집하거나 보유하고 있는 정보에 관한 변경 시 행정안전부와 협의, 각 기관의 정부수집에서 파기에 이르는 각 단계별 정보관리사항에 대한 보고조치를 할 경우, 이에 대해 종합 및 관보 게재의 역할을 담당하고 있다. 한편 독일은 공공 및 민간기관의 정보보호에 관해 '정보보호책임자'에게 감독의 책임을 부여하고 있다. 전술한 바와 같이 개인정보보호에 관해 기관내부의 자기통제를 기본으로 하여, '정보보호책임자'에게 관리감독을 맡기는 대신 통제기관을 따로 만드는 비용을 절감하며, 민간에 대한 감독에 있어 국가의 지나친 간섭을 방지하고자 하였다. 민간 및 공공기관의 중앙감독기관이 분리되어 존재하며, 개인정보처리에 관한 구체적인 법적기준을 별도의 장에서 달리 규정하고 있다.

공공기관의 경우, 정보화책임자는 연방정보보호자유담당관(BDI)에게 보고해야 하며, 민간은 감독관청에 보고의 의무가 있다. 미국의 관리예산처(OMB)는 개인정보보호와 관련한 예산을 통해 기관을 통제하는 역할을 하며, 행정기관의 정보수집을 검토(review)하고, 승인(approval)하는 역할을 한다. 한국의 경우 그 권한은 행정안전부와 각 기관 간 사전 협의 및 개선, 또는 권고의 수준에 그치고 있다. 한국은 개인정보 목록, 주민등록등본, 출입국사실증명 등 총 92종의 행정정보 메타 DB가 존재하지만 통합데이터베이스라기보다는 부처별로 개별 관리 및 보유하고 있는 상황이다. 미국의 경우도 포괄적 행정정보 이용체계라기 보다는 사안별, 영역별 필요에 따라 행정정보 공동이용을 추진하고 있다.

그 범위는 복지영역, 범죄수사관련 법집행 영역에서 공공안전 및 재난관리, 테러, 국토방위 영역으로 확장되고 있다. 개인정보의 수집 동의에 관해서는 개인의 자기정보결정권을 존중하고 있으나 미국과 한국 모두 예외사항을 인정하고 있다. 독일은 정보자원생애자원 주기 중 수집/생성에 관한 조항이 다른 과정에 비해 두드러진다. '익명화의 원칙' 및 '특수한 개인정보에 대한 특별한 보호의 원칙'이 특징적이다. 독일은 정보의 수집/생성에 있어 개인정보보호에 대해 기관내부통제에 중점을 두고 있으며, 사후적 감독조치를 취하고 있다.

<표 5-9> 정보자원 수집/생성 단계에서의 법제 비교

비교 내용(index)		한국	미국	독일
중앙 관리 기구	담당 기구	- 행정안전부, 개인정보보호위원회	- OMB(관리예산국,공공)	- 공공기관: 연방정보보호정보자유담당관(BDIB) - 민간기관: 감독관청
	담당 범위	- 컴퓨터로 처리되는 문서 및 수기 문서포함 - 개인정보를 새로 수집하거나 보유한 개인정보파일에 관한 사항을 변경할 시 행정안전부와 협의 - 부처별 관리 개인정보 목록 실태 점검	- 연방의 정보정책, 원칙, 표준, 지침 등의 개발 및 구현 - 통계 활동, 자료관리, 프라이버시, 기간 간 정보공유 - 자료처리 자동화 도구나 기술의 획득 및 활용	- 연방정보보호법(BDSG) 준수 여부에 대한 감독
	권한 정도	- 사전 협의, 개선 권고	- OMB는 프라이버시보호와 관련하여 예산관리차원에서만 제한적인 기능 담당 - OMB는 행정기관의 정부수집을 검토(review) 및 승인(approval)	- 사후적 감독권한
메타 DB	존재 여부	- 행정정보공동이용 DB 존재 - 통합 DB가 아니라 각 부처별 개별 관할 - 부처별 보유하고 있는 개인정보 목록	-포괄적 행정정보 이용체계가 아니라 사안별, 영역별 필요에 따라 행정정보 공동이용 추진	
	관리 주체	- 각 부처 담당자, 행정안전부	- OMB 및 해당 기관	- 개인정보보호책임자(DSB)
	포함 범위	- 개인정보 목록 - 공동이용(조회, 유통) 정보목록	- 복지영역, 범죄수사관련 법집행에서 공공안전, 재난관리, 테러, 국토방위 영역으로 확장	

	공개 정도	- 주민등록등본, 출입국 사실증명, 병적증명서 등 총 92종		
단위별 관리지침	**책임자 권한**	- 부처별 정보화담당자 존재		- 개인정보보호책임자(DSB)의 감독권
	강제성 정도	- 낮음		
	공개 정도	- (행정안전부 제공) 공공기관 개인정보보호기본지침 공개	- 행정기관의 사인(私人)에 대한 정보공개를 제한[26]	
외적 통제 체계	**존재 여부**	- 개인정보침해신고센터 및 개인정보분쟁조정위원회	- 주정부 CIO협의회(NASCIO)는 정보공동활용을 위한 국회의 입법 활동 촉구	- 공공기관: 연방정보보호정보자유담당관(BDIB)
	수집동의과정	- 동의를 받을 때에는 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적 등의 사항을 정보주체에게 알려야 함(개인정보보호법 제 9조 정보제공) - 전기통신망법 제22조 제1항	- 개인기록접근권 (Pravacy Act) - 원칙적으로 수집은 본인으로부터 직접 수집 (Privacy Act) - 각 행정기관의 장은 정보수집에 관리번호 등을 매겨 관리하고 유효기간을 명시하며, 정보수집 대상자에게 정보수집의 필요성, 활용방법, 부담을 지우는 범위 등의 사항 고지(문서감축법)	- 저장된 개인정보에 대한 정보제공요구권 (BDSG 제19조, 제33조)과 정보제공의무(제19a조, 제34조) - 개인정보는 본인으로부터 수집되어야 한다는 원칙(BDSG 제4조 제2항) - 정보주체가 정보수집 관련 내용을 고지 받을 권리의 보장(BDSG 제4조 제3항) - 정보수집기관의 고지의무

2) 저장

한국은 전자정부법의 행정정보공동이용에 관한 법에서 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부 구현에 필요한 정보통신망과 행정정보 등의 안정성 및 신뢰성 확보를 위한 보안대책을 마련

26) 정보공개법(Freedom of Imformation Act, 1966)이 행정기관이 보유한 정보에 대한 국민의 (적극적) Access권을 보장하기 위한 것이라면, 프라이버시법(Privacy Act, 1974)은 (소극적) Access권을 보장하기 위해 제정되었다. 우리 법제상으로는 '공공기관의정보공개에관한법률'에서 정보의 공개를 원칙적으로 규정(5조)하고 사생활의 비밀을 또는 자유를 침해할 우려가 있는 정보 등에 대해서 공개를 제한(9조)하고 있다. 이 경우 정보공개에 따른 공익과 그로 인해 침해되는 사익 간의 비례성원칙의 적용이 요구된다. 프라이버시법(Privacy Act)에서도 개인에 관한 정보수집에 있어 필요최소한의 정보를 보유할 것을 명시하고 있다. 1988년 Computer Matching and Privacy Protection Act가 제정됨에 따라 컴퓨터를 이용한 개인정보의 제공을 제한함으로써 보호법익의 외연을 확대하였다.

하고 시행하도록 규정하고 있다.

관리예산처(OMB)가 구체적 지침을 제공하여 정보화예산을 요청할 때 영향평가서를 제출하도록 하고, 그 보고서를 토대로 예산편성을 하는 실질적인 요소로 적용하고 있다. 특히, 전자정부법은 프라이버시 영향평가의 대상, 평가주체, 평가시기 등을 명시하고, 이를 수행한 결과를 심사 및 공개하도록 하였다. 미국의 경우 연방정보보안관리법 및 연방정보보안관리법 및 연장정보보안지침의 “프라이버시 보호가이드라인”을 통해 보안관리 지침을 제시하고 있다.

가이드라인은 개인식별정보 보호를 기관의 기본의무로 규정하고, 수기문서, 전자문서형태로 기록된 개인정보보호를 위한 관리적·기술적·물리적 안전조치 통제사항을 규정하고 있다. 동 가이드라인은 개인정보의 수집 시 고지 및 동의 획득에서, 이용·제공의 제한, 무결성, 사고대응, 리스크 관리, 감사, 교육 등에 대한 개인정보처리자가 준수해야 할 23개 통제사항을 제시하고 있다. 특히 정보의 저장과 관련하여 개인정보의 유지보수에 관계된 모든 프로그램, 정보시스템 목록을 작성하여 운영하고 이를 정기적으로 갱신하도로고 하고 있다.

그리고 그 목록을 CIO 또는 보안관리자에게 제공하여 적절한 보안요구사항을 수립하도록 한다. 또 프라이버시 침해사고 대응 계획을 수립 및 이행하고, 이 계획에 따라 비인가 된 개인정보의 노출에 대응하도록 한다. 이 가이드라인에서는 개인식별정보 관련 책임을 가진자에게 포괄적인 교육가 훈련을 실시하도록 한다. 시스템 상의 기록 관리와 관련 해 한국의 경우, 행정안전부에서 매년 전 공공기관의 개인정보파일 보유현황을 조사하여, 관보에 공고하도록 하고 있으며, 미국의 경우도 개인식별정보의 수집, 이용, 유지보수, 공유에 관계된 모든 기록을 작성하여 정기적으로 갱신하고 이를 연방관보에 공고하도록 하고 있다. 또 정기적으로 실시하는 정보보안 평가결과 및 정보보안 감사결과를 관리예산처장에게 보고하여 관리예산처장은 그 결과를 의회에 제출하고 있다.

저장된 정보와 관련하여 외부적 통제체계로서 한국에서는 행정안전부

와 감사원, 개인정보보호위원회가 기능한다. 독일의 경우, 정보의 저장단계에 있어 개인정보 관련자의 권리가 강조된다. 미국과 한국의 경우, 저장에 대한 정보보안에의 기술적 관리지침이 구체적으로 제시되어 있는 것에 반해 법규정의 내용상 독일은 정보관리자의 책임이나 의무보다는 정보주체의 권리에 보다 중점을 둔 것으로 보여진다. 저장되어 있는 정보에 관한 설명과 동의요구를 통해 자신에 관한 정보를 교정하거나 통제할 기회가 관련자에게 보장된다(김일환, 2010). 저장단계에서도 감독기구는 민간기관과 공공기관이 분리되어, 공공기관은 정보자유책임관(BDI)이, 민간부문은 감독관청이 유출피해 감시와 저장관리 관행 감시를 담당한다.

<표 5-10> 정보자원 저장 단계에서의 법제 비교

비교 내용(index)		한국	미국	독일
보안관리	보안관리 지침 존재	- 전자정부법의 행정정보공동이용에 관한 법(국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책 마련하고 시행할 것을 명기)	- 연방정보보안관리법[27], -연방정보보안지침 "프라이버시 보호가이드라인(안)" 제시 SP 800-53(2011년 12월 공포 예정)	- 주 및 지방 데이터보호 담당관(Datensenschutzbeauf-tragte)은 연방의 행정청이 데이터보호를 잘 수행하고 있는지 통제
	보안관리 정도	- "개인정보보호 수준 측정을 위한 진단프로그램"의 적용 및 보급하고 진단결과를 개인정보보호지수(EPI)	- 개인정보수집 시 고지 및 동의 획득, 이용·제공의 제한, 무결성, 사고대응, 리스크관리, 감사, 교육 등에 대해 개인정보처리자가 준수해야 할 23가지 통제사항 명기	- 공공기관: 직무수행과 목적 범위내로 한정(BDSG 제14조 제1항)
	시스템상 기록관리	- 행정안전부에서 매년 전 공공기관의 개인 정보파일 보유현황을 조사, 관보에 공고하고, 최상위기관은 하위, 산하기관에 대한 보유 및 파기현황 확인	- 개인식별정보 수집, 이용, 유지보수, 공유에 관계된 모든 프로그램, 정보시스템 목록을 작성·운영 및 정기적 갱신	

외부적 통제 체계	**통제 기관**	- 행정안전부 및 감사원, 개인정보위원회(민간인위원장)	- 정보보안 평가결과 및 정보보안 감사결과를 OMB 장에게 보고 - OMB 장은 그 결과를 의회에 제출	- 공공기관: 연방개인정보・정보자유책임관(BDI) - 민간기관: 감독관청
	유출 피해 감시	- 행안부 총괄실태조사 및 감사원·정부합동 기획점검		- 공공기관: 개인정보보호책임자(DSB) → 연방정보보호・정보자유책임관(BDI) - 민간기관: 개인정보보호책임자(DSB) → 감독관청

3) 분배/공유

정보의 공유/분배를 위해 한국에서는 행정안전부 장관 소속 행정정보 공동이용센터를 이용하고 있다. 2000년 대 초 전자정부의 본격적인 추진과 함께 행정정보DB 구축 및 공동이용을 확대하게 되었다. 정보통신망 구축을 통해 중앙부처 및 지자체, 행정기관과 연계된 공공기관이 통합・연계되어 운영된다. 그 범위는 일부 비연계 DB가 존재하지만 제 2금융권을 포함한 금융권 및 교육기관을 포함한다. 미국의 경우 영역별, 사안별로 시스템의 연계가 이루어지고 있다.

예를 들어, 법무부에서는 범죄예방 및 수사 등을 위한 정책과 집행, 서버와 기술표준을 정비하기 위해 법집행 정보공동활용 프로그램(Law Enforcement Information Sharing Program: LEISP)를 추진하였다. 이를 통해 기존에 연방정부와 주정부, 지방정부 각각으로 분리되어 있던 수사 관련 정부를 전국적으로 통합하게 되었다. 현재 전국적 차원에서 범죄수사에 필요한 사건기록, 체포기록, 범죄이력 등을 검색하고 연결할 수 있는 강력한 도구로서 기능하고 있다. 또한 정부보조금지급 프로그램에서 실수

27) OMB의 장은 범정부차원의 보안정책을 수립하여야 한다. 연방정보시스템의 비용효과적인 보안, Clinger-Cohen법에 제시된 정보기술아키텍쳐, 정보시스템 위험의 확인 및 평가를 통한 위험관리 사이클 구축, 위험의 적절한 통제, 정보보안 위험에 대한 인식제고 및 정보보안 절차의 효과성 감시 평가 등을 포함하는 정책을 수립한다.

나 남용을 발견하기 위해 연방정부는 컴퓨터 연결프로그램[28]을 사용하였다. 개인정보 특히 SSN(Social Security Number:사회보장번호)는 보험, 금융, 부동산 등 민간영역에서도 사용되고 있으나 이의 제공은 정보주체의 선택사항으로 하고 있다. 정보의 분배/공유와 관련한 표준관리지침은 한국의 경우 공공기관 개인정보보호 지침이 있으며, 기관 별 실무지침이 이를 대신하고 있다. 미국의 경우도 OMB Circular(회람) A-130과 연방정보보안개혁법에서 일부 규정하고 있으나 포괄적 표준관리지침은 연방정보보안관리법(FISMA) 시행을 위한 보안지침인 SP 800-53의 부속문서인 Appendix J에 포함되며, 의견수렴 결과를 반영하여 2011년 12월에 공표가 예정되어 있다.

정보공유의 제한과 관련해 한국은 국가의 안전보장과 관련된 행정정보, 법령에 따라 비밀로 지정된 행정정보 또는 이에 준하는 행정정보는 대상정보에서 제외하고 있으며, 정당한 접근 권한을 가진자에게만 접근을 허용하고 있다. 정보공유의 제한 절차는 그 신청과 절차를 간소화 하여 공동이용의 활성화를 유도하고 있는데, 공동이용의 신청 후, 심사, 개인정보보호심의위원회의 심의, 보유기관의 승인이 있으면 공동이용승인이 이루어진다.

미국은 연방정보보호법 및 Privacy Act에서 공공기관의 SSN(사회보장번호) 공개를 원칙적으로 금지하고 있으나, 연방이나 주정부 기관이 이를 요구하는 경우, 제출의 필요성 및 법적근거, 사용목적 등을 미리 고지하도록 규정하고 있다. 독일의 '이의제기권(Widerspruchsrecht)'은 타 국가의 법률에 비해 보다 구체적으로 세분화되어 있다. 정보제공요구권, 수정요구권, 삭제요구권, 차단요구권을 상세하게 기술하고 있다. 수정요구권은 저장하고 있는 개인정보가 부정확하거나 불완전한 내용을 수정해야 하고, 차단요구권을 통해 본인과 관련된 개인정보가 적절한 조치를 통해 배포될

28) 컴퓨터연결이란 '여러개 파일에 담겨 있는 개인을 찾기 위해 둘 또는 그 이상의 컴퓨터 기록시스템을 비교(대조)하는 것(CIO리포트 30호: 행정정보공동이용 법제분석 및 시사점, 2010) 컴퓨터 연결프로그램을 통해 대조되는 기록이 프라이버시권 침해의 소지가 있다는 의견이 반영되어 1988년 '컴퓨터연결및프라이버시보호법'이 제정되었다.

수 없도록 차단을 요구할 수 있다. 정보의 제공 또는 이용은 제3자의 정당한 이익 또는 공익을 지키기 위해 필요한 경우이어야 하고, 행정기관이 정보주체의 수정, 차단 등의 요청을 거부하면, 연방정보보호·정보자유책임관(BDI)에게 신고하거나 관할법원에 소송을 제기할 수 있다.

<표 5-11> 정보자원 분배/공유 단계에서의 법제 비교

비교 내용(index)		한국	미국	독일
시스템 연계	운영 주체	- 행정안전부장관 소속 행정정보공동이용센터	- OMB,법무부, 국토관리부,	- 개인정보보호책임자(DSB)
	시스템 연계 범위	- 정보통신망의 구축을 통해 중앙부처 및 지자체, 행정기관과 연계된 공공기관의 통합·연계 운영	- 영역별, 사안별 - 예시로 법무부에서는 범죄예방 및 수사 등을 위한 정책과 집행, 서비스와 기술표준을 정비하기 위해 법집행 정보공동활용 프로그램(Law Enforcement Information Sharing Program: LEISP)추진 - 법무부와 국토방위부는 2005년 2월 NIEM(National Information Exchange Model; 정보교환을 위한 일련의 표준으로 분산된 시스템간에 정보의 공동활용과 변환을 가능하게 해주는 정보교환모델) 출범시킴. - 연방정부는 정부보조금혜택을 받고자하는 수혜자의 자격여부를 결정하기 위해 컴퓨터 연결(여러 개 파일에 담겨있을 수 있는 개인들을 찾기 위해 둘 또는 그 이상의 컴퓨터기록시스템을 비교하는 것)프로그램사용	
	외부/ 민간 연계 범위	- 금융권(제2금융권 포함) 및 교육기관(일부 비연계 DB존재)	- 보험, 금융, 부동산 등 민간영역에서 SSN(사회보장번호)를 요구하고 있으나 이의 제공은 정보주체의 선택사항	

표준 관리 지침	**표준 관리 지침 존재 여부**	- 공공기관 개인정보보호 지침 및 기관 별 실무 지침	- OMB Circular A-130 - 연방정보보안개혁법 - 연방정보보호지침	
중앙 관리 기구	**담당 기구**	- 행정안전부 및 정보보유 기관의 장 - 행안부는 행정정보 수요조사 및 행정안전부 장관의 공동이용 승인	- 정보화책임관협의회 (OMB의 장, 전자정부국장, CIA, 육·해·공군 3청의 정보화 책임관, CIO(최고정보관리책임자)	- 연방정보보호정보자유담당관(BDIB: 공공기관에 대한 감독) 및 감독관청(민간기관에 대한 감독)
	권한 정도	- 의견제시, 지도 및 권고, 감독	- 자료관리, 프라이버시, 기간 간 정보공유, 자료처리 자동화 도구나 기술의 획득 및 활용 등 제반 분야에 권한 미침, 정보자원관리권고안개발	- 연방정보보호법 (BDSG) 준수 여부에 대한 감독
	공유 과정 관리	- 처리정보이용제공대장에 기록하여 관리	- 각 행정기관의 장은 정보에 관리번호 등을 매겨서 관리하고 유효기간을 명시 - 관련기관들이 연결기록을 사용하기 위해서는 개인 프라이버시보호를위해 해당 기관들의 서면동의를 요구하고, 제안된 연결들에 관해 연방기록소(Federal Register)에 기록함으로써 시민들에게 사전 통지가 의무 - 컴퓨터연결프로그램을 수행하기 위한 목적과 법적 권한, 연결을 통해 사용될 각 정보, 연결될 기록들에 관한 구체적인 서면동의가 있어야만 컴퓨터연결 행해질 수 있음	
정보 공유의 범위	**공유 기관의 범위**	- 모든 행정기관, 79개 공공기관, 17개 금융기관 및 6개 교육기관		- 공공기관: 다른 공공기관(BDSG 제15조 제1항)이나 민간기관(BDSG 제16조 제1항)과의 공유 가능 - 민간기관: 정보제공업체에 대한 정보제공의 예외적 허용 (BDSG 제28a조 제1항)

	공유 정보의 수	- 92 종 공동이용 대상정보 - 민간기관과의 공유를 통한 부가가치 창출 도모		- EU 가맹국간 일부 개인정보 정보공유
	공유 비용 부담	- 공동이용센터를 통해 행정정보를 제공하는 기관은 이용기관에 비용을 청구하여 공동이용비용을 충당할 수 있음		
정보 공유의 제한	**열람권 제한**	- 국가의 안전보장과 관련된 행정정보, 법령에 따라 비밀로 지정된 행정정보 또는 이에 준하는 행정정보는 대상정보에서 제외, 정당한 권한을 가진자에게만 접근 허용	- 미국연방정보보호법은 공공기관에서의 사회보장번호(SSN)의 공개를 금지하고, 연방이나 주 정부기관이 이를 요구하는 경우 제출의 필요성, 요구의 법적 근거, 제공된 사회보장번호의 사용목적 및 제시거부의 경우 처리 방법등을 미리 고지하도록 규정 - 1975년 Privacy Act 제정 후 주정부, 지방정부기관에 대해 SSN사용 제한	- 차단요구권(BDSG 제20조 제3항 및 제35조 제3항)을 통해 개인주체가 본인에 관한 정보를 배포하거나 사용하는 것에 대한 차단을 요구할 수 있음
	절차 관리	- 신청·등록 간소화로 공동이용 활성화(공동이용신청→공동이용심사→개인정보보호심의위 심의→보유기관승인→공동이용승인)	- 행정기관은 10이상으로부터 필요한 자료를 요청할 경우 정당한 사유, 관리방안, 설문지안을 제출할 의무 부담(1942년 연방보고서법)	
외적 통제 체계	**아웃소싱 감시 관리**	- 감사원 및 시민단체		- 감리제도(BDSG 제9a조)
	공유 범위 및 과정 참여			- 정보제공·수정·삭제·차단요구권(BDSG 제6조 제1항)

4) 사용

정보의 질과 관련하여 두 국가에서 상위법에는 정보의 정확성을 위해 정보주체의 개인정보에 대한 정정 및 삭제의 요구가 있을 경우 즉시 조치를 취하도록 규정하고 있다. 개인정보 오남용 감시는 공공기관 개인정보보호에 관한 법률 제 3조 2항과 제 9조에서 내부통제, 이용자 접근 통제,

정보이용 실태에 대한 상시 모니터링 등 행정정보 오·남용 방지체계에 대해 명시하고 있다. 정보의 오남용이 있을 경우, 한국의 경우 개인정보 침해센터에 신고할 수 있으며, 분쟁사항이 발생시 개인정보분쟁조정위원회를 통해 해결 할 수 있다. 미국은 개인정보보호법(Privacy Act)과 컴퓨터연결 및 프라이버시보호법에서 목적외의 전산화된 기록 사용을 제한하고 있다. 제 3자에게 제공시, 개인정보의 사용을 감시 및 그에 대한 감사를 하도록 하고 있다. 오남용 보고체계의 경우, 미국은 개인정보 유출을 발견한지 60일 이내에 대상자에 통지해야 하며, 정보관리 및 처리기관은 프라이버시 담당자를 임명해야 한다. 또 민간정보를 소지한 기관의 소속 직원에 대한 정보보호 교육 및 훈련을 강화할 것을 규정하고 있다.

미국에서 먼저 시작한 개인정보영향 사전평가는 사전에 개인정보 유출 위험을 줄이는 정책으로 판단되며, 한국에서도 개인정보보호법 시행과 함께 도입된다. 독일이 경우 정보의 분배/공유 부분에서와 같이 '이의제기권(Widerspruchsrecht)'의 행사를 통해 본인과 관련된 개인정보가 적절한 조치를 통해 배포될 수 없도록 차단을 요구하거나 요청 거부 시, 소송을 제기할 수 있다. 독일의 전자매체법(TMG)의 정보보호원칙 제 12조 2항에 법률이 허용하거나 당사자의 동의가 있는 경우에만 전자매체의 개설을 위해 수집한 개인정보를 다른 목적이 이용할 수 있음을 명기하여, 원칙적으로 기타 목적을 위해 사용할 수 없도록 하고 있다.

<표 5-12> 정보자원 사용 단계에서의 법제 비교

비교 내용(index)		한국	미국	독일
정보의 질 관리	정확성 관리	- 정보주체의 개인정보에 대한 정정 및 삭제 청구시 조치	- 프라이버시법(Privacy Act)에서 정확성 및 비밀유지 등 규제 - 프라이버시 담당자에 대한 정보주체의 접근을 보장하고, 웹사이트를 통한 프라이버시 활동 등의 자료 공개 - 정보주체가 자신의 정보를 수정할 수 있도록 자기정보에 대한 접근 보장	- 이의제기권(Widerspruchsrecht)의 수정요구권

오남용 관리	**오남용 감시 절차**	- 공공기관의 개인정보 보호에 관한 법률 제3조의 2항과 제9조에서 내부통제, 이용자 접근 통제, 정보이용 실태에 대한 상시 모니터링 등 행정정보 오·남용 방지체계 명시	- '컴퓨터연결 및 프라이버시법보호법'에서 연방복지계획의 혜택을 받을 수 있는 자격 확인 및 만기일 넘은 채무공제 할 목적으로만 전산화된 기록을 비교하는데에만 적용하도록 목적 제한 - 개인식별정보를 내부적으로 활용시, 개인정보보호법(Privacy Act) 또는 공지된 바에 따라 인가된 목적으로만 사용 - 제3자에게 제공시 개인정보보호법(Privacy Act), 공지된 내용 또는 목적관련 범위 내에서 인가된 목적으로만 제공 - 제 3자의 개인정보사용을 감시, 감사	- 주 및 지방 데이터 보호 담당관(Datensenschutzbeauf-tragte)은 연방의 행정청이 데이터보호를 잘 수행하고 있는지 통제
	오남용 보고 체계	- 개인정보침해센터, 개인정보분쟁조정위원회	- 개인정보 유출을 발견한지 60일 이내에 대상자에 통지 - 정보관리 및 처리기관은 프라이버시 담당자를 임명 - 민간정보를 소지한 기관 소속 직원의 정보보호 교육을 강화	
목적외 사용 통제	**통제 규정 존재**	- 개인정보보호법, 개인정보사전영향평가제도입	- 프라이버시법, 프라이버시 영향평가제, OMB Circular A-130	-연방정보보호법(BDSG) 제2장 및 3장에 정보처리종사자는 적정한 임무수행에 속하는 목적이외의 보호되는 개인정보를 임의로 생산, 수집, 이용하지 못하도록 규정
	자율적 규제	- 행정안전부 개인정보보호지침	- 내부 프라이버시 감시 정책 존재	-기관내부 '자기통제'
외부적 통제 체계	**접근 가능 대상**	- 감사원, 국정감사, 정보주체	- OMB, 의회	
	접근 편의	- 정보주체의 개인정보에 대한 정정 및 삭제 청구할 경우 즉시 조치	- 정보주체가 프라이버시 담당자에게 접근이 용이하며, 자신의 정보를 수정할 수 있도록 자기 정보에 대한 접근 보장	

	통제 권한 정도	- 권고 및 시정조치 - 정보주체의 개인정보에 대한 정정 및 삭제 청구할 경우 즉시 조치	- 모니터링, 감사 - 정부주체에게 개인식별정보 수정 절차의제공 및 수정되는 개인식별정보에 관계되는 주체에게 수정 내용의 전차 절차 수립, 정보주체가 직접 수정할 수도 있음	- 감리제도

5) 폐기

정보의 폐기와 관련해서는 미국과 독일에 비해 한국에서 보다 적극적이면서도 구체적인 법제를 갖추고 있다. 한국의 개인정보보호법 및 행정안전부 개인정보보호 지침은 정보의 폐기에 대해 명백하게 규정하고 있음을 알 수 있다. 보유기간이 경과하고 개인정보의 처리 목적을 달성했을 경우와 같이 개인정보가 더 이상 필요하지 않게 되었을 때, 개인정보를 파기하여야 하며, 개인정보의 파기방법 및 절차 등에 관한 사항을 법률로 정하고 있으며, 개인정보를 보존해야 하는 경우, 개인정보처리자는 해당 정보 파일을 다른 정보와 분리하여 저장 및 관리하도록 하고 있다.

행정안전부 개인정보보호 지침의 경우 정보자원생애주기 중 정보의 폐기 부문에 비교적 많은 부문을 규정하고 있다. 개인정보 총괄부서는 정보의 보유 및 파기 현황을 주기적으로 조사하여 관리하며, 나아가 중앙행정기관, 광역자치단체와 같은 최상위기관은 하위기관의 정보보유 및 파기 현황을 주기적으로 조사하고 관리하도록 하고 있고, 개별 개인정보에 대해 변경, 수정, 보유기관의 만료와 같은 정보 보유가 불필요, 정보의 삭제에 대한 개인의 청구가 발생할 경우 이를 적극적으로 반영하여 조치를 취하도록 하고 있다.

그리고 개별 개인정보를 삭제할 경우 재사용이 불가능하도록 영구삭제를 규정하고 하고 있다. 이는 복구 할 수 없는 기술적 방법을 통해 원본을 포함해 백업본까지 파기하는 것을 원칙으로 한다. 미국의 경우, 많은 법률이 정보의 폐기에 관해서는 구체적인 규정을 하고 있지 않다. 보다 구체적인 폐기절차에 관해 한국의 개인정보보호법 및 공공기관의 개인정

보보호지침에는 개인정보처리부서의 장으로 하여금 입출력자료관리대장 및 개인정보 파일대장에 개인정보파일명과 주요기록항목 및 폐기일, 처리담당자와 처리부서장을 기록하도록 하고 있다. 또한 개인정보 취급자는 개인정보파일을 파기한 경우, 그 사실을 즉시 개인정보 총괄부서에 그 사실을 통보하고, 개인정보 총괄부서는 파기현황과 관련해 매월 조사하여 그 내용을 관보 및 기관 홈페이지에 공고해야 한다.

미국의 컴퓨터연결프라이버시보호법에서는 확인절차가 끝난 후, 해당 기관들은 관련정보를 삭제할 의무가 있다. 이 규정한 것은 지나친 정보획득 및 정보사용기관이 미래의 또 다른 사용을 위해 다른 기관에 넘겨줄 가능성을 제거하기 위한 목적으로 판단된다. 독일의 연방정보호법(BDSG)에 구체적인 폐기정보에 관한 내용은 보이지 않으나 정보의 폐기기한이 존재하고, 정보보호책임자는 자동화처리절차를 운영하기 전에 연방정보보호・정보자유담당관에게 정보폐기기한에 대해 보고할 의무가 있다. 또한 개인은 정보를 축적하는 것이 금지되어 있는 경우에는 삭제청구권을 가진다(김상겸, 김성준; 2008).

<표 5-13> 정보자원 폐기 단계에서의 법제 비교

비교 내용(index)		한국	미국	독일
중앙 관리 체계	담당 기구	- 행정안전부, 정보최상위 기관	- 해당기관	-해당기관
	관련 규정 존재	- 개인정보보호법 및 공공기관의 개인정보보호지침	- 컴퓨터연결및프라이버시보호법 (확인절차가 끝난 후에는 해당 기관들은 관련 내용 삭제 의무 있음)	
	폐기 정보 목록 관리	- 개인정보처리부서의 장은 파기사항에 대해 입출력자료관리대장 및 개인정보 파일대장에 관리 (개인정보파일명과 주요기록항목, 폐기일, 처리담당자 성명, 처리부서장 만 기재)		

	폐기 보고 체계	- 개인정보취급자는 개인정보파일을 파기한 경우 그 사실을 즉시 개인정보총괄부서에 통보하고, 개인정보 총괄부서가 파기현황과 관련하여 주기적(매월)으로 조사하여 관보 및 기관 홈페이지에 공고		
재생 및 재사용 가능성	**보존 비용의 부담**	- 해당 부처 관리		
	재생/ 재사용 가능성 평가	-없음		

Ⅵ. 우리나라의 정보자원관리와 갈등사례 분석

1. 정보자원관리 관련 갈등 분석의 필요성

과거와는 달리, 현대사회의 다원화와 이에 따른 불확실성 및 상호의존성의 증가는 다양한 분쟁과 갈등의 원인이 되고 있으며(주재복, 2000), 대형국책사업이나 지역개발, 비선호시설입지 등 정부의 공공사업을 둘러싼 갈등은 빈번하게 나타나고 있다(정건화, 2007). 기존의 공공갈등들은 특정한 시설 입지나 지역의 이익과 관련하여 표면화된 경제적 이익을 둘러싸고 나타난 것들이 대부분이었다. 하지만 기존 갈등상황과는 다르게 정보자원과 관련한 갈등양상은 정부행위와 관련한 특정 지역이나 집단들의 이해 문제가 아니며 정부가 정보자원을 통합 · 수집 · 사용 · 공유하는 과정에서 나타날 수 있는 인권이라는 측면에 대한 부분이기 때문에 기존의 갈등연구와 유사한 틀에서 갈등을 바라보기 보다는 정보자원이 가지고 있는 속성을 중심으로 또 다른 시각에서 갈등사례를 분석해야 할 것이다.

정보자원에 스며들어 있는 인권이라는 인간으로서 개인의 존엄성과 온전함 자체는 협상과 타협의 대상이 아니라는 측면에서 기존의 공공갈등사례의 시각으로만 다루어서는 안 되는 것이다. 정보자원이 가지는 속성과 더불어 기존 갈등과 다른 측면은 갈등의 이해당사자에 대한 부분이다. 정보자원과 관련한 갈등에 있어 본질적 이해당사자는 정보자원을 관리하는 정부와 정보자원의 주체인 국민이지만 정보자원의 인권적 문제에 대해 특정 개인의 침해가 이루어지기 이전에는 국민들 적극적인 행동양태가 나타나지 않은 경우가 많다. 따라서 정부행위에 대해 직접적으로 영향을 받게 되는 국민과 정보자원을 활용하는 정부 간의 이해와 관련한 갈등이라기보다는 정보자원 활용에 대한 서로 다른 가치를 가진 정부와 시민단체 간의 정보자원 관리에 대한 견해차로 발생하고 있는 것이다. 다시 말하면, 진보된 기술의 도입을 통해 효율성과 편의성에 대한 부분을 강조하여 조직

관리 및 국민편의라는 가치를 중시하는 정부조직과 변화된 기술 적용에 따른 이익 이면에 정보자원 관리에 의해 손상 받을 수 있는 인간의 기본적 권리에 보다 높은 가치기준을 두고 있는 시민단체들 간의 갈등이 나타나고 있는 양상이다.

한 사회에 새로운 기술이 도입되면 보다 빠른 기술의 도입을 위해 해당 기술이 가지고 있는 생산성 측면의 장점을 부각하게 되면서 변화된 기술적용에 따른 사회적 부작용에 대해 우려하는 집단과의 마찰과 갈등은 정도의 차이가 있을 뿐 지속적으로 발생되어 왔다. 이러한 갈등의 발생은 기술변화에 비해 제도의 변화 속도가 상대적으로 늦기 때문으로, 특히 가시적인 물적 성과 보다는 사회현상과 관련한 제도 및 관리의 변화가 더디게 이루어지면서 정보자원과 관련한 이해당사자들 간의 갈등이 발생하게 되었다.

현재 전자정부라는 개념을 도입한 이후, 여러 정부기관에서는 정보자원 활용 및 공유에 따른 효율성과 국민 편의성을 강조하면서 통합DB를 구축하고 있는 반면, 시민단체 등에서는 통합DB로 인한 정보인권의 침해에 대한 부분을 강조하면서 통합DB 구축에 대해 반대활동을 계속하고 있다. 이와 같이 정보자원을 다룸에 있어 각각 강조하는 측면과 견해차이로 인해 지속적인 갈등상황이 발생하고 있으며 정보자원과 관련한 갈등상황은 앞으로도 계속될 것으로 보인다. 따라서 정보자원의 보다 원활한 관리와 사용을 위해서는 정보자원과 관련한 갈등에 대해 분석하고 정보자원 관련 갈등관리에 대해 논의할 필요가 있다.

2. 갈등사례 분석 방법 및 기준

1) 분석 사례의 선정

정보자원관리의 실제를 알기 위해서, 전자정부 추진과정에서 효율성 가치와 인권적 가치가 충돌했던 대표적인 갈등사례를 대상으로 어떤 단계

에서 문제가 발생하였으며 어떠한 가치와 주장이 나타났는지를 분석하도록 한다. 지난 20여 년간 전자정부 추진과정에서 정부 정보관리와 관련하여 사회적 갈등을 일으켰던 갈등사례를 대상으로 정보자원생애주기 중 어떤 단계에서 무엇이 문제가 된 것인지 분석하고 현재까지의 갈등 패턴과 앞으로 도래할 정부 정보자원관리의 인권적 문제들을 추론하고자 한다. 이를 통해서 정보자원관리의 각 단계별로 어떤 인권적 요구들이 실제로 등장하고 있는지, 어떤 부분에서 법과 현실의 갈등이 나타나는지, 어떤 원칙들이 마련되어져야 하는지 등을 알 수 있을 것이다. 이와 같은 정보자원 관련 갈등사례 분석은 행위자간의 이해관계의 충돌에 초점을 두었던 기존의 분석과는 달리, 정보자원의 관리라는 측면에서 무엇이 실제로 문제가 되는가를 귀납적으로 도출함으로써 정보자원관리의 문제가 어디에서 오고 있는가를 알 수 있을 것으로 본다.

정보자원의 관리와 관련한 갈등사례들은 정보화 추진 과정상 갈등 사례를 분석한 선행연구들을 기반으로 하여, 사회적으로도 중요한 이슈가 되었고 학술적으로도 의미 있는 사례로 연구되었던 것들을 대상으로 하였다. 또한 정보인권과 관련된 NGO(진보넷 등)의 문헌 및 홈페이지 상에서 중요한 이슈로 다루었던 사례들을 기준으로 하여 선정하였다. 정보화 추진과정에서 새롭게 정책이 수립되거나 현재 진행 중인 사례 보다는 지금까지 구축되어 운영되고 있는 정보자원 관리의 사례를 다루도록 한다. 정보화가 구축되지 않은 사례의 경우는 해당 문제에 대한 갈등을 예측할 뿐이며 정보자원 관리에 있어 인권적 측면에 대한 문제와 갈등을 실제적으로 분석하기 어려운 측면이 있기 때문이다.

본 갈등사례의 분석대상은 교육행정정보시스템(NEIS), 형사사법통합정보체계(KICS), 보건기관정보통합이다. 이러한 세 가지 분석대상은 정보의 성격, 서비스의 성격, 시간의 구분이라는 이유에 따라 선정하였다.

먼저, 정보의 성격 측면에서는 세 가지 사례 모두 국민 개인의 생애주기에 따른 민감한 인적 정보를 다루고 있다는 공통점을 가지고 있다. 교육 정보, 형사사법 정보, 보건의료 정보는 거의 대부분의 사람들이 태

어나 삶을 살아가는 과정에서 발생하는 정보이고 이는 개인의 삶에 대한 일련의 과정을 설명해 주는 것들이다. 우리는 누구나 교육을 받게 되고, 의도하든 의도하지 않든 형사사법과 관련한 일을 겪게 되며, 보건의료와 관련하여 질병치료나 예방행위를 하기 위해 병의원을 찾게 된다. 그리고 그 과정에서 보다 나은 서비스를 받기 위해 정보를 제공하게 된다. 모여진 정보들은 개인이 어떠한 교육을 어느 곳에서 받았는지, 언제 운전면허를 취득하고 어떤 형사사안과 관계가 있는지, 무슨 병을 얻어서 어떤 병의원에서 치료를 받았는지에 대한 것들이어서 이를 통해 개인의 삶을 투영할 수 있는 기재로 활용이 가능하다. 따라서 해당 인적정보가 가지는 민감성을 고려했을 때, 해당 사례들은 정보자원의 관리와 관련하여 상당한 중요성을 가지고 있으며 이에 따라 높은 수준의 갈등이 나타났거나 나타날 가능성이 높은 것들이다.

두 번째 서비스의 성격이라는 점에서, 세 가지 사례에서 제공하고 있는 교육서비스, 형사사법서비스, 보건의료서비스는 국민과 접점하고 있는 서비스이고, 이들 서비스를 관리하고 제공하는 과정에서 국민과 직·간접적으로 대면하게 되는 경우가 많다. 국민과 접점하고 있는 서비스는 국민들과 마주하게 되는 경우가 상대적으로 많기 때문에 공공 서비스의 제공과정에서 민원이 발생할 소지가 높으며, 서비스 제공을 위한 정보자원 활용에 있어서도 국민과 직접적으로 갈등이 발생할 가능성이 높다.

세 번째, 시간의 구분이라는 측면에서 세 가지 사례는 정보자원의 인권적 측면과 관련한 갈등에 있어 과거, 현재, 미래를 조망할 수 있는 사례로, 과거사례에서의 교훈을 현재에 대입하고, 미래에 도입될 시스템에 대한 대비라는 점에서 갈등사례로 선정하게 되었다. 전자정부 이후, 가장 사회적으로 이슈화된 갈등사례는 NEIS 사례이다. 정보자원 통합DB와 관련하여 사회적으로 가장 이슈화되었으며, 정부 정보자원에 대한 인권적 문제가 본격적으로 제기된 것이었다. 이후, 2010년에 운영을 시작한 KICS의 경우는 여러 시민단체에서 정보인권문제를 지속적으로 제기하고 있으며, 보안 사항이라는 이유에서 정보주체의 권리를 인정해 주고 있지 않는

형사사법 당국과 갈등양상을 나타내고 있다. 특히 형사사법에 대한 정보는 인권과 직접적인 관계를 가진다는 측면에서 높은 갈등수준을 가진 사례라는 점에서 현재 이슈화되고 진행 중인 사례이다. 정보자원과 관련한 갈등에 있어 보건의료정보통합은 현재 추진 중인 사업으로 의료정보라는 개인의 민감한 정보자원을 통합DB화함에 있어 나타날 수 있는 인권적 문제들을 가지고 있는 사례이다. 본격적으로 구축되어 있지 않기 때문에 이에 대한 표면적인 갈등이나 대립구조가 명확하지 않으나 보건의료정보는 병의원 등에서 수집 · 저장 · 공유 빈도가 상당히 높은 정보이고, 개인의 질병과 관련한 민감한 사항이기 때문에 해당 의료정보의 통합화가 본격화될 경우에 인권적 이슈가 제기될 가능성이 높은 부분이다.

이와 같은 세 가지 이유를 바탕으로 교육행정정보시스템, 형사사법통합정보체계, 보건기관통합정보시스템을 본 갈등분석의 사례로 삼았으며, 각 사례에서 발생하는 이슈와 세 사례를 통합한 관점에서의 이슈에 대해 논의하도록 하겠다.

2) 분석 방법

정보자원을 둘러싼 갈등사례에 대해 다루었던 연구들이 있지만, 기존 연구에서는 정보자원의 생애주기 차원에서 어떤 특징을 보이는지에 대해서는 분석되지 않은 경우가 대부분이다. 정보자원과 관련한 갈등사례들은 기존 이해관계를 중심으로 한 공공갈등사례들이 가지는 갈등단계(갈등잠복-갈등표면화-갈등확대-갈등완화-갈등해소)라는 특징에 크게 부합되지 않는다. 왜냐 하면 정보자원은 특정 정책 등과 같이 협상과 조정을 통해 관리해야 하는 성격이 아니라 정부활동에 상시적으로 필요한 자원 중 하나로, 효과적으로 사용하기 위해 지속적으로 관리해야 하는 대상이기 때문이다. 그리고 정보자원은 전자정부의 개념이 도입된 이후로 지속적으로 활용되고 있는 정보화시대의 핵심자원 중 하나로, 정보화와 관련한 새로운 기술의 진보가 있을 경우에 정보자원의 활용은 더욱 활발하게 이루어 질 것이다.

앞서 언급한 바와 같이 정부는 2009년부터 2013년까지 국가DB구축 중기계획을 가지고 있는 등 정보자원 활용을 더욱 원활하게 하기 위한 노력을 지속할 것으로 예상 할 수 있다. 이에 공공기관에서 활용하게 되는 정보는 지속적으로 생성되고 폐기되는 과정을 반복할 것이기 때문에 새로운 정보의 활용이 또 다른 갈등을 야기 할 수 있다. 따라서 정책수립에 따른 시설이나 제도와 관련한 이해관계에 대한 갈등사례와 같이 갈등이 완화되거나 해소될 가능성이 그리 높지 않다. 이러한 이유에서 정보자원과 관련한 갈등사례에서는 협상이나 조정의 방법으로 갈등을 완화하기 보다는 상시적으로 관리해야 한다는 관점에서 갈등사례를 바라봐야 할 것이다.

우리나라의 경우는 개별 중앙정부 부처 및 기관의 수준에서의 정보자원관리는 정보를 수집 및 생성, 보관, 분배 및 공유, 사용, 폐기하는 단계를 효과적이고 효율적으로 수행하는 것(최홍석 · 구상회 · 이정준, 1999)으로 개념화하고 있다. 정보자원을 생애주기에 따른 흐름으로 관리함으로써 보다 체계적인 정보자원의 관리가 가능하도록 하고 있다. 정보자원생애주기 단계별 적절한 정보자원관리의 목표를 검토하면서 관리계층과 생애주기의 결합(최홍석 외, 1999)이 가능할 것이고, 각 정보자원생애주기 별로 각각의 이슈를 가지고 있기 때문에 정보자원생애주기라는 관리흐름 속에서 정보자원과 관련한 갈등사례를 분석하는 것이 필요하다. 이에 본 장에서는 정보자원 생애주기라는 관점에서 기존 자료를 바탕으로 사례를 재구성하여 특징을 도출하려 한다.

3. 정보자원생애주기에 따른 갈등사례 분석

1) 교육행정정보시스템

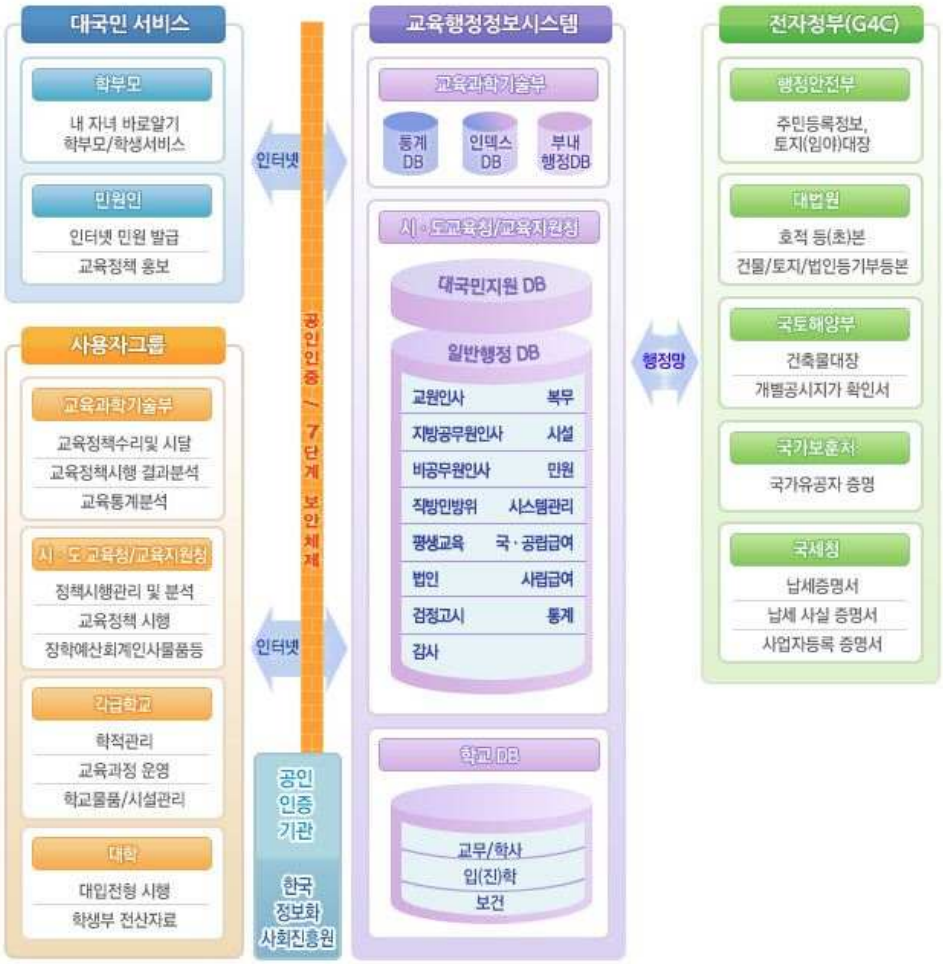
(1) 교육행정정보시스템의 사업개요

교육행정정보시스템(NEIS: National Education Information System, 이하 NEIS)는 전국 1만여 개 초·중·고·특수학교, 178개 교육지원청, 16개 시·도 교육청 및 교육과학기술부가 모든 교육행정 정보를 전자적으로 연계 처리하며, 행정안전부(G4C), 대법원 등 유관기관의 행정정보를 이용하는 종합 교육행정정보시스템으로 교육행정기관의 제반 업무를 전자적으로 연계·처리하는 시스템으로, 학교의 모든 행정 정보, 학생 정보를 포함하여 27개 영역, 약 6,000여개 항목에 달하는 상당한 규모의 행정정보시스템이다. NEIS는 '교육기본법 제23조의2(학교 및 교육행정기관 업무의 전자화)', '초·중등교육법 제30조의4(교육정보시스템의 구축·운영 등)', '동법 제30조의5(정보시스템에 의한 업무처리)', '공공기관의 개인정보보호에 관한 법률 제4조(개인정보의 수집)', '교육공무원법 제 23 조의 2(인사관리의 전자화)' 등에 운영근거를 두고 있으며, 기존에 학교 단위로 구축되어 있었던 정보시스템을 개편하여 교육부, 교육청 등 모든 교육행정기관과 초·중등학교를 인터넷으로 연결하여 교육행정 업무를 전자적으로 연계하여 처리 할 수 있도록 구축한 시스템을 의미하는 것으로, 교원, 학생, 학부모의 교육정보에 대한 요구를 충족시키기 위한다는 목적을 가지고 있다. 대국민 교육행정서비스를 개선하고 학부모의 교육 관심과 참여를 확대하며 교육행정 업무의 효율성을 향상시키고 교원들이 교육 본연의 임무에 충실한 환경을 조성(나태준, 2006)할 수 있을 거라는 가정 하에 해당 사업은 추진된 것이다.

NEIS 도입에 따른 기대 효과는 ① 국민과 학부모를 위한 서비스의 질 향상(인터넷을 통해 졸업증명서, 성적증명서 등의 민원서비스 가능) ② 자

녀의 학교생활 정보의 손쉬운 접근(자녀의 학업성취 등을 비롯한 학교생활의 기록 등) ③ 교원들의 잡무 경감과 교육의 질 향상(통계 자료 작성, 관련 공문서 작성 등의 행정 업무 부담 감소), 그리고 ④ 업무의 효율적 처리(기관 간, 업무 간 자료의 공동 활용 등으로 간편화)가 가능해 진다는 것이다.

<그림 6-1> NEIS 개념도



자료: NEIS 홈페이지(http://www.neis.go.kr/)

<표 6-1> NEIS 시스템 업무 영역(27개 영역)

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, 실험실습재료관리, 기자재 기준안관리, 기자재 현황관리, 기자재 통계
예산	예산편성, 예산배정, 예산이월, 예산운용, 예산통계
회계	세입, 세출, 세입세출 외 현금, 계약/압류, 결산, 자금
학교회계	예산, 세입, 세출, 결산, 세입·세출 외 현금, 세무관리, 발전기금
급식	학교급식통계, 급식관리, 급식외 관리, 급식분석
시스템	코드관리, 시스템연계, 보안, 사용자 인증 및 권한관리, 로그관리, 인터페이스관리, 배치작업관리, 업무처리승인관리

자료: NEIS 홈페이지(http://www.neis.go.kr/)

(2) 추진배경

NEIS는 2009년 시작하여 2001년 전자정부 11대 사업의 하나로 추진되었으며, 총 521억원의 사업비가 소요되었다. NEIS의 추진목적은 ① 업무처리방식 개편을 통한 교원 업무 경감, ② 자녀의 학교생활정보 제공을 통한 학교와 가정의 역할제고, ③ 국민을 위한 빠르고 편리한 민원서비스 제공, ④ 교육행정업무의 효율적 처리와 투명성 제고, ⑤ 대입전형자료의 전자적 One-Stop 서비스 제공을 통한 투명하고 편리한 대학입시 지원, ⑥ 국가경쟁력제로를 위한 지식정보사회형 전자정보 확립 등으로 기존의 C/S(Client Server)에 비해 대국민 교육행정서비스를 개선하고 학부모의 교육관심과 참여를 확대하며, 교육행정업무의 효율성을 향상시키고 교원들이 교육 본연의 임무에 충실한 환경을 조성 할 수 있을 것으로 기대하였다.

(3) 추진경과

국민의 정부 시절, 2000년 신년사에서 지식정보강국을 위한 교육정보화계획이 처음 언급되었고, 2000년 7월에 '전국단위 교육행정정보시스템 구축을 위한 기본계획 수립하고 1단계 사업으로 '업무 재설계 및 정보화 전략계획 수립"에 대하여 정보통신부 및 한국전산원에 정책 사업 지원을 신청하면서 본 사업은 시작하게 되었다. 이후 2001년 3월에 '교육행정정보시스템구축을 위한 재설계 및 정보화 전략계획'을 수립하였고, 동년 7월에 교육행정정보시스템 구축계획을 확정하였다. 해당 사업이 확정된 이후, 2002년 10월부터 '전국단위 교육행정정보시스템'으로 통합되어 운영하였으나, 보급초기 전교조에서 학생 및 학부모 신상공개에 인권문제차원에서 반대에 부딪히게 되었고, 2003년 4월 NEIS 시행 때는 시행결정에 따른 전교조 연가투쟁 결정되는 등 NEIS에 대한 반대운동은 사회적으로 큰 이슈가 되었다. 이에 2003년 5월에 국가인권위원회가 NEIS의 인권침해소지 인정 및 수정 권고되었고, 교육부-전교조 합의 발표로 국가인권위원회의

권고안을 수용하게 되어 2003년 5월 31일에 NEIS를 재시행하도록 하였다.

최종적으로는 2003년 12월 15일에 당시 국무총리실 산하 교육정보화위원회에서 교무/학사, 보건, 입/진학 등 3개 영역은 기존 NEIS로 부터 물리적으로 분리해 별도 시스템을 구축/운영키로 하고, 3개영역의 데이터 베이스서버를 16개 시도교육청에 두되 통합시스템이 아닌 학교별 단독서버로 나눠 운영하도록 확정하는 교육부의 최종합의안이 발표되면서 NEIS는 현재의 모습으로 운영되고 있다.

<그림 6-2> NEIS 추진경과

자료: NEIS 홈페이지(http://www.neis.go.kr/)

(4) 정보자원 생애주기에 따른 분석

정보자원의 인권적 측면에 관련한 갈등사례는 정보자원 생애주기에 따라 분석할 필요가 있다. 앞서 언급한 바와 같이 우리나라의 정보자원관리는 정보를 수집 및 생성, 보관, 분배 및 공유, 사용, 폐기하는 단계를 효과적이고 효율적으로 수행하는 것으로 개념화하고 있으며, 각 생애주기의 단계별로 인권적 이슈가 달라질 수 있으므로 정보자원 생애주기에 따라

갈등사례를 분석해야 할 것이다.

① 수집 및 생성

교육 과정에서 학생의 개인 정보를 수집하는 것은 불가피할 뿐만 아니라 반드시 필요한 일이기도 하다. 교사, 학생, 학부모 모두 이를 부정하는 사람은 아무도 없을 것이다. 하지만, NEIS의 가장 큰 문제점은 정보 자체를 수집하는 것이 아니라 정보 주체의 동의 없이 개인 정보를 집적했다고 하는 점이다. 이는 수집제한과 관련한 자기정보통제권에 대한 침해 문제이다. 지금까지는 학생, 학부모, 교사들에 대한 정보를 명확한 목적이나 정보 주체의 동의 없이 무분별하게 수집해왔으며, 또 수집된 정보를 안전하게 보호하기 위한 원칙도 없었다. 국가든 민간이든 어느 정도의 개인정보를 수집, 관리하는 것은 필요할 것이다.

따라서 NEIS의 문제는 국가가 개인 정보를 수집해서는 안 된다는 것이 아니라, 국가가 국민들의 개인 정보를 수집할 경우에도 정보인권 보호라는 원칙이 적용되어야 한다는 것이다. 이에 수집제한의 원칙이 요구된다. 수집제한의 원칙이란 정당한 수집목적 하에, 필요한 범위 내에서, 공정하고 합리적인 방식으로, 정보주체의 분명한 인식 또는 동의하에 수집되어야 한다는 원칙이다. 하지만, 교육당국은 NEIS 도입 초기에 학생의 민감한 각종 개인정보를 개별 당사자의 동의 없이 국가에서 일방적으로 수집하거나 기존에 수집된 정보에 대한 통합화와 관련하여 개별 당사자의 동의를 구하지 않았다. 이는 정보의 수집 및 생성과 관련하여 정보주체의 동의와 선택권을 정부에게 보장하고 있지 않는 것으로, 정보주체가 당연히 누려야 할 자기 정보에 대한 통제권한을 정부의 필요에 의해 보장하지 않고 있었다.

학생이나 학부모의 신상정보를 기록하기 위해서는 이에 대한 명확한 목적과 법적 근거를 마련해야 하며, 이를 바탕으로 정보수집 및 생성 활동을 해야 한다. 이에 교육부에서는 「초 · 중등교육법 제25조」에 근거하

여 학생과 학부모의 정보를 수집할 수 있다는 주장하면서 개인정보 집적에 대한 법적근거를 내세웠고, NEIS 도입에 대한 정보수집의 정당성을 주장하였다. 하지만, 이에 대해 참교육학무보회 등 24개 교육관련 시민단체와 더불어 전교조는 해당 법적 근거와 관련하여 NEIS의 인권침해에 대해 국가인권위원회에 제소하였고, 국가인권위는 2003년 5월에 해당 법령에서는 학교생활기록부 작성기준 만을 의미하는 것으로, '전산화 내지 자료의 수집과 대학에의 자료제공에 관해서는 사생활 보호 등을 감안하여 별도의 법적근거가 필요하다' 는 권고사항을 발표하게 되었다.

또한 이와 관련하여 헌법재판소는 학교에서 수집하는 불필요한 개인정보의 불법 유통을 금지하도록 결정을 내리면서 교육부는 NEIS 반대의 목소리를 수용하여 수집정보의 종류를 축소하여, 교무/학사, 입(진)학 및 보건 영역은 NEIS 정보입력 대상에서 제외되었다. 정보자원을 수집하기 위해서는 이를 정당화할 수 있는 명확한 목적과 법적 근거가 수반되어야 하는데, 현재 여러 정보자원들이 NEIS 사례와 유사하게 명확한 법적 근거가 나타나지 않고 수집을 통한 축적을 우선시하는 경우가 많아 이에 대한 갈등이 발생하게 되었다.

정보를 수집하는 정부기관은 정보를 자원으로 인식하기 때문에 되도록 많은 정보를 축적하고 싶어 한다. NEIS를 통해 교육부가 추구하는 궁극적인 목표는(나태준, 2006)은 행정의 효율성이다. 이에 NEIS를 통해 수집된 정보들은 학생을 지도하는데 자료로 활용하기 위해 정보를 수집함에 있어 되도록 많은 자료를 적은 시간 내에 취합하고자 하였다. 하지만 새로운 정보를 수집하거나 이미 수집된 문서자료를 DB화하는 과정에서 정보 주체의 동의를 일일이 받거나 법적 근거의 마련이 완료될 때까지 기다린다면 NEIS를 통해 추구하려던 행정의 효율성은 기대한 만큼 확보되기 어렵다. 이에 자원의 활용의 효율성을 우선시 하여 정보수집에 필요한 동의와 근거마련을 소홀히 한 것이다.

많은 정부들은 '정보를 공기와 같은 자유재로 인식하고 언제든지 얻을 수 있는 것' 으로 보는 인식체계를 가지고 있었기 때문에 정보수집에

있어 정보주체의 동의와 선택권을 보장하거나 명확한 근거를 마련하여 정보를 수집하지 않는 모습을 보여주었다. 하지만, OECD 개인정보보호에 관한 8원칙, APEC 개인정보보호에 관한 원칙 등에 의하면 정보의 수집 · 이용 · 공개와 관련하여 정보주체가 선택권을 행사할 수 있도록 하고 정보주체의 동의를 얻어 개인정보수집을 하도록 하는 등 정보자원은 자유재가 아닌 정보주체가 가지고 있는 고유의 가치로 인식하고 있다.

따라서 각 개인의 가지고 있는 고유의 가치를 활용하기 위해서는 각 개인에 대해 자신의 정보를 제공받을 수 있는 동의 혹은 많은 사람들이 인정하는 명확한 법적 근거를 마련해야 하는 것이다. 그러나 이러한 정보인권에 대한 원칙 보다는 자원 활용의 효율성을 우선시 한 교육부에 대해 명확한 법적 근거의 마련과 정보주체의 동의 및 선택권과 관련하여 정보주체자인 학생과 학부모, 시민단체들이 반발을 하면서 갈등이 발생하게 되었다.

② 보관 및 저장

보관 및 저장과 관련하여 정보자원의 인권적 관리가 이루어지기 위해서는 개인정보분리의 원칙이 보장되어야 한다. 이 원칙은 특정 목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 통합되지 않고 분리된 상태로 유지되어야 한다는 요청이다. 정보자원이 통합화되어 운영될 경우, 단 한 번의 정보유출을 통해 다량의 정보자원 가 유출되면서 상당한 수준의 정보인권의 침해가 나타날 가능성이 높다. 보유하고 있는 개인정보의 손실, 허가받지 않은 접근, 파괴, 수정 혹은 오용을 방지하기 위해 적절한 보안수단을 제공해야 하는 안정성의 원칙이라는 측면과도 관련이 있다. 이에 정보의 통합화를 진행하려는 교육부와 통합된 정보화에 의한 정보인권 침해에 대해 우려하는 시민단체 간 갈등이 발생하였다.

<표 6-1>의 NEIS 시스템 업무 영역을 보면, 총 27개 영역에 대한 교육

관련 정보가 NEIS에 저장되어 있다. 해당 정보들은 학생 및 학부모 뿐 아니라 교원과 관련한 정보들도 포함되어 있는 것으로 해킹 등 외부로 부터의 공격이나 내부자에 의한 유출이 발생할 경우는 한꺼번에 많은 정보가 유출되어 심각한 인권적 문제를 야기할 수 있다. 이러한 이유에서 시민단체들은 집적화되어 있는 정보를 독립화하여 집적화에 따른 대규모 정보유출의 위험방지하기를 요구하였다. 하지만, 정보 통합화의 목적은 정보의 집적을 통해 정보공유에 따른 행정비용과 소요시간을 줄이기 위함이기 때문에, 교육부는 별도 서버 구축에 따른 시스템 구축비용을 강조하면서 One-Stop 서비스를 가능하게 하고 시스템 구축비용을 최소화하기 위해서는 가급적 서버의 숫자를 줄이고 일괄적으로 관리 · 운영해야 한다고 주장했다(지속가능발전위원회, 2006).

또한 서버를 학교별로 두고 각 학교가 관리해야 한다는 전교조 등 시민단체의 주장에 대해 서버를 학교별로 둘 경우에는 교원이 시스템을 직접 운영해야 하는 문제가 있기 때문에 비용의 발생과 더불어 교원 업무경감이라는 본래의 취지가 훼손될 우려가 있음을 언급하였다. 이는 효율성을 강조하는 도구적 합리성이나 기술 관료제적 의사결정에 대한 관점으로, 앞서 언급한 바와 같이 과학기술의 발전에 따른 인간의 생산능력을 발전시켜 인간의 행복을 증진시키는 입장이다.

하지만, 여러 시민단체들은 정보 집적으로 인해 나타날 수 있는 대규모 정보유출의 문제를 제기하면서 교육부의 주장에 대해 반대의견을 내세웠고, 교육정보의 분리 저장에 대한 주장을 전개하면서 갈등양상을 보였다. 정보의 저장과 관련한 양 측의 갈등과 관련하여 국가인권위원회에서는 초·중등교육법 제25조, 교육기본법 제23조2에 근거하여 학교에서 수집한 학생관련 개인정보를 16개 시도교육청 서버에 집적하여 관리하는 NEIS 법적근거를 불분명하다고 밝히고, 민원사무처리에 관한 법률 제5조 제1항, 법시행령 제11조 제2항에 근거하여 학교에서 수집 작성된 개인정보를 NEIS에 집적하는 법적근거의 모호성 제시하면서 NEIS 정보집적에 대해 부정적 입장을 취하였다.

정보자원의 집적화와 관련한 양 측의 갈등에 의해 2003년 국무총리실 산하 교육정보화위원회에서 교무/학사, 보건, 입/진학 등 3개 영역은 기존 NEIS로 부터 물리적으로 분리해 별도 시스템을 구축/운영키로 하고, 3개 영역의 데이터 베이스서버를 16개 시도교육청에 두되 통합시스템이 아닌 학교별 단독서버로 나눠 운영하도록 확정하는 교육부의 최종합의안이 발표하여 NEIS 관련 정보들의 분산 저장을 통해 저장의 안정성을 확보하고 정보자원의 저장관리에 따른 갈등소지를 줄이려는 노력이 이루어졌다.

수집된 정보를 보관 및 저장하는데 있어서 중요한 것은 저장된 정보를 안전하게 보관하기 위한 조치가 이루어져야 하는 것인데, 통합DB에 의한 정보의 집적화는 정보의 안전한 저장에 대한 문제를 야기 할 수 있는 부분이다. 많은 조직에서 정보보안을 위해 노력하고 있지만, 외부의 침입으로 인해 정보가 유출되는 사례는 심심치 않게 나타나고 있다. 따라서 외부 침입의 가능성이 상존하는 상황에서 정보를 하나의 서버에 집적하는 것은 한 번의 침입으로 다수의 정보가 유출 될 가능성을 높이는 관리상의 문제를 야기할 수 있다. 이에 집적화를 통해 효율성을 확보하려는 교육부와 혹시 발생할 수 있는 외부 침입에 대한 피해를 최소화하고 저장된 개인정보의 안전한 관리를 주장하는 시민단체 간에 갈등이 발생하게 되었다.

③ 분배 및 공유

2003년 NEIS와 관련한 국가인권위원회 결정과 국무총리실 산하 교육정보화위원회의 발표에 따라 NEIS는 분산된 서버의 형태로 운영 중에 있다. 정보의 분산은 정보의 원활한 공유를 통한 정보 요구 충족이나 정보의 효율적 공유를 위한 기술적 환경의 마련에 측면에서는 바람직하지 못한 결과라 할 수 있다. 그래서 교육부는 전국 시 · 도 교육청과 초 · 중등학교에서 활용하고 있는 현 NEIS의 노후화된 서버와 비효율적인 서버운영을 개선하기 위해 2010년부터 서버시스템 교체와 통합을 추진하고 있다. 정보의 집적을 다시 추진하면서 정보자원 활용의 효율성을 확보하는 관리의 측면

은 일정부분 필요하다. 그러나 정보의 집적화는 저장에서의 문제와 더불어 정보의 공유와 분배에 있어 목적외 이용을 확대시킬 가능성이 있다.

지난 2003년 12월 충남지역 고3 학생 768명이 대입용 NEIS CD에 자신의 정보를 제거해 달라는 내용의 서명서를 충남도교육청에 제출했다. NEIS CD는 교육부에서 대입전형자료를 제출하도록 지시한 것으로, 학생들의 신상정보를 CD에 담아 자신이 지원하는 대학 뿐 아니라 지원하지도 않은 전국의 모든 대학에 배포하게 한 것이다. 해당 정보자원의 공유는 법적 근거 없이 개인정보를 제3자에게 제공하는 것으로 인격권을 침해하고 사생활의 비밀과 사생활의 자유의 불가침에 반하는 것으로, 정보의 공유와 분배에 있어 목적외 이용이 용이하도록 하는 위헌적 행위라 할 수 있다. 해당 내용이 알려지고 위헌판결이 났지만, 교육부는 해당 학생들을 제외한 나머지 학생들의 정보들은 CD로 배포하겠다는 주장을 하면서 시민단체와 갈등을 빚은바 있다.

대학입시와 관련하여 집적되어 있는 학생들의 정보를 목적에 맞게 최소한으로 공유하지 않고 대규모로 배포하려 한 것과 해당 공유 및 배포는 정보주체인 재학생의 동의가 있지 않은 채 정부의 일방적 결정으로 이루어 진 측면에서 인권적 관리에 있어 큰 문제를 가져올 소지가 있었다. 정보주체의 동의가 있거나 법 규정에 있는 경우를 제외한 목적외 이용 및 공개 금지(이용 제한의 원칙)를 준수하지 않은 사례로, 정보의 집적에 따라 CD의 제작이 용이해 졌다는 점에서 정보의 집적이 쉽게 정보를 공유할 수 있도록 하였지만, 이에 따른 인권적 문제를 가져올 수 있다는 점을 보여주고 있다. 또한 목적외 이용과 관련하여 NEIS 관련 시행령에서는 수집된 자료가 다른 기관에 제공될 수 있는 길을 열어 놓아서, 개인의 신상기록이 행정안전부나 병무청, 경찰청, 국정원 등 교육과 관련이 없는 기관에 광범위하고도 용이하게 정보가 공유될 가능성이 높아서 정보주체의 권리를 침해할 가능성이 높다.

정보자원의 목적외 이용금지 외에도 분배 및 공유에 있어 정보주체의 자기정보 접근에 대한 부분도 중요한 이슈이다 정보자원이 어떤 과정을

통해 어느 기관에서 공유되어 활용되었는지 확인하기 위해서 자기정보 접근이 필요하며, 이는 정보주체의 권리에 해당하는 것이다. 하지만, 교육부는 NEIS에 수집된 본인 정보를 담임선생님 또는 학부모를 통해서만 열람하도록 하여 정보주체인 재학생의 접근을 시스템 상에서 차단한 사례가 있다. 이에 시민단체에서는 정보주체인 학생들의 접근이 가능하도록 하는 관리적 차원의 조치가 필요하다고 주장하고 있지만, 교육부는 재학생의 자기정보열람과 관련해서는 시스템 구축비용과 관련하여 차후 NEIS 중장기 발전계획 수립에 포함시키겠다는 입장이다. 아직까지도 정보주체가 자신의 정보의 공유여부에 대해 확인할 방법이 제시되지 않고 있다는 면에서 해당 이슈에 대한 갈등의 소지는 상존하는 것이며, 인권적 문제를 다시금 불러일으킬 가능성이 높은 상황이다.

④ 사용

OECD 개인정보보호 8원칙에서는 정보자원의 사용과 관련하여 이용 목적과의 관련성(정확성확보의 원칙), 명시된 목적에 적합한 개인정보의 이용(목적명시의 원칙), 정보주체의 동의가 있거나 법 규정이 있는 경우를 제외하고는 목적외 이용 및 공개 금지(이용제한의 원칙)을 말하고 있다. 그리고 ‘공공기관의 개인정보보호에 관한 법률’ 제3조의2와 제9조에서 정한 바와 같이 공동 이용하는 정보가 안전하게 관리·유통될 수 있도록 해야 함을 명시하고 있다. 하지만, NEIS CD 배포와 같이 정보가 안전하게 관리·유통되는지 여부를 확인할 수 없는 방식이 다시 활용된다면, 정보자원의 사용 측면에서 정보인권의 문제가 다시 붉어질 수 있게 된다.

NEIS 생활기록부 CD 제작 및 배포와 관련한 이의 제기는 충남지역 뿐 아니라 타 지역에서 나타난바 있다. 해당 사안과 관련하여 서울지방법원 민사50부는 “교육기본법 제23조의 규정은 국가 및 지방자치단체에 교육의 정보화, 학교교육행정의 전자화를 위한 시책을 수립할 의무만 부과하고 있을 뿐, 국가 및 지방자치단체에 생활기록부 전산자료를 사용할 권한

까지 부여하고 있지 않다”고 판결하면서 NEIS 정보사용과 관련한 판결을 내린바 있다. 하지만, 여전히 NEIS의 사용과 관련한 명확한 법 규정은 제정되지 않고 있다. 명확한 법 규정이 존재하지 않는 다는 것은 정확성 확보의 원칙, 목적명시의 원칙, 이용제한의 원칙이 정보자원의 사용과 관련하여 확보되지 못함을 의미한다. 이에 동 법원은 “교육부 장관에게 대학입시 전형자료인 생활기록부 전산자료를 제출받아 이를 각 대학에 배포할 수 있는 권한까지를 부여한 것이라고는 볼 수 없다”고 밝혔다.

이처럼 NEIS 사용과 관련한 갈등발생 이유는 관련 제3자에 정보를 제공하는 것과 관련한 법 규정이 명확히 제시되지 않기 때문이다. 이는 자칫 정보자원의 관리에 있어 관리주체인 정부가 자의적 판단에 따라 정보자원을 사용할 가능성이 있는 것으로, 정보자원의 효율적 사용을 우선시하는 정부기관의 입장에서는 NEIS CD와 같은 사례를 또 다시 만들 수 있게 된다. 명확한 근거가 있지 않은 상황에서 정보를 사용하는 것은 목적외 활용금지라는 원칙을 배제하는 것으로 정보주체의 정보인권을 침해하는 문제로 연결될 수 있다. 이러한 오남용을 막기 위해 ‘공공기관의 개인정보보호에 관한 법률’ 제3조의2와 제9조에서는 정보가 안전하게 관리·유통될 수 있도록 내부통제, 이용자 접근통제, 정보이용 실태에 대한 상시 모니터링 등 신뢰할 수 있는 행정정보 보호 및 오남용 방지체계를 갖추도록 하고 있지만, 해당 법 규정에서는 구체적인 내용을 확인 할 수 없으며, NEIS 관련 법 규정 또한 정보자원의 오남용을 상시 모니터링 할 수 있는 체계에 대해 언급하고 있지 않다. 그 의미는 정보자원을 관리하는 정부기관 스스로 엄격한 자기통제를 해야 함을 나타내는데, 정보자원 효율성의 가치를 더 우선시 하고 있는 현 상황에서는 정보자원의 오남용과 관련한 갈등이 다시 나타날 수 있다는 것을 의미하기도 한다.

⑤ 폐기

정보사회에서 특히 위험한 요소는 한번 입력된 정보가 자동으로 지워

지지 않는다는 사실에 있다. 현재 우리나라는 정보주체의 요청이 있지 않는 한, 정보자원에 대한 폐기에 대해 적극적이지 않은 편이다. 따라서 정보자원의 폐기가 제대로 이루어져 정보주체의 정보인권을 확보하기 위해서는 정보주체의 자기정보 접근을 통한 정보주체에게는 정보열람 및 정보갱신청구권이 인정되어야 한다.

이것은 타인에 의해 처리되고 있는 개인정보의 내용에 대해 정보주체가 이를 열람하여, 그 정확성과 최신성 및 충실성을 유지하도록 요구할 수 있는 권리이다. 개인의 일거수일투족에 관한 상세한 정보가 쉽고 값싼 비용으로 무한대로 저장 · 처리될 수 있다. 이처럼 지속적으로 정보자원이 공유되어 실존인격에 영향을 미칠 수 있는 가능성을 차단하기 위해서는 이 같은 정보열람청구권과 정보갱신청구권이 확실하게 보장되어야 한다.

정보주체의 정보열람과 관련하여 NEIS 관련 법 규범에는 '교육정보시스템 운영 등에 관한 규칙'에 전산자료 열람 및 제공과 관련하여 개인정보열람청구권을 명시적으로 인정하고 있다(국가인권위원회, 2009). 하지만, 인천 소재 고등학교에 재학 중인 학생이 NEIS에 집적된 재학생 본인의 정보를 열람할 수 없게 한 것은 개인정보자기결정권을 침해한 것이라며 2008년 1월 국가인권위원회에 진정을 사례가 있었다.

'교육정보시스템 운영 등에 관한 규칙' 제9조 제1항에 '정보시스템을 활용하는 학교에 재학 중인 학생 또는 학생의 부모 등 법정대리인은 정보시스템에 접속하여 당해 학생의 전산자료를 열람' 할 수 있고, 같은 규칙 제9조 제2항은 제1항의 규정에 의하여 '전산자료의 열람을 신청한 자가 본인 또는 정당한 법정대리인인지 여부를 확인한 후 학교의 장은 당해 학생의 전산자료에 대한 열람을 승인해야 한다'고 규정하고 있음에도 불구하고 (현)교육과학기술부는 NEIS에 수집된 본인 정보를 담임 선생님 또는 학부모를 통해서만 열람하도록 하였다. 이에 시민단체에서는 해당 건에 대해 크게 반발하였다. 하지만 교육부는 '학부모 서비스'를 통해 제공되는 정보의 대부분은 재학생이 학교생활을 통해 이미 알고 있는 것이기 때문에 정보주체임에도 불구하고 재학생의 정보열람을 제한했으며,

재학생의 열람서비스를 시행하기 위해서는 시스템 용량 증대 및 예산확보 등이 소요되어 NEIS 중장기 발전계획 수립에 포함시키겠다는 입장을 밝힌바 있다.

결과적으로 해당 건은 국가인권위원회의 인권침해 결정으로 재학생의 개인정보 자기결정권을 침해하는 사례가 발생하기 않도록 각급 학교에 시달할 것을 권고하면서 마무리 되었다. 하지만, 여전히 재학 중인 학생이 NEIS에 직접 접속하여 자신에 관한 정보를 열람할 수 있는 방법은 마련되어 있지 않다. '개인정보보호법', '공공기관 개인정보보호 기본지침' 등에서는 정보주체의 정보 삭제 청구가 있을 시에 해당 정보를 폐기하도록 명시되어 있다. 하지만, NEIS와 관련하여서는 정보주체인 재학생이 삭제할 정보가 존재하는지 여부조차 직접 확인할 수 없도록 관리되고 있다는 점에서 갈등의 소지가 남아 있다.

정보주체의 열람과 관련한 이슈 이외에도 NEIS CD와 같이 정부가 제3자에게 정보를 제공할 경우, 이것이 사용 후에 적절히 폐기되었는지에 대해 확인할 방법이 나타나고 있지 않다. 정보자원을 제3자가 사용한 이후에 폐기해야 한다는 의무가 제시되고 있지 않아서 정보 보유기관에서 정보를 폐기했다고 하더라도, 여전히 제3자에 의해 정보자원은 공유되거나 사용되고 있을 가능성이 있다. 이에 대한 법규정이나 보다 엄격한 관리기재에 대해 시민단체에서는 요구하였지만, 명확한 관리상의 대응이 나타나지 않고 있다는 점에서 갈등이 발생하였다.

(6) 소결론

통합DB구축을 통한 정보자원의 효율적 관리를 목적으로 하는 정부기관의 인권적 관리 측면을 중시하지 않는 경향이 나타나고 있다. 각 개인으로부터 수집되고 활용되는 정보는 자원으로써의 기능과 더불어 정보주체자의 삶의 흔적이 녹아들어가 있다. 따라서 이를 수집하고 공유하고 활용하는 과정에서 정보주체자의 삶이 타인에게 공개되어 예상치 못한 불이

익을 얻거나 프라이버시를 훼손당할 수 있다. 특히 NEIS 운영의 경우는 시스템을 구축하고 정보를 통합하는 것에 초점이 모아져서 명확한 관련 규정이 부족하다. 특히 정보를 공유하고 사용하는 단계에서는 교육관련 법규정에 대한 자의적 적용으로 인해 오남용이 발생한 우려가 매우 크다.

각 생애주기 별로, 먼저 수집 및 생성 부분에서는 정보제공에 대한 동의 없이 정보를 수집하거나 정보수집과 관련한 명확한 법적 근거 없이 정보수집행위를 우선시 한 부분 등의 이슈가 도출되었다. 정보의 저장 측면에서는 정보의 집적화에 따른 대규모 정보유출에 대한 우려와 관련한 이슈가 나타났으며, 공유 및 분배에 있어서는 목적외의 정보공유에 대한 부분과 정보주체가 자신의 정보가 공유되었는지 확인할 수 없는 알권리 행사의 어려움이 문제시 되고 있다.

정보의 사용에서는 정보사용의 명확한 규정이 없음에 따라 정부가 자의적 판단에 따라 정보자원을 사용할 가능성이 있다는 점, 폐기에서는 정보주체가 자신의 정보폐기 여부를 확인하기 어렵다는 점과 정보사용 후의 폐기 여부를 확인할 방법이 뚜렷하지 않다는 점에서 갈등을 불러일으키고 있다.

새로운 기술이 등장으로 기술적으로 진보된 정보자원의 활용과 관리가 용이해 졌다. 하지만, 기술의 혁신에 따른 체계적인 법규정이 존재하지 않게 되면 안정된 정보사회의 정착이 어려운 측면이 있다. NEIS 도입으로 교육행정과 관련한 정보자원의 효율적 관리와 국민의 정보접근성이 높아진 측면이 있다. 하지만 그 이면에 정보자원에 대한 인권적 관리가 부족하게 되면서 진보된 기술을 제대로 활용하지 못하는 경우가 발생 할 수 있다.

NEIS는 교육 및 공공기관 정보관리와 관련한 법규정을 적용하면서 도입되었지만, NEIS의 활용과 관련한 직접적인 법규정이 미비하여 정부기관의 재량이 지나치게 발생할 수 있어 여러 가지 갈등상황을 야기하게 되었다. 따라서 정보인권과 관련한 규정의 명확화는 효과적인 NEIS 활용을 위해 매우 중요한 부분으로 여겨진다.

NEIS로 인해 발생한 갈등은 통합DB의 기술적 이점을 통한 정부 정보자원 관리의 효율성을 높이고자 하는 정부의 가치와 해당 교육 정보의 주

체인 학생 및 학부모 등 국민들이 가지는 자기정보통제권 간의 충돌에 의해 나타나게 되었다. 교육부의 인식프레임은 효율성의 강조로 나타났다. NEIS의 도입으로 학부모에 대한 알권리를 충족시키며, 민원처리절차의 간소화, 교원의 업무 경감 등 전반적인 교육행정의 생산성이 향상(나태준, 2006) 될 것이라는 기대로 인해 해당 사업을 추진한 것이다.

하지만, 전교조로 대표되는 NEIS 반대 관련 시민단체들은 NEIS라는 대규모DB가 가지는 정보인권에 대한 문제를 중요한 이슈로 생각하고 있었다. 상당수의 국가DB구축과정에서 이러한 인식이 차이가 계속 발생하게 되는데, 국가DB의 필요는 국민들의 수요에 따른 요구라기보다는 정보자원을 관리하는 정부의 입장에서 시작되었기 때문이다. 정보화 사회로의 진입이후, 정부입장에서의 정보자원은 효과적으로 활용해야 하는 자원의 성격으로 인지를 하게 되었고 해당 정보자원을 관리하고 활용하는데 있어 새로운 기술의 도입을 통해 보다 효율적이고 간편하게 자원을 관리하고자 하는 욕구를 가지고 있다.

따라서 정부가 주도하는 통합DB 구축은 효율적 관리라는 정부의 주요 관심사를 대변할 수밖에 없게 된다. 또한 주민등록번호 등 그간 우리나라 정부는 국민에 대한 정보를 다수 가지고 있었으며, 필요한 경우에는 임의로 수집하면 되었음에도 불구하고 이를 위해 국민에게 동의를 구하는 과정을 거친 경우가 없다.

그리고 우리나라에서는 과거 국가가 개인에 대한 정보를 과도하게 수집하고 있기 때문에 정보인권에 대한 국민의 권리의식이 상당히 미흡한 편이었다. 이러한 상황 속에서 정보의 수집, 사용, 공유 등에 있어 국민의 자기정보통제권은 크게 인정받지 못하게 되었다. 하지만, 인권에 대한 관심이 높아지고 정보통신기술의 발달로 시민들의 참여가 증가하고 개인정보의 중요성이 강조되면서 정부의 정보자원관리에 있어 정보인권 측면을 고려할 필요에 대해 요구하기 시작했고, 정보인권에 대한 국민들이 인식이 높아지면서 효율성이라는 가치를 중심으로 두었던 정부와 NEIS 사례를 계기로 갈등이 가져오게 된 것이다.

〈표 6-2〉 NEIS의 정보자원 생애주기에 따른 이슈

	정보자원생애주기				
	수집/생성	저장	분배/공유	사용	폐기
생애주기별 인권적 이슈	▪ 정보 주체의 동의 없이 개인정보를 집적 ▪ 자기정보 통제권, 선택권 침해 ▪ 정보수집에 대한 명확한 법적 근거 미비	▪ 정보자원 집적에 따른 대규모 유출의 우려 ▪ 정보의 저장 및 보관과 관련하여 보다 엄격한 규정 필요	▪ 목적외 사용의 우려 ▪ 행정상 편의를 위해 공유 ▪ 정보주체의 알권리 행사의 어려움	▪ 관리주체의 자의적 정보사용 ▪ 정보주체의 알권리 행사의 어려움| ▪ 사용과 관련한 명확한 법규정의 미비	▪ 정보주체의 알권리 행사의 어려움 ▪ 폐기 규정의 미비 ▪ 자료의 사용 후 폐기를 확인하기 어려움

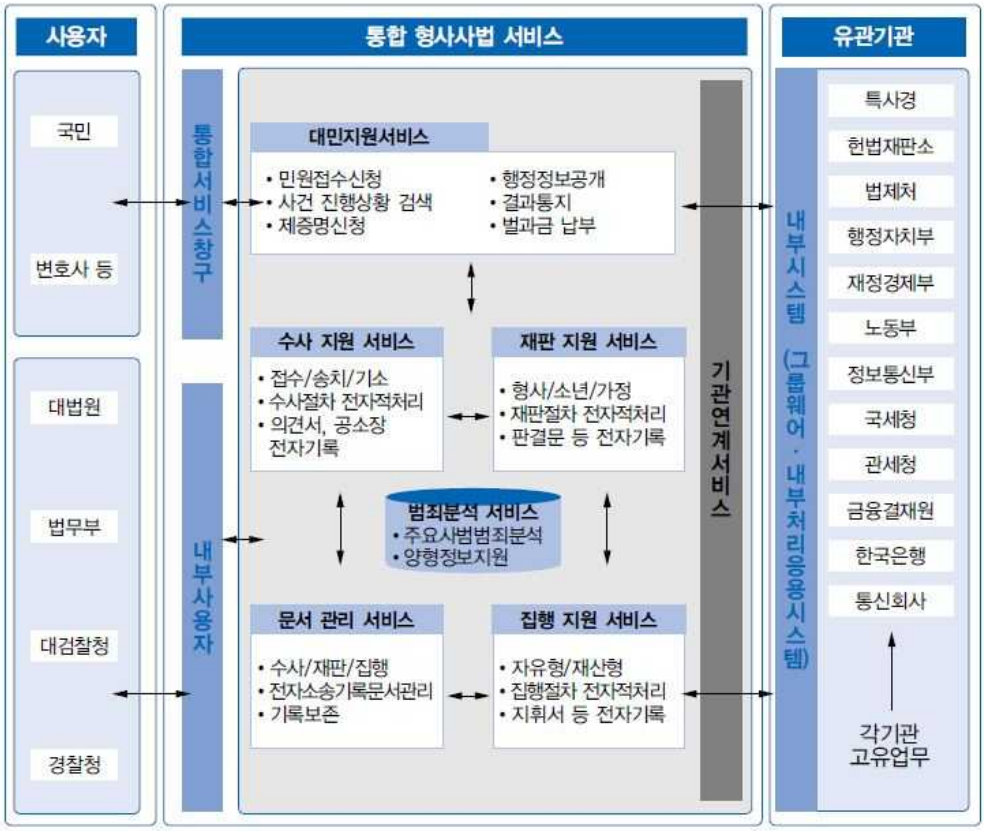
2) 형사사법통합정보체계

(1) 형사사법통합정보체계 사업개요

형사사법통합정보체계(KICS: Korea Information system of Criminal justice Sercices, 이하 KICS)[29]는 "신속 · 공정 · 투명한 형사사법절차를 실현하기 위하여 형사사건의 접수 · 수사 · 결정 · 재판 · 형집행 등 형사사법 업무를 표준화 · 전자화하여 처리하고, 형사사법 기관이 전자적 · 체계적으로 관리하고 있는 정보를 공동으로 활용할 수 있는 통합관리 체계(정부혁신지방분권위원회, 2008)"로, 대검찰청, 법원, 법무부, 경찰청 등 형사사법 유관기관 간의 형사사법업무 절차를 표준화하고 전자화 하여 기관 간 정보공동 활용체계를 구축한 DB이다. KICS의 목적은 업무 효율성과 정확성, 신속한 정보공개 및 민원처리를 위한 것으로, KICS는 지난 참여정부의 전자정부 31개 과제 중 하나로, '전자적 업무처리 정착'이라는 의제의 하부 과제로 진행되었다. 참여 정부는 범정부적으로 추진하는 '일하는 방식 혁신'과 '정보자원 공동활용' 등 전자정부 혁신사업의 방향성을 반영하도록 하였으며, 전자문서 유통 · 결제 등 공통서비스의 정보자원은 공동 활용하도록 하고 기관의 업무처리시스템은 서비스별(수사, 재판, 집행 등)로 나누어 구축하도록 하였다(정부혁신지방분권위원회, 2008).

29) 형사사법절차전자화촉진법(2010.01.25. 제정)에 근거하여 운영되고 있다.

<그림 6-3> KICS 시스템 개념도



자료: 정부혁신지방분권위원회(2005)

(2) 추진배경

KICS는 모든 형사사법업무가 하나의 네트워크에서 처리 될 수 있는 전자화 된 통합형사사법체계를 구축해야 할 필요성에 의해 제기되었다. 기존에 형사사법업무는 각 기관별로 정보화 사업이 별도로 진행되어 온 결과, 서로 상이한 정보화 환경이 구축되어 있어서(백승민, 2007), 수사 및 사건송치(경찰청, 노동부, 관세청, 국세청, 국정원 등), 수사 및 결정(검찰), 공판(법원), 집행(법무부) 등에서 상호 연계성 없이 각 기관별로 형사사법업무를 지원하는 시스템이 구축 · 관리되고 있어 동일 정보의 중복 입력

등 인력 및 비용의 낭비가 많으며 국민들이 각 기관을 개별 방문해야 하는 불편을 초래할 우려가 있는 상황이었다. 첫째, 정보환경의 변화로 수사 및 공판 단계에서 형사사법 관련 음성 · 화상 등 형사사건 정보의 디지털화 및 관리요구가 증가하고, 둘째, 인터넷 생활화를 통한 국민의 형사사법절차 참여활동 영역이 확대되면서 형사절차의 신속 · 공정 · 투명성 및 인권에 대한 국민의식이 변화하고 있는 측면, 셋째, 생산자인 정부기관 중심에서 소비자인 국민중심으로 패러다임이 변화하고, 형사사법에서 국민을 고객으로 여기는 인식의 전환이 필요, 넷째, 각 기관의 정보화 사업에도 불구하고 기관 간 업무처리는 종이문서 중심으로 처리되고 기관 중심의 정보관리 체계로 정보공유가 미비하다는 점, 마지막으로, 전자적 업무처리 정착을 통한 형사사법 업무방식의 혁신을 추가하여 전자정부 구현을 위한 주요 기반을 확보해야 한다는 환경적 필요에 의해 KICS를 추진하게 되었다.

이에 따라 KICS는 첫째, 수작업 업무처리는 최소화하고 전자적 사건처리로 프로세스를 최적 · 간소화하여 수작업 업무처리를 최소화하고, 형사사법기관 간 자료교환을 원활하게 하여 신속 · 정확한 업무처리가 이루어지도록 e-형사절차 도입을 통한 업무 효율성을 제고에 있다. 둘째로는 유관기관 간 긴밀한 협조체제로 수사경쟁력을 강화할 필요성과 정보화 사업의 한계성, 정보 및 프로세스의 표준화를 통한 공정하고 신속한 사건처리를 위한 정보공동이용 체계를 구축할 필요성을 목적으로 하고 있으며, 마지막으로 형사사건 진행절차, 형사사법 정보에 대한 접근 · 보안을 강화하고 국민의 권리보호 및 참여 확대 및 형사사법 분야에 One-Stop 민원서비스체제의 필요를 충족하여 사건 처리절차의 투명성 확보 및 민원서비스의 질적 향상을 도모를 목적으로 사업이 추진되었다.

(3) 추진경과

형사사법통합망과 관련한 사업추진은 1990년대부터 경찰, 검찰, 법원

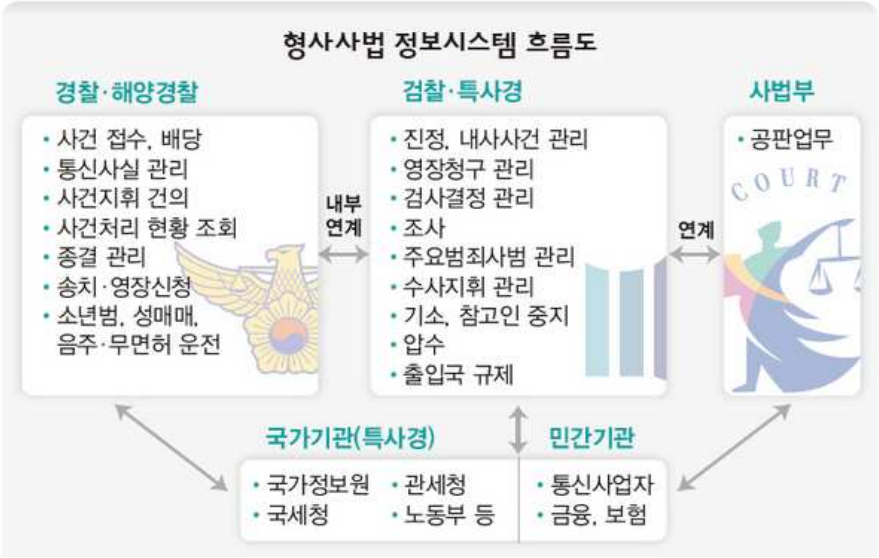
등 각 기관별 전산화에서부터 시작되었으며, 지난 1995년에 법무부 주관으로, 법원과 검찰의 두 기관 사이에서 각각 가지고 있는 형사사건 전산자료를 공동활용하는 차원에서 시작되었다. 1996년 '사법기관 간 형사 DB 공용망 구축' 계획에 따라 법무부 보호국이 참여하면서 확대되었고, 1997년 형사사법정보화추진분과위원회가 설치되면서 경찰과의 연계를 통해 재판결과에 이르는 일련의 형사사건 처리절차의 단계 속에서 각종 자료의 공유를 확대하고자 진행되었다. 1999년 ' 형사사법기관 간 범죄수사정보 공동활용체계 구축' 계획이 추진되면서 형사사법기관 전체에 결치는 형사사법통합망 구축이 진행되었다.

2002년 1월에는 '형사사법망범죄정보검색시스템'을 개통하여, 피의자원표 등의 정보를 제공하거나, 출입국 사실/재출소자 현황 등의 조회에 이용되도록 하였고, 2004년 12월에는 통합형사사법체계구축기획단규정(대통령훈련 135호) 공포하여 KICS 구축을 본격적으로 시작하였다. 본 사업은 2005년 12월부터 2009년까지 마스터플랜 작성(2005. 1~7), 경찰, 검찰, 법원, 법무부 전자형사절차 기반 구축(2005. 8~2006. 11), 대국민 형사사법서비스 통합민원창구 구축 및 관세청, 국세청 등 기타 기관과 연계(2006. 12~2007. 12), 네트워크 고도화와 안정화 추진(2008~) 등 4단계로 사업이 진행되며, 2007년 12월까지 연계기관을 국세청, 노동청, 관세청 등 특별사법경찰관서까지 확대하고 대국민 형사사법서비스 제공을 위한 인터넷상의 통합민원창구를 구축하도록 하였다. 총 4단계에 걸쳐 사업을 진행하였고, 2010년 7월에 형사사법공통시스템 구축 완료하고 동년 8월에 형사사법공통시스템 운영단(법무부 기획조정실) 출범하여 운영 중에 있다.

<표 6-3> 단계별 사업 추진 내용

단 계	추 진 내 용
2004년도 사업 (BPR/ISP)	- 기관 간 전자적 업무수행 방안 도출 - 업무 프로세스 개선 과제 도출(18개 과제) - 통합 서비스 제공을 위한 표준체계 수립 - 대국민 서비스 구축 방안 도출 등
2005년도 사업 (제1차 사업)	- 사건수사시스템 구축 - 수사결정 중 수리·배당업무 기능 개발
2006년도 사업 (제2차 사업)	- 수사결정시스템 구축 - 재판지원서비스(형사 공판·약식, 영장, 재판사무공통 등) 구축 - 집행지원서비스(재산형시스템) 구축 - 대국민 서비스 개발
2007년도 사업 (제3차 사업)	- 음주·무면허 운전사건 등 전자약식 시스템 구축 - 사건수사시스템 분리를 위한 KICS 재구성 - 법무부 집행지원시스템(수용관리,보호관찰,소년보호 등) 구축 - 법원 가정/성매매, 소년보호시스템 구축 - 대국민 서비스 포털 인프라 구축 - 법률 제·개정 사항 반영 (재정신청 대상 확대, 압수수색 영장제도 변경, 배심원 제도 도입, 강제집행 절차 변경 및, 신규 서식 30여종 추가 등)
2008년도 사업 (제4차 사업)	- 집행지원서비스(수용관리·보호관찰·소년보호·감호치료 등) 관련 인프라 도입, 공통 서비스 및 대국민 인프라 확충 - 사용자 서비스를 위한 네트워크 및 백업체계 구축

<그림 6-4> 형사사법 정보시스템 흐름도



(4) 정보자원 생애주기에 따른 분석

① 수집 및 생성

KICS의 구축과 관련한 수집 및 생성 단계에서는 형사사법과 관련한 정보수집은 정보수집자와 정보제공자가 상호 대등한 관계가 전제될 수 없다는 점에서 출발부터 문제가 발생하게 된다. 피의자 등에게 진술거부권 등의 방어권이 보장되기는 하지만, 수사라는 특성상 대등성을 전제하기가 곤란하며, 이런 불평등은 결국 정보주체의 의사를 배제하는 결과로 나타날 수 있다. 개인의 인격권, 프라이버시권, 사상과 양심의 자유를 침해하는 각종 정보를 수사기관이 수집 · 저장 · 공동 활용함으로써 정보자원을 수집하는 행위과정에서 국민 개인의 인권적 가치를 훼손할 가능성이 높을 것이다. 형사사법관련 개인정보의 생성은 범죄수사 및 범죄수사 지원 기능에 종사하는 공무원에 의해 이루어진다. 그리고 고소 · 고발 · 이송 사건은 접수 즉시 입력하고 인지 · 발생 · 검거사건은 수사팀 인계 즉시 입력하

고 모든 사건의 종결내용은 기록 송치 이전에 입력하도록 되어 있다. 그런데 KICS에 있는 정보는 피의자를 상대로 받은 신문조서 뿐 아니라 피해자와 참고인에게서 받은 진술조서나 수사보고서, 의견서 등도 모두 포함되어 있다. 수사보고서와 각종 조서는 수사과정에서 얻은 정보를 자의적으로 기록해 남긴 것으로(국가인권위원회, 2009), 사실인 내용과 주관적 판단이 포함된 내용이 섞여 있다. 객관적인 사실 뿐 아니라 해당 사건을 담당한 공무집행자의 주관적 판단이 정보자원으로 수집 및 생성되어 타 기관과 공유할 가능성이 높은 것이다.

정보가 자원으로서 관리되면 그것을 가공하여 새로운 정보의 생성이 가능해 진다(김성태, 2007). 형사사법과 관련한 정보의 경우는 수사보고서와 각종 조서와 같은 주관적 판단이 개입된 문서들이 정보로서 수집되고 생성되면서 이를 공유 및 활용하는 타인으로 하여금 이에 영향을 받도록 하고 있는 것이다. 자의성이 개입된 정보는 다른 수사관이나 공무원으로 하여금 선입견을 심어주거나 예단을 발생시킬 수 있어 해당 정보의 주체 또는 관련자들의 인권을 무시하거나 침해 할 가능성을 높이게 된다. 따라서 형사사법 정보 수집과정에서 수사자의 주관성이 개입되지 않도록 하는 장치 혹은 자의성이 개입되지 않는 정보만을 수집해야 할 것이다.

정보수집의 명확한 목적과 법적 근거에 있어서도 인권적 관리의 문제가 있다. KICS의 구축은 정보자원을 활용하고자 하는 효율성 측면이 중시하기 때문에 정보주체의 권리에 대한 배려는 충분하지 않은 경우가 많다. 정보주체에게 민감할 수 있는 정보에 대한 통합 및 공유에 있어 정보주체가 선별적으로 정보를 제공할 수 있도록 하는 법적 근거 등이 마련되어 있지 않은 경우가 그것인데, ‘공공기관의 개인정보보호에 관한 법률’에서는 정보의 수집 및 보유와 관련하여, 사상 · 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하는 것이 금지하고 있는데 형사사법과 관련한 대다수의 개인 정보가 개인의 기본적 인권을 현저히 침해 할 우려가 있는 민감한 정보이다. 하지만 ‘형사사법 통합정보체계 추진단 규정’ 등 만이 해당 사례와 직접 관련된 법적근거로, 정보

수집이나 활동들과 관련한 세부적이고 구체적인 법적 근거 마련이 되어 있지 않은 상황이다.

정보수집에 있어 또 다른 인권적 문제는 정보주체의 동의가 올바로 이루어 졌느냐 하는 것이다. 새로 수집하는 정보에 대해서는 '공공기관의 개인정보보호에 관한 법률'이나 '개인정보보호법' 등에서 규정하는 바와 같이 수집단계에서 정보주체의 동의를 받게 되겠지만, 기존에 수집된 형사사법과 관련한 개인의 정보의 경우에는 정보통합과 관련하여 정보주체의 동의를 사전에 구하지 않은 상황에서 수집된 것이 대부분이기 때문에 각 형사사법 관련 기관의 정보들을 수집하여 통합화하는 것은 정보주체의 동의를 구하지 않았다는 측면이 강하다.

정보주체의 선택권 측면에서, 통합화과정에서 각 형사사법기관이 가지고 있는 개인의 주민등록번호, 주소 등을 포함한 기본적 개인정보를 비롯하여 차적, 건강상태, 피의자의 가족관계나 인적 사항, 이성 관계, 재산, 병역, 종교, 가입 단체 등 가운데 국민이 공개를 원치 않은 정도를 선택할 수 있는 권한을 부여하지 않은 것이 대부분이며, 정보주체가 원할 경우에만 정보의 삭제와 수정이 가능하도록 하고 있어서 정보자원의 관리라는 측면에서 정보주체의 권한과 인권 보호에 대한 적극적인 조치는 이루어지지 않고 있다.

현실적으로, 그동안 축적한 상당한 정도의 개인정보에 대해 해당 정보주체에게 어떠한 정보수집에 동의하는지에 관한 선택여부 등을 재차 묻는 것은 거의 불가능한 일이고 실제 이루어지더라도 상당한 비용과 시간이 소요될 것이므로 정보화에 따른 전산화 이전에 수집한 자료에 대한 동의를 구하는 건 어려운 일이며 효율적이지도 않은 것이다. 따라서 이러한 선택권을 부여하지 않은 채 정보통합의 효율성에 초점을 두고 통합화를 시작하는 자체에서부터 정보수집과 생성과 관련한 정보주체의 선택권을 부여되지 않고 있는 것으로 판단될 수 있을 것이다.

② 보관 및 저장

KICS와 같이 통합DB를 대규모로 구축하고 자료를 집적시킬 경우, 기관 내부자 혹은 외부 침투자들에 의해 개인정보가 언제라도 유출될 가능성이 높으며, 일단 정보유출이 발생하면 그 피해 정도는 상당한 수준에 이르게 될 것이다. 공공기관 개인정보보호 기본지침에 '기술 및 시스템적 보호장치 강화' 등에 저장과 관련한 내용이 있으며, 전산 및 네트워크, 서버 관리 등에 있어서는 지침이 존재하고 해당 부분에 대한 경각심이 높아져서 지속적으로 개선되고 있으나 공공기관 종사자 개인 수준에서의 보안관리는 취약한 편이다. 실제로, 2005년 이후 사이에 기관내부자에 의한 형사사법정보 오남용에 대한 사례는 계속적으로 지고 있으며, 이러한 사례들은 언론을 통해 지속적으로 언급되고 있다. 일단 수집된 정보자원은 외부에 유출되면 정보주체자의 인권을 침해하는 문제를 발생시키므로 안전한 저장이 최우선되어야 한다. 이는 기술적 측면에서의 외부공격을 방어하는 기재를 구축하는 부분과 더불어 해당 정보에 접근하게 되는 개별 구성원의 행태에 대한 관리가 수반되어야 한다.

하지만, 지인의 부탁이나 개인적 이유에 의해 형사사법 관련 정보를 유출하는 사례가 지속적으로 발생하고 있다는 것은 형사사법관련 정보를 관리 · 활용하는 공무원들에 대한 감시 · 감독이 제대로 이루어지지 않고 있음을 의미하는 것이다. 현재 내부자의 정보유출에 대한 엄격한 규정의 제시와 처벌이 이루어지지 않게 되면서 한 두 명이 아닌 다수의 내부자가 정보유출을 시도할 수 있는 가능성이 존재 한다. 이는 한 번의 외부공격보다 더 많은 정보유출 사례를 만들 수 있는 심각한 문제이다. 따라서 형사사법관련 정보의 저장 및 보관과 관련하여 보다 엄격한 규정이 있어야 한다. 최근 DDoS 공격이나 농협전산망해킹 사례 등 일련의 전자보안침투 사례가 지속적으로 나타나는 전산망을 공격하는 사례도 점차 증가하고 있는 추세이다. 이는 완벽한 전산 보안을 보장하기 어려운 상황에서 외부로의 정보유출의 가능성을 상존할 수 있다는 것이기 때문에 형사사법관련 정보의 안전한 관리를 위해 조직적, 기술적 조치에 대한 의무를 강화해야 하는 것이다.

저장과 관련한 내외부적인 안전관리 이외에도 형사사법 정보 관련 관리체계에 대한 문제점을 시민단체에서는 지적하며 개선을 주장하고 있다. 현재 '공공기관의 개인정보보호에 관한법률'에서는 공공기관의 장은 개인정보를 처리함에 있어서 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 강구하도록 하고 있다. 그리고 공공기관의 장이 개인정보파일을 보유(변경 · 폐지 포함)하고자 하는 경우에는 중앙행정기관의 장은 소정의 사항을 행정안전부장관에게 통보하고, 기타 공공기관의 장은 관계중앙행정기관의 장에게 통보하여야 하며, 통보를 받은 관계중앙행정기관의 장은 이를 종합하여 행정안전부장관에게 제출하여야 함을 규정하고 있다. 하지만, 형사사법정보의 경우는 행정안전부 소속 기관이 아닌 기관이 관여되어 있기 때문에 해당법률로는 사후감독과 시정조치를 효과적으로 할 수 없다. 혹시 발생할 수 있는 시스템에 대한 개인의 권익침해를 감소시키기 위해서는 형사사법 정보의 안전성 확보와 관련한 별도의 규정을 마련하거나 현재의 법제도를 수정할 필요가 있다.

③ 분배 및 공유

정보의 공유와 관련하여, 정보가 공유될 경우에는 해당 정보가 어떠한 이유에서 누구에게 공유되었으며, 공유 후에 해당 정보에 대한 폐기 여부 등에 대해 기록해야 한다. 그리고 해당 정보와 관련하여 정보주체의 동의가 필요하다. 하지만, 해당 통합망은 형사사법과 관련한 것으로 신속한 범죄해결을 위해 빠른 정보의 활용을 목적으로 하고 있어서 형사사법 사안의 해결을 위해 정보주체의 동의를 일일이 구할 경우, 신속한 범죄해결을 어려울 수 있다. 이러한 이유에서 정보주체의 동의 없이 필요한 정보를 여러 기관에서 공유할 가능성이 높다. 이는 다른 분야의 정보자원 공유와 유사한 것으로 동의 없는 정보자원의 공유는 정보인권 침해라는 결과를 가져오게 된다.

통합데이터베이스는 태생적으로 여러 기관이 자료를 수집 및 통합하고 이를 활용하기 때문에 다양한 목적을 위해 정보를 활용할 가능성 또한 높다. 특히 KICS는 범죄의 수사와 공소의 제기 등에 대한 내용이 대부분이다. 해당 정보들은 활용에 따라 개인의 인권을 직접적으로 침해할 수 있는 것들로, 목적 외 이용 금지가 엄격히 이루어져야 한다. '공공기관의 개인정보보호에 관한 법률' 이나 개인정보보호와 관련한 각종 법률에는 목적 외 사용에 대한 규정이 존재하지만 처리정보의 이용 및 제공의 제한과 관련하여 예외규정을 두고 있는데, 이 중 하나가 범죄의 수사와 공소의 제기 및 유지에 필요한 경우이다. 형사사법과 관련한 정보를 대다수가 이에 해당하며, 관련 기관들을 해당정보를 이러한 목적에 의해 활용하는 것이다. 시민단체 에서는 정보공유 및 활용 등과 관련하여 개인정보 활용에 따른 인권적 침해가 이루어질 가능성을 열어 놓은 것이나 다름 없다는 주장을 하면서 별도의 법적인 근거조치가 필요하다는 주장을 하고 있다. 현재 '공공기관의 개인정보보호에 관한 법률' 의 제3조의2와 제9조에서 정한 바와 같이 공동 이용하는 정보가 안전하게 관리 · 유통될 수 있도록 내부통제, 이용자 접근통제, 정보이용 실태에 대한 상시 모니터링 등 신뢰할 수 있는 행정정보 보호 및 오·남용 방지체계를 갖추도록 되어 있다. 하지만 구체적인 내용에 대한 언급은 확인되지 않고 있어서 처리정보의 이용 및 제공의 제한과 관련한 예외규정에 해당 할 수 있는 형사사법과 관련한 정보자원의 공유가 폭넓게 이루어질 가능성이 높다[30]. 정보의 공유는 목적에 따라서 이루어져야 하며, 그렇지 않은 경우는 정보주체자의 정보인권을 침해하는 것이다. 따라서 해당 규정에 대한 강화와 예외규정에 대한 보다 상세한 언급 등 엄격한 법적용이 가능하도록 관리되어야 한다. 그렇지 않을 경우, 이에 대한 시민단체와의 갈등은 지속화 될 것이며 정보인권이라는 측면에서의 정부의 관리는 효과적으로 이루어지고 있다고 보기 어렵게 된다.

30) 행정안전부 개인정보보호지침과 개인정보파일 관리지침에 공유과정에 대한 내용이 간략하지만 나타나고 있다. 하지만, 공유 과정에서 작성되어야 할 문서나 관리대장을 지침대로 운영하지 않은 경우도 있다.

④ 사용

통합데이터베이스의 특성상 다양한 기관에서 정보를 열람하고 제공을 요청하게 된다. 이 과정에서 사법기관의 특성상 신속적 정보와 다양한 성격의 정보를 통해 범죄를 해결하고자 하는 경향이 있기 때문에 일련의 범죄와 관련한 다양한 기관관계자들에게 정보를 활용될 가능성이 높다. 하지만, '공공기관의 개인정보보호에 관한 법률'의 제6호에서 '범죄의 수사와 공소의 제기 및 유지에 필요한 경우', 제7호에 '법원의 재판업무수행을 위하여 필요한 경우'로 개인정보파일의 보유목적외의 사용을 폭넓게 인정하고 있는데, 이러한 예외사유는 너무 포괄적이기도 하고 형사사법정보는 대부분이 위의 예외 경우에 해당되지 때문에 정보 활용의 오남용과 목적 외 사용금지를 막기 어렵게 된다. 형사사법정보의 사용은 엄격한 법의 테두리 내에서 이루어져야 한다. 그 이유는 피의자의 주민번호, 주소, 가족관계, 인적사항, 이성 관계, 종교 등 뿐 아니라 피해자의 인적 사항과 피해내역이나 금전 거래 내역까지 담고 있는 것이 형사사법정보이기 때문이다. 이러한 정보들의 사용에 대한 감시·감독이 엄격히 이루어져야 하는 이유이다. 법적인 예외 뿐 아니라 광범위한 정보의 축적으로 인해 기관내부자가 개인적인 요청에 의해 정보를 열람하고 이를 타인에게 제공할 경우도 충분히 있을 가능성이 있으며, 금품을 받고 제3자에게 정보를 제공하는 사례가 언론보도를 통해 종종 나타나고 있다. 따라서 형사사법에 대한 제3자 제공규제를 보다 엄격히 해야 한다. 외국의 형사정보공용시스템의 경우는 제한적 업무에 필요한 범위 내에서만 서로 연계하여 정보를 공동 활용하는 방식을 채택하고 있는데, 이러한 부분을 벤치마킹할 필요가 있다.

정보이용이 어떠한 목적으로, 누구에 의해 되었는지에 대해 알려야 하는 의무규정이 있지 않으며, 각종 개인정보보호와 관련한 법률에서는 형사사법과 관련한 내용은 예외규정으로 두고 있어서 정보주체의 알권리가 폭넓게 보장되어 있지 않고 있다. 실제 2009년 진보네트워크센터에서 개

인정보에 대한 열람 청구 시 정보의 타 기관 제공(조회) 현황에 대한 열람청구 요청에 대해 해당 정보를 관리하는 경찰관서를 직접 방문하여 열람하도록 하고 있는데, 이는 정보주체의 알권리를 적극적으로 행사할 수 있게 하고 있다고 보기는 어렵다. 정보주체는 자신의 개인정보에 대한 조회와 제공 현황을 언제든지 직접 확인하고 그에 따른 권리 행사를 할 수 있어야 하는데, 해당 정보의 주체자임에도 불구하고 직접 관서로 찾아가서 확인을 해야 하는 불편을 감수해야만 자신의 권리를 행사할 수 있다. 정보보유 기관의 정보자원에 관한 정보주체의 알권리 확보에 소극적이라면, 이는 정보주체의 권리를 일정부분 침해하는 것으로 해석이 가능하므로 이에 대한 관리적 차원의 개선이 필요하다.

⑤ 폐기

통합망의 존재는 여러 기관의 수많은 관계자가 정보를 공유하고 이를 활용하기 때문에 활용된 자료가 목적을 위한 사용 이후에 폐기되었는지 알 수 있는 방법이 현재는 없다. 형자전자화법안에서는 시스템의 설치와 운용에 관한 대략적인 부분만을 언급하고 있기 때문에 실제 형사사법정보의 이용과 유통에 대한 실질적 내용이 부족하다. 정보자원의 폐기와 관련한 규정은 개인정보보호법, 공공기관 개인정보보호 기본지침 등에 명시되어 있다. 원칙적으로 개인정보파일의 보유목적 달성 등 해당 개인정보파일의 보유가 불필요하게 된 경우 해당 개인정보파일을 지체 없이 파기해야 한다. 하지만, 정보주체의 삭제 청구가 있더라도 다른 법률에 따라 보유해야 하는 경우에 있어 개인정보항목에 대한 삭제를 기관에서 거부할 수 있도록 하고 있다. 상당수의 공공기관들은 수집한 자료를 자신들의 자산이라 여기는 경우가 많아 폐기하지 않은 경우가 많은데, 특히 사법기관의 경우는 기존의 수사 자료를 통해 새로운 수사에 활용하는 경우가 많아 정보자원을 폐기하지 않으려 하지 않는다. 그리고 KICS에 작성되는 수사서류는 전자결재기능이 있어서 결재된 서류는 수정 및 삭제불가하게 되기

때문에 형사사법정보자원의 폐기는 쉽게 이루어지지 않는다. 그리고 피의자가 검찰에서 무혐의로 불기소 처분을 받거나 법원에서 무죄 판결을 받았더라도 경찰에서 조사받은 내용은 무기한 저장되고 있다. 그리고 국회 행정안전위원회 소속 한나라당 박대해 의원이 경찰청에서 제출받은 자료에 따르면 경찰은 형사사법 정보자원의 폐기와 관련하여 “규정이 없어 그동안 개인 정보를 삭제하지 못한 것을 인정한다”고 밝히는 등 2011년 4월말 기준 총 5532만 5068명(중복 포함)의 개인 정보가 고스라니 모여 있다.

정보자원은 정보주체의 인권과 관련한 내용을 담고 있기 때문에 사용목적이 사라지게 되거나 정보주체의 요청이 있을 경우에는 폐기해야 한다. 하지만, 형사사법과 관련한 정보들은 거의 대부분 폐기되지 않아 통합DB에 상존하고 있으며, 이때, 무죄판결이나 기소유해의 경우와 같이 범죄의 사실이 없기 때문에 삭제해야 하는 정보를 삭제하지 않은 상태에서 이를 타 사법기관이 공유·활용하여 특정인에게 적용하여 피의자 신분으로 취급하게 되면, 또 다른 형태의 인권침해가 나타날 가능성이 높다.

(6) 소결론

각 생애주기 별로, 먼저 수집 및 생성 부분에서는 정보수집자와 제공자 간의 관계가 대등하지 않다는 점과 형사사법 기록에 있어 수사자의 주관적 판단이 정보에 개입될 수 있다는 이슈가 특징적으로 나타났다. 정보의 저장 측면에서는 정보에 접근 가능한 내부자의 개인적 이유에서의 정보유출 가능성에 대한 부분이 특징적이며, 공유 및 분배, 사용에 있어서는 형사사법 사안이라는 특징으로 인해 포괄적 예외가 적용된다는 문제가 갈등의 이슈로 나타나고 있다. 폐기에서는 정보주체가 자신의 정보폐기 여부를 확인하기 어렵다는 점과 더불어 규정의 미비로 인해 개인정보가 삭제되지 않고 있고 여러 기관이 걸쳐 있으면서 한 기관의 폐기로 정보가 완전히 폐기되지 않을 가능성으로 인해 갈등을 나타나고 있다.

<표 6-4> KICS의 정보자원 생애주기에 따른 이슈

	정보자원생애주기				
	수집/생성	보관/저장	분배/공유	사용	폐기
생애 주기별 인권적 이슈	▪ 정보수집 과정에서의 대등하지 않은 관계 ▪ 수자기록에 주관적 판단 개입 ▪ 수집에 대한 포괄적 예외 조항 ▪ 기존에 수집된 정보에 대한 정보주체의 선택권 미부여	▪ 공공기관 종사자 개인 수준에서의 취약한 보안관리 ▪ 저장에 대한 포괄적 예외 조항 적용 가능	▪ 정보의 이용 및 제공의 제한과 관련하여 예외규정 ▪ 범죄해결을 이유로 공유에 대한 사전조치 미흡	▪ 목적외의 사용을 폭넓게 인정 ▪ 개인적 이유로 제3자에 정보제공 ▪ 정보주체의 알권리 행사의 어려움	▪ 명확한 폐기규정 없음 ▪ 결재된 서류는 수정 및 삭제불가 ▪ 한 기관의 삭제로 정보가 폐기되지 않을 우려

KICS에는 방대한 양의 개인정보가 누적되어 관리되는 시스템이다. KICS의 정보 중 피해자와 참고인 등 죄 없는 사람들의 정보가 전체 개인정보의 43%에 달해, '죄 없는' 사람들의 개인 정보가 무차별적으로 저장되고 있는 상황이다. 피의자 역시 검찰에서 무혐의로 불기소 처분을 받거나 법원에서 무죄 판결을 받아 '죄 없음'이 증명되더라도 해당 규정이 없거나 시스템 상의 문제로 인해 경찰에서 조사받은 내용은 무기한 저장되고 있다. 결국 어떤 이유에서든 국민이 경찰서 문턱만 넘었다면 개인 정보가 수집돼 영구 보존되고 있는 것이다. 형사사법과 관련한 정보는 개인의 민감한 내용을 포함하고 있으며, 여러 형사사법정보의 조합으로 또 다른 인권적 문제를 야기 할 수 있는 정보이다. 따라서 이를 관리함에 있어

효율성을 측면으로 접근하기 보다는 정보주체자의 권리와 정보인권에 대한 침해를 최소화할 수 있는 관리적 차원의 대안이 필요하다. 하지만, 아직까지 이에 대한 적극적인 조치는 이루어지지 않고 있어서 전 국민의 사생활 정보의 보고가 될 가능성이 있다.

그리고 형사사법이라는 특수성으로 인해 정보자원관리에 있어 예외조항의 적용이 상당히 폭넓게 되어 있는 것 또한 인권적 차원에서 문제의 소지가 될 수 있다. 형사사법정보는 개인의 직접적 신체적 제한과도 관련있는 것들로 자원 활용의 효율성 이전에 인권의 시각을 우선적으로 적용해야 하는 정보가 다수이다. 하지만, 보다 효율적 활용에 형사사법 당국의 초점이 모아져 있어서 이에 대한 법적, 실질적 관리제도 보완이 시급하다.

3) 보건의료정보통합

(1) 보건의료정보통합의 개요

개인의 의료정보는 민감한 개인정보 중 하나이다. 환자의 질환에 대한 진단과 처방, 의료기록 등의 의료정보가 외부에 알려지게 되면 정보주체의 사회적 관계를 위축 또는 제한시킬 수도 있다. 따라서 의료정보의 수집 및 활용 등에 있어 정보주체인 환자의 권리를 적극적으로 확보할 필요가 있다. 하지만, 의료정보는 흔히 의사가 환자에 대한 의료행위를 실시하면서 수집된 자료들과 이 자료들을 기초로 하여 연구·분석된 정보를 포괄(한국보건의료연구원, 2011)하기 때문에, 의료정보를 환자의 개인정보라기 보다는 병원이나 의사들이 생산하고 통제하는 정보로 인식되어 왔다(국가인권위원회, 2009).

이러한 인식 때문인지 그동안 의료정보보호에 대한 민감성 정도는 그리 크지 않았다. 하지만, 진보된 형태의 정보화가 진행되기 이전에는 의료정보의 공유자체가 원활치 않았기 때문에 의료정보에 따른 인권적 문제는 여타의 정보자원과 마찬가지로 큰 문제로 인식되지 않았다. 하지만, 개별 의료기관의 정보화 수준이 높아지고, 인터넷을 통한 의료정보의 전송 및 공유 등에 대한 논의가 진행되면서 개인의료정보의 보호 문제가 부각되고 있다.

의료기관에서 취급하는 개인의료정보는 개인의 신체의 신상에 대한 정보가 담겨져 있는 것으로, 일반적인 개인정보나 금융정보 등 타 분야에서 다루는 정보에 비해 매우 민감한 정보 때문에 개인의료정보보호 수준 제고를 위한 종합적이고 체계적인 노력이 요구된다(김동수·김민수, 2006). 특히 전자정부가 도입된 이후 지속된 정보자원의 통합DB 구축에 따라 보건의료정보 또한 통합된 DB의 형태의 정보자원 관리를 지속적으로 추구하고 있는바, 보건의료정보자원관리와 관련한 인권적 문제들은 앞으로 계속적으로 나타날 가능성이 매우 높다. 특히 보건의료정보는 보험회사 등

해당 정보의 활용을 통해 금전적 이해를 획득할 수 있는 조직이나 집단이 존재하고 많은 정보를 확보하고 활용하려하기 때문에 보건의료정보에 대한 정보주체의 인권에 대해 더욱 민감하게 반응해야 하는 정보 중 하나인 것이다.

정부의 국가통합DB 구축추진에 따라, 지난 2011년 6월 7일 보건복지부는 개인의 예방접종정보, 건강검진정보 등 개인건강정보를 전국 253개 보건소에서 공유할 수 있는 방안 마련을 위해 '지역보건의료분야 중장기 정보화전략(ISP) 수립' 사업을 추진한다고 밝혔다. 해당 사업은 개인건강정보관리를 통합하기 위해 기존에 보건소별로 자체 구축한 보건행정시스템, 전자의무기록(EMR: Electronic Medical Record)[31]시스템 등 보건소 정보시스템을 통합, 구축한 시스템인 '보건기관통합정보시스템[32]'을 활용하고자 하는 계획이다.

이후 보건복지부는 보건기관통합정보시스템과 연계해 개인건강증진시스템을 구축, 보건소에서 발생되는 모든 개인건강정보를 통합 관리할 예정에 있으며, ISP 기반의 개인건강증진시스템 구축 사업은 오는 2012년 말 완료 예정에 있다. 국내외적으로 EHR 시대의 진입을 핵심 목표로 국가보건의료정보인프라(NHII: National Healthcare Information Infrastructure) 구축을 위한 여러 가지 노력이 진행되고 있는 것이다. 이처럼 보건기관의 운영 및 진료업무에 대해 정보시스템에 의존하는 비중이 높아지면서, 정보의 사용범위가 넓어지게 될 것이고 정보의 공유와 사용은 통합DB 이전에 비해 원활해지게 될 것이다. 시스템 도입이 가속화 되면서 컴퓨터와 네트워크를 통한 정보의 원활한 접근, 관리, 공유가 이루어지지 않고서는 의료기관의 업무가 효율적으로 진행되기 어려운 상황이라는 점에서 시스템의 구축이 필수적 일 수 있다.

---

31) 전자의무기록은 환자의 의무기록(medical chart)을 컴퓨터로 관리하는 것을 의미하며, 단순히 종이 의무기록을 스캐닝한 것으로부터 전자건강기록(EHR:Electronic Health Record)에 이르기까지 다양한 유형이 존재한다.

32) 이 시스템은 지난 2005년부터 시작해 지난해 말까지 180개 보건소에 적용 완료하고, 올해 추가로 73개 보건소에 확대 적용해 253개 전 보건소에 적용 완료할 방침이다.

그러나, 환자의 진료 과정에서 생성되는 정보를 컴퓨터를 이용하여 입력, 저장, 관리하는 전자의무기록 시스템은 기존의 종이 의무기록에 비해 접근성이 뛰어나고 효율적인 정보 공유가 가능하다는 장점을 가지고 있지만, 전자의무기록에는 환자의 진료정보 뿐만 아니라 환자 개개인을 식별할 수 있는 개인정보를 포함하고 있기 때문에 정보보호가 매우 중요하다.

즉, 의료정보화가 발전되고, 국가 차원의 보건의료정보인프라 구축 논의가 진전되어감에 따라 환자의 개인정보와 의료정보의 보호가 매우 중요한 이슈로 부각되고 있다(보건복지부, 2005). 전자의무기록이 의료기관 경계를 넘어서서 진정한 개인의 평생 건강기록인 EHR 개념으로 발전하기 위해서는 전자의무기록에 대한 정보보호 수준 제고와 함께 개인의료정보 보호 마인드 제고가 필요하다. 환자 진료를 위한 정보의 공유 및 사용과 정보보호 및 프라이버시 보장이 균형화될 때 보안에 대한 우려가 해소될 수 있다.

(2) 추진배경

보건의료정보를 통합하고 관리하는 시스템을 추진하게 된 배경은 다음과 같다. 먼저 의학기술이 발달하고 정보화가 진전되는 등 보건의료 환경의 변화가 지속적으로 나타났다는 점이다. 생명과학, 생명공학 기술의 급격한 발달로 새로운 장비, 치료방법 등이 개발 도입되어 정보화에서 담아야 할 정보의 내용 유형이 매우 다양해지고 있으며, 특히, 인터넷 기술의 발달로 보건의료 영역의 정보에서 인터넷 활용 정보기술이 비약적으로 발전하고 있어 이를 활용할 필요성이 보다 높아지고 있기 때문이다.

다음으로 보건의료 정책이 질병치료 중심에서 건강증진을 위한 활동으로 전환되면서 보건복지 지식기반 사회조성을 위한 전문분야 간 협력강화가 더욱 필요하게 되었다. 이는 보건 · 의료 · 복지의 통합적인 서비스 체계를 강화하기 위함으로, 각 분야의 정보가 체계적으로 공유될 수 있는 기재를 마련해야 한다는 것이다. 보건복지부 정보화 정책 수립을 통해 보건복지부 자체 정보화 종합 기획 기능의 강화하고 국민을 위한 평생 의료

의 실현, 전 국민 중심의 정보서비스 제공, 전문화된 운영관리 체계(일원화된 특정 센터 중심)의 구축, 보건복지 통합망 등을 제시하고 있다. 그러나 그동안의 국가보건의료분야의 정보화사업은 보건의료정보 공유 및 활용의 제한, 시범사업 추진 전략의 미흡, 교육훈련 및 법·제도 개선의 미흡, 정보화 기반환경의 문제 등으로 부정적 평가를 받고 있다. 이러한 이유에서 보건의료 정보화기반을 더욱 강화하려 하고 있고, 국가보건의료정보인프라 구축을 지속적으로 진행하고 있다.

또한 보건복지부에서는 보건의료이용의 편리성과 새로운 보건의료서비스 창출에 대한 욕구, 의료이용자들의 보건교육 및 정보제공 욕구, 보건의료인력 및 훈련에 대한 욕구, 환자-의사관계 변화에서 요구되는 정보서비스의 필요, 보건의료조직 변화에 대응할 보건의료정보서비스의 필요, 병원 내 정보체계와 지역사회 정보체계 통합에 대한 욕구, 상업적거래 변화에 따른 정보서비스 필요, 표준화 및 통합적 데이터베이스에 대한 욕구, 의학교육 변화에 따른 교육정보화의 필요, 국가 보건의료체계 관점에서의 정보화서비스지원환경 수립의 필요와 같은 보건의료정보화의 수요를 언급하면서 보건의료정보의 통합을 추진하고 있다.

<그림 6-5> 보건의료정보화 체계도

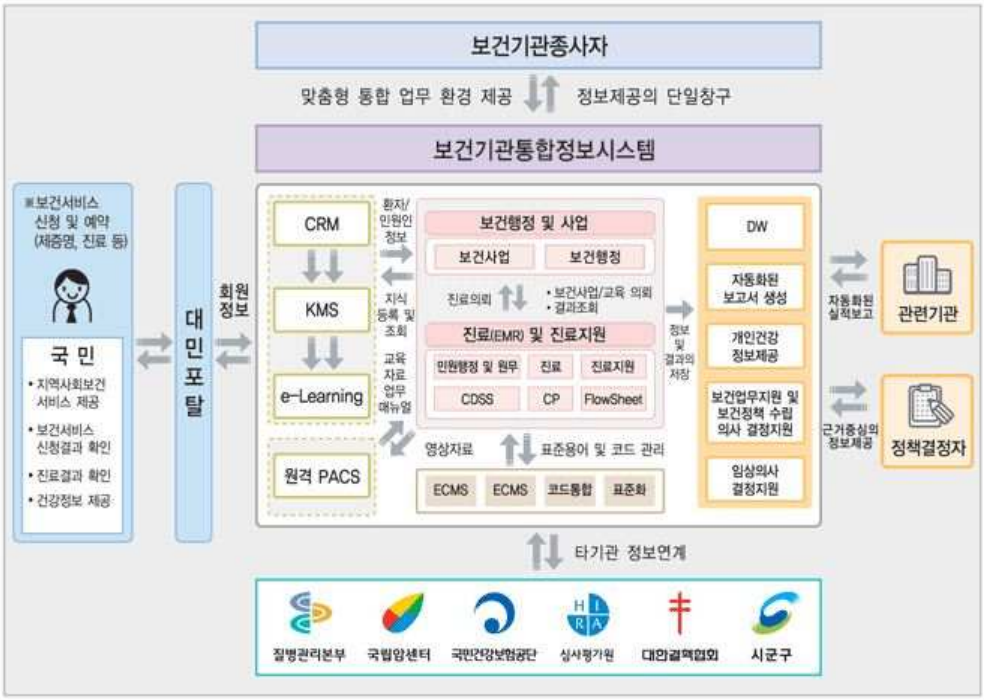
(3) 추진경과

보건의료정보화의 목적은 국민 모두에게 언제, 어디서나 질 높은 의료서비스 이용의 편리성과 효율성을 보장하기 위함으로, 보건의료기관의 업무를 효율화하고 유관기관과 전자적 정보교류체계 강화를 통한 공공보건의료 서비스의 질을 향상시키고, 보건의료소비자의 다양한 요구 및 의료환경변화에 대응할 수 있는 선진의료서비스 체계 마련 및 양질의 서비스 제공하는 것이다.

이를 위해 보건복지부는 'u-Health 서비스' 등 보건의료정보산업을 국제 경쟁력을 갖춘 고부가가치 산업으로 육성하고 있으며, 전국 보건소, 보건지소 등 약 3,500개의 공공보건기관을 대상으로 하는 정보화 사업인

‘공공보건 정보화’와 국립대병원, 지방공사의료원, 국립정신병원 등 공공의료기관을 대상으로 하는 정보화 사업인 ‘공공의료 정보화’의 큰 줄기 속에서 보건의료정보화를 추진하고 있다.

〈그림 6-6〉 보건의료정보화 시스템 구성도



자료 : 한국보건복지정보개발원(http://www.khwis.or.kr/)

2003년 8월 전자정부 로드맵 추진체계에 국가복지종합서비스가 선정되면서 본격적으로 시작되었다. 이후 2004년 12월부터 2005년 10월에 지역보건의료분야의 정보화전략계획(ISP) 수립되었고, 2005년 12월에는 공공보건의료확충 종합계획이 확정되고, 보건의료정보화사업추진단이 발족하였다. 2006년 7월부터 2007년 8월까지 ‘보건기관정보화사업 1단계’ 구축이 진행되었는데, 보건기관통합정보시스템과 대민 및 업무포털 구축을 내용으로 하고 있다.

2007년 9월부터 2008년 12월까지는 보건기관통합정보시스템의 고도화와 시범운영, 대민 및 업무포털의 리뉴얼과 고도화 등의 내용을 담은 ‘보건기관정보화사업 2단계’ 구축이 진행되었으며, 2008년 3월에 ‘공공보건포털’이 서비스 제공을 시작하게 되었다. 2009년 6월부터는 ‘보건기관정보화사업 3단계’를 진행하고 현재의 보건기관통합정보시스템 유지보수 및 운영이 이루어지고 있으며, 2010년부터 지금까지 ‘보건기관정보화사업 4단계’사업을 진행하고 있다. 지난 2011년 6월 7일 보건복지부는 전국 253개 보건소에서 개인의 보건의료정보를 공유할 수 있는 ‘지역보건의료분야 중장기정보화전략(ISP) 수립’ 사업을 추진한다고 밝혔으며, 해당 사업은 2012년 말 까지 완료할 예정에 있다.

(4) 정보자원 생애주기에 따른 분석

① 수집 및 생성

보건의료정보는 「의료법」 제22조에 의해 진료기록부 등 의료기록으로 보존된다. 진료기록부에 작성되는 내용은 「의료법시행규칙」 제14조(진료기록부 등의 기재 사항)에 명시되어 있으며 이에 준하여 환자의 개인정보 및 의료정보를 작성하도록 되어 있다. 따라서 개인의 보건의료정보를 수집할 시에는 두 법적 근거에 따라 작성되어야 하는 것이다. 하지만, 개인정보 수집 및 제공과 관련한 2009년 진보네트워크센터의 보고서에 따르면 국립병원 및 국립대학교 병원에서 보유하고 있는 진료기록부의 내용에는 「의료법시행규칙」 제14조에서 언급되지 않은 결혼여부, 학력, 종교 등 여타 민감한 개인정보까지 수립하고 있으며, 개인정보의 수집과 이용, 공유에 대한 별도의 동의문서를 정보주체에게 받지 않고 있다. 이는 정보주체인 환자가 자신의 정보를 선별적으로 제공할 수 있는 권한을 침해한 것으로 볼 수 있으며, 이로 인한 갈등이 나타날 우려가 있다.

현행 「개인정보보호법」에는 개인정보의 처리 목적을 명확하게 하여

야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하도록 하고 있으며, 법률이 정하는 경우에 한하여 개인정보를 수집할 수 있도록 하고 수집목적의 범위에서 이용할 수 있도록 하고 있다. 또한 'OECD 개인정보보호 8원칙'에서도 이용 및 목적 상 필요한 범위 내에서 개인정보를 확보하도록 하고 있다. 따라서 진보네트워크센터의 조사에 의하면 공공기관인 국립병원과 국립대학교 병원에서는 법에서 정하고 있는 정보수집의 기준을 따르지 않고 있는 것이다. 이는 정보에 대한 자기결정권은 공공기관에서 침해하고 있는 것으로, 병원의 관리 효율을 위한 정보수집이 아닌 질병의 치료를 위해 정보를 수집하고자 하더라도 정보를 제공자가 가지고 있는 자기결정권은 필히 확보했어야 한다.

만약 법률에 명시되지 않은 정보 제공을 요청해야 하는 경우는 필수사항과 선택사항을 구분하여 정보주체의 자기결정권을 보장하는 필요한 것이다. 이는 단지 국립병원의 문제는 아니다. 보건의료정보를 취급하는 곳은 국민건강보험공단, 건강보험심사평가원, 질병관리본부 등이 있는데, 이들은 의료기관으로부터 의료정보를 제공받아 수집하고 있는 곳이다. 하지만, 이들 기관에서 정보를 수집하는 방법은 정보주체의 동의를 받고 수집하는 것이 아닌 법률에 근거하여 타 기관으로부터 제공받고 있다. 이는 해당기관에서 주어진 업무를 처리하기 위해 개인의 보건의료정보를 스스로의 판단에 의해 수집하는 것과 다르지 않다.

이처럼 보건의료정보의 수집은 정보주체의 동의를 충분히 구하지 않거나 법적 기준 외의 정보까지 수집하는 등 인권적 관리에 있어 문제점을 가지고 있다. 많은 개인들은 병원에 방문할 때 환자라는 입장이 되기 때문에 병원에서 요구하는 정보를 제공할 수밖에 없는 경우가 많다. 그렇게 때문에 해당 정보제공에 대한 정보제공자의 권리를 공공기관에서 고지해야 할 필요와 의무를 가지고 있는 것이다.

병의원은 보다 많은 정보를 확보하여 질병의 치료 이외의 부분에도 해당 정보를 활용할 수 있기 때문에 해당 정보가 질병 치료를 위해 활용될 것이라는 정보제공자인 환자의 생각과는 다른 측면을 보일 수 있다. 그리

고 보건의료정보화에 따른 통합DB가 보다 확장된 경우, 수집된 보건의료정보는 단지 해당 병원 뿐 아니라 여러 기관에서 보다 쉽게 공유할 수 있기 때문에 보건의료정보의 수집은 명확한 법적 근거에 따라 정보제공자의 동의를 반드시 구하도록 해야 하며 정보제공의 선택권을 보장해야 한다. 현재 보건의료정보의 수집에 있어 이와 같은 정보제공자의 자기결정권을 보장하지 못하고 있는 부분은 인권적 측면에 있어 갈등을 야기할 가능성이 있으며, 만약 갈등 상황의 발생으로 인해 현재까지 수집된 정보들에 대한 동의를 다시 구해야 하는 일이 벌어지게 되면 상당한 시간과 비용이 소요될 것이다. 따라서 수집과 관련한 갈등이 발생하지 않도록 자기결정권을 보장하는 정보자원의 관리가 필요하다.

② 보관 및 저장

과거에는 보건의료정보가 병원에 문서로 보관되어 있었으나 현재는 전자의무기록(EMR), 처방전달시스템(OCS), 의료영상저장전송시스템(PACS) 등 병원 정보화시스템 보급률이 높아지면서 저장된 보건의료정보가 유출될 수 있는 위험은 여타의 정보자원들과 다르지 않다. 환자의 개인정보가 이들 전자시스템으로 관리되면서 해킹 등을 통한 대량 유출 가능성은 상존하게 되는 것이다. 「개인정보보호법」에는 저장과 관련하여 개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 법률이 정하는 대로 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하도록 하고 있다.

다시 말하면 보건의료정보의 관리를 위한 표준화 된 기준이나 지침에 따라 정보의 보관과 저장이 이루어져야 하며 이에 따른 관리 감독이 수반되어야 한다. 하지만, 의료기관의 개인정보보호 강화를 위해 배포한 「500병상 이상 의료기관 대상 개인정보보호 가이드라인」은 유명무실한 상황이고 개인정보보호 관리 및 조직체계, 인적보안, 정보시스템 보안관리 및 접근관리 등을 내용으로 하는 의료기관 인증 조사기준에의 개인정

보보호 관련 항목 추가나 보건의료정보 보호와 관련한 「건강정보보호법안」은 아직 제정되지 않고 있다. 저장과 관련한 명확한 법적 근거가 미비하고 규정된 지침 등이 실제적 효력을 발휘하지 못해 유명무실하다는 문제를 안고 있다.

이러한 상황에서 데이터화된 정보가 네트워크를 통해 많은 병의원에 공유 및 저장되고 있으며, 해킹 등 외부의 공격이나 내부자의 정보유출은 지속적으로 나타나고 있다. 특히 내부자의 정보유출은 조직관리라는 측면에서 충분히 통제할 수 있는 부분임에도 불구하고 지속적으로 발생하고 있는데, 예를 들어 보건의료정보를 다수고 있는 국민건강보험공단의 경우, 2011년 국정감사 자료에 따르면 개인정보 유출 징계처분 건수가 2009년에 19건, 2010년에는 13건, 2011년 9월 기준 9건으로 내부자에 의한 정보자원의 인권적 문제가 지속적으로 야기되고 있다. 사적인 용도로 활용하기 위해 개인정보를 무단열람하거나 지인의 부탁을 받고 수급자들의 개인정보를 무단열람, 유출하는 문제가 여전히 나타나 있다.

그리고 개인정보취급 업무담당자들의 업무용 PC에 대한 개인정보 관리점검 결과에서도, 점검대상 100대의 PC 중 4대의 PC에서 삭제되었어야 할 개인정보파일이 발견되었다. 외부의 침입으로 인한 정보인권의 문제 이전에 정보자원을 저장 · 사용 · 공유하는 정부기관 내부에서의 관리적 문제가 지속적으로 발생되고 있는 것이다. 이는 관리의 측면으로, 정보자원을 다루는 정부나 공공기관에서 정보자원의 주체가 가지는 권리를 중요시하지 않고 있으며 기관이나 개인의 필요에 의해 활용 가능한 자원으로 인지하고 있기 때문이다.

하지만 정보자원, 특히 보건의료정보는 단순히 개인의 신상과 관련한 인권의 문제 뿐 아니라 해당 정보는 개인의 건강과 관련되어 있는 것들이기 때문에 더욱 신중하게 다루어야 하는 문제이다. 개인의 보건의료정보의 유출이나 이에 따른 오남용으로 인해 개인의 병력정보 등이 알려지면 정보주체는 이를 통해 사회활동과 관계에 제약을 받을 수도 있으며, 해당 정보가 보험회사 등 건강의료 관련 기업에 들어가게 되면 이에 따른 개인

의 보건의료 활동에 영향을 미칠 수밖에 없다.

따라서 이러한 보건의료정보를 다루는 기관과 구성원들은 해당 정보를 다룸에 있어 상당한 신중함이 필요하며, 위법한 행위를 하지 못하도록 하는 관리 측면에서의 장치가 설치되어 있어야 한다. 이러한 관리 장치가 존재하지 않는다면, 보건의료정보의 인권적 측면에 대한 문제는 매년 지속적으로 발생하게 될 수 있으며 보건의료정보가 국가통합DB화 될 경우에는 더 많은 정보들이 많은 조직이나 구성원들에게 노출될 수 있어서 현재의 직원 윤리에 대한 문제를 넘어 정보인권과 관련한 사회적 갈등을 야기할 소지가 충분하다. 이와 같이 저장관리의 문제로 인해 보건의료정보가 유출되고 이러한 유출에 의해 특정 개인에게 피해가 가는 경우에 나타날 수 있는 갈등의 정도가 상당할 가능성이 있다. 개인정보보호에 대한 법률이 존재함과 더불어 정보유출이 지속적으로 발생하고 있음에도 불구하고 관리상의 어려움 등으로 정보보호가 제대로 이루어지지 않게 되면 병의원에서 이루어지는 정보수집과 저장에 대한 신뢰 저하와 이로 인한 갈등은 소수의 병의원에서만 나타나지 않을 것이기 때문이다.

③ 분배 및 공유

보건의료정보는 「의료법」에 따라 의약품의 필요나 치료의 목적을 위해 1차 의료기관에서 2·3차 의료기관으로 진료 병원을 이동할 때 등의 이유에서 진료기록이 제공된다. 그리고 병원에서 보유하고 있는 의료정보는 약국이나 병원 뿐 아니라 「국민건강보험법」에 따라 국민건강보험공단 등 의료정보를 필요로 하는 공공기관에 공유되어지고 있다.

그리고 수사의 목적이나 산재보험의 심사 등의 이유로 보건의료정보가 공유되고 있다. 그러나 이러한 공유의 상당수는 정보주체의 동의하에 이루어지기 보다는 법률에 근거하여 이루어지고 있는데, 정보를 제공한 정보주체는 자신의 보건의료정보가 어떠한 목적에 따라 누구에 의해 공유되고 있는지 모르는 상태에서 정보 공유가 이루어지고 있는 것이다. 현재

국립서울병원에서 개인정보에 대한 근거로 [공공기관의 개인정보보호에 관한 법률] 제10조(이용 및 제공의 제한)를 제시하고 있는데, 해당 법률에서는 '다른 법률에 의해 보유기관 내부에서 이용하거나 보유기관이외의 자에게 제공하는 경우' 등 과 같이 여타의 법적 근거만 마련하면 정보공유가 이루어질 수 있도록 하고 있다.

해당 정보의 활용을 위해 행정입법에 의한 법 근거만 마련한다면 정보주체의 동의 없이 보건의료정보가 공유될 수 있다. 이는 단순히 보건의료정보의 공유에만 해당하는 문제가 아닌 현재 정부에서 저장하고 있는 모든 개인정보에 해당하는 것으로, 정보관리에 있어 효율성 측면이 지나치게 강조되어 있다는 것을 보여주고 있다.

「개인정보보호법」 제18조 (개인정보의 이용·제공 제한)에서도 '정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다' 고 명시하는 등 개인정보의 공유에 대해 엄격한 기준을 정해놓고 있지 않다. 현재 보건의료정보는 법적 근거에 따라 공유되고 있는데, 법류에서는 공유의 예외조항을 지나치지 넓게 설정하고 있어 정보자원의 인권적 관리가 원활히 이루어지지 못하도록 하고 있다. 그리고 정보주체의 권리를 침해하고 있다. NEIS나 KICS에서도 자신의 정보가 자신도 모르게 공유될 수 있다는 문제로 인해 갈등이 발생되었는데, 보건의료정보의 경우도 불명확한 법률로 인해 목적외의 공유가 가능하도록 함으로써 갈등의 소지를 충분히 가지고 있고, 이러한 부분을 보완해야 할 것으로 판단된다.

④ 사용

개인정보의 사용과 관련하여 'OECD 개인정보보호 8원칙' 에서는 명시된 목적에 적합한 개인정보의 이용에 대해서 언급하고 있고, 「개인정보보호법」에서는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적외의 용도로 활용해서는 안 되는 것과

정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다는 규정을 명시하고 있다.

하지만, 분배 및 공유에서 언급한 바와 같이 보건의료정보의 사용에 대해 형사사건 등의 이유에서 폭넓은 예외규정을 두고 있어 목적 외 사용을 제재하기 어려운 상황이다. 이러한 넓은 예외규정은 'OECD 개인정보보호 8원칙' 중 하나인 목적 구체성의 원칙과 이용제한의 원칙에 위배되는 것으로(국가인권위원회, 2009), 「공공기관의 개인정보보호에 관한 법률」에서 개인정보파일을 보유목적외의 목적으로 이용하거나 제공할 수 있는 예외 사항을 지속하는 한 이로 인한 정보주체의 정보인권 침해를 지속적으로 이루어 질 수 있다. 그리고 정부기관 입장에서의 정보자원 사용 근거의 마련은 정보자원과 관련한 다른 갈등사례에서와 마찬가지고 정보자원과 관련한 갈등을 발생시킬 우려를 가지고 있다.

⑤ 폐기

보건의료정보는 「의료법 시행규칙」에 의거하여 보존기간이 정해져 있다. 하지만 이는 의무적인 보존기간일 뿐 이것을 폐기해야 한다는 규정이 명시되어 있지는 않다. 보건의료정보의 폐기와 관련한 규정이 명확하지 않다는 것이다. 따라서 병의원에서 이를 폐기하지 않는다 하더라도 제대할 근거가 마련되어 있지 않고 있는 것으로, 전국 80개 의료기관을 대상으로 한 조혜경의 연구에서는 개인건강정보의 수집목적 또는 제공받은 목적을 달성한 경우에 개인건강정보를 파기하지 않는 의료기관은 51.3%, 파기하는 의료기관은 48.8%로 나타났으며, 개인건강정보의 수집목적 또는 제공받은 목적을 달성한 경우에 개인건강정보를 파기하고 환자에게 고지하는 절차가 없는 의료기관은 93.8%,개인건강정보를 복구 불가능하도록 파기하는 절차가 수립되지 않은 의료기관은 85.0%로 나타났다.

또한 행정안전부가 김을동 의원에서 제출한 자료에 따르면, 질병과 신체적 특징 등의 민감한 개인 정보를 대량 보유하고 있는 국민건강보험공

단이 보유 기한을 초과한 1억6000여만 건의 개인 정보를 파기하지 않고 불법 보유한 것으로 나타났다. 특히 건보공단이 불법 보유한 개인 정보 중에는 개인별 건강검진 기록 9000여만 건이 포함되어 있었으며, 정부 특별 점검에서 이 사실이 적발된 직후에는 보유 기간을 '준영구(準永久)'로 바꿔 검진 정보를 평생 보유하려는 시도를 했던 것으로 나타났다. 「개인정보보호법」 제21조(개인정보의 파기)에서는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때는 그 개인정보를 파기하여야 한다고 명시되어 있지만, 실제 보건의료정보를 보유하고 있는 공공기관이나 병원에서는 정보를 폐기하지 않고 있다. 정보를 보유하고 있는 공공기관과 병원에서 정보를 스스로 폐기하지 않는다면 정보주체가 자신의 보건의료정보를 폐기를 청구해야 한다.

그러나, 「보건의료기본법」과 「의료법」에서는 정보주체의 정보폐기 청구권에 대해 규정하고 있지 않고 있다. 정보를 보유하고 있는 공공기관이나 병원에서 정보주체의 정보인권을 보장하기 위해서는 보유 목적이 사라진 정보를 자발적으로 폐기해야 하며, 이에 대해 「개인정보보호법」에서도 언급하고 있다. 하지만 규정과 실제가 다르게 나타나고 있는 점은 정보보유기관과 정보주체간의 갈등을 불러일으키는 원인이 될 수 있다.

(6) 소결론

보건의료정보자원과 관련하여 사회적으로 표면화된 갈등은 아직 나타나지 않고 있다. 보건의료정보는 개인정보라는 인식 이전에 의료기관에서 다루는 전문정보라는 인식이 있고 보다 효과적인 의료서비스를 제공받기 위해 개인의 건강정보를 자발적으로 제공하고 있다는 생각을 가지고 있다. 이와 더불어 2010년 국정감사에서 지적된 바와 같이 국가의 보건의료 통합정보화추진이 다소 늦어진 측면이 있었기 때문에 보건의료정보와 관련한 갈등은 크게 부각되거나 나타나지 않았으며, 최근에 보건소의 의료정보를 통합 관리하는 시스템이 운영되고 있는 등 보건의료정보의 통합화

는 앞의 NEIS나 형사사법통합정보시스템과 같이 본격적으로 운영되고 있지는 못하다.

특히 보건의료분야는 상당수를 차지하는 민간병원과의 정보연계와 통합이라는 문제가 있기 때문에 해당 분야에 대한 정보인권과 관련한 갈등은 아직까지 두드러지게 나타나지는 않았다. 하지만, 보건의료분야의 경우는 민간병원과 정보를 공유해야 하는 경우가 많아 정보유출에 따른 인권적 문제에 대해 더욱 민감하게 다루어야 한다. 과거에 비해 인터넷 사용, 웹 환경 전환 및 웹 서비스 확대, 병원 간 진료정보 공유 등 협진체계 구축 · 확대 등으로 외부와 직접 연결되는 통로가 증가하고 넓어지면서 병원 환경이 개방되고 있어(이유지, 2005) 정보에 대한 보다 높은 수준의 관리가 필요할 것으로 보인다.

특히 언제 어디서나 의료 서비스가 찾아가는 'u-health' 환경으로 의료 서비스가 전환되고 점차 통합DB화되면서 모여지는 정보의 수가 많아지고 접근할 수 있는 사람들과 경로가 증가하게 되면서 정보유출의 우려가 높아지고 있다. 만약 해킹이나 사이버 테러를 통해 보건의료정보망을 통해 정보를 디지털화된 정보를 빼내거나 위조하는 경우에는 환자의 프라이버시를 침해하는 것이 되며, 환자의 안전에 대한 우려도 발생할 수 있다. 이렇듯 보건의료정보는 해당 정보의 민간과의 공유와 활용, 환자의 안전에 영향을 미치는 중요성 때문에 이러한 정보를 다룸에 있어 정보보호와 인권이라는 측면에 더욱 관심을 두어야 한다.

갈등관리에 있어 가장 효과적인 것은 갈등이 증폭되는 것을 방지하는 것으로, NEIS나 형사사법통합정보시스템 사례와 같이 갈등이 증폭하지 않도록 정보자원의 인권적 관리를 지속적으로 강화할 필요가 있다. 하지만, 보건의료정보통합과 관련하여 이전 사례에서 나타난 인권적 문제가 여전히 나타나고 있으며, 이는 차후에 보건의료정보가 지금보다 더 광범위한 네트워크 통합망을 구축하게 되면 과거의 사례와 같은 갈등이 발생할 우려가 많다. 과거의 정보자원과 관련한 갈등 사례에서 나타난 문제점에 대한 보완이 충분히 이루어지지 않고 있으며, 보건의료정보와 관련한 내부

자의 무단 열람과 공유 등의 문제는 매년 되풀이 되고 있다.

각 생애주기 별 이슈를 살펴보면, 먼저 수집 및 생성 부분에서는 법령에서 제시하고 있는 진료기록부 이외의 정보를 수집하고 있다는 이슈가 특징적으로 나타났다. 정보의 저장, 공유 및 분배 측면에서는 정보에 접근 가능한 내부자의 개인적 이유에서의 정보유출 가능성에 대한 부분이 특징적이며, 사용에 있어서는 포괄적 예외가 적용된다는 문제가 갈등의 이슈로 나타나고 있다. 폐기에서는 보건의료정보에 대한 폐기규정이 미비하여 많은 병의원 및 관련기관들이 정보를 폐기하지 않고 있으며, 정보보유 기관에서는 의도적으로 정보를 준영구화하여 폐기하지 않으려는 시도를 계속하면서 갈등발생의 소지를 나타내고 있다.

〈표 6-5〉 보건의료정보통합의 정보자원 생애주기에 따른 이슈

	정보자원생애주기				
	수집/생성	저장	분배/공유	사용	폐기
생애주기별 인권적 이슈	▪ 정보주체의 동의를 구하지 않은 정보수집 ▪ 법령외의 정보를 수집	▪ 명확하고 엄격한 규정의 필요 ▪ 내부자에 의한 정보유출	▪ 목적외 사용의 우려 ▪ 내부자에 의한 무단정보 열람과 공유	▪ 목적외의 사용을 폭넓게 인정 ▪ 사용과 관련한 명확한 법 규정의 미비	▪ 폐기 규정의 미비 ▪ 정보보유 기관의 의도적인 정보 미폐기

보건의료정보가 가지는 갈등적 요소에 대해 관리상의 문제를 국정감사에서 지적된 바 있으며, 이에 보건복지부는 의료기관의 개인정보보호 강화를 위해 「500병상 이상 의료기관 대상 개인정보보호 가이드라인」을 마련하여 배포하면서 보건의료정보보호를 위해 지속적 노력을 하고 있다는 시정조치를 취하였다. 하지만, 이러한 가이드라인은 강제성이 없는 것

이어서 상당수의 병의원에서는 해당 가이드라인은 그저 개인정보보호를 잘해야 한다는 정도의 내용으로만 받아들이고 있다.

실제 2011년 2월 조사에 따르면, 가이드라인 상으로는 병원에는 비 의료인을 포함한 5인 이상의 개인정보보호위원회를 구성하고 1인 이상의 보안 전담 정규직원을 둬야 하며, 또 2~3년마다 정보보호 감사를 받아야 하고 정보보호 교육, 정보자산 목록화, 보안등급 부여 등을 시행할 것을 명시하고 있지만, 한 국립대학병원의 경우는 기존 정보화 담당부서 직원들이 보안에 대한 업무도 함께 맡고 있는 등 정보자원의 관리에 있어 가이드라인을 따르지 않고 있다. 그리고 한 신문의 인터뷰에서 보건복지부 관계자는 "10명의 정보화 담당부서 인력으로 200여개의 대형 병원의 보안을 감독하기는 사실상 어렵다"고 언급한 바, 현재는 정보인권에 직접적 영향을 미치는 정보보안관리가 효과적일 수가 없는 조건이 마련되어 졌다. 현재는 지역 보건소간 정보통합이 이루어졌으며, 이와 같은 보건의료정보의 통합은 계속 진행되고 있는 등 기술적 측면에서의 정보자원의 효율적 관리에 대해서는 많은 진보를 가져왔다.

하지만 이에 수반되는 정보자원의 인권적 관리는 그 사안의 중요성이 상당함에도 불구하고 관리적 측면의 관심에서는 멀어져 있다. 정보자원과 관련한 다른 갈등사례들을 보면 정보자원의 효과적 활용과 정보자원의 인권적 측면에 대한 관리상의 고려가 불균형을 이루게 되면 사회적 갈등을 야기한다. 현재 보건의료정보를 관리함에 있어 이와 같은 불균형을 법제도나 조직 관리 등에 있어 나타나고 있기 때문에 갈등이 발생할 우려가 있는 것이다.

4. 종합분석

지금까지 언급한 세 가지 사례의 정보자원과 관련한 생애주기 별 이슈를 정리하면 <표 4-8>과 같다. 전체적으로는 정보자원 관리와 관련한 명확하고 엄격한 규정이 없거나 미비한 측면으로 인해 시민단체와 갈등을 불러 일으켰다. 정부는 전자정부를 실현하는 과정에서 기술의 도입과 효율적 관리에 중심을 두면서 정보인권과 관련한 법 · 제도적 측면을 부차적으로 고려하고 있다. 이에 정보인권에 대한 명확한 규정이 드러나 있지 않음으로 인해 이에 대한 정부의 조치나 활동이 부족하면서 이에 대한 시민단체의 우려가 갈등이라는 현상으로 나타났다. 따라서 정보자원 관리의 기술적 측면의 강화를 우선시 하면서 이에 대한 사회적 문제를 예방할 수 있는 법적, 제도적 측면에서의 조치가 부족하여 갈등을 일으켰다고 해석할 수 있다.

각 정보자원생애주기별로, 수집 및 생성에서는 공통적으로 정보 주체의 동의 없이 개인 정보를 수집하거나 포괄적인 규정으로 인한 정보수집으로 인해 정보주체의 선택권이 부여되고 있지 않음이 나타나고 있다. 저장과 관련해서는 정보의 저장 및 보관과 관련한 보다 엄격한 규정의 필요성이 나타나고 있으며, 공유에 대해서는 정보자원의 목적외 사용에 대한 우려와 정보주체의 동의를 얻지 않은 공유가 문제로 나타났다. 사용에 대해서는 보유목적외의 사용을 폭넓게 인정하고 있는 점, 폐기와 관련하서는 폐기에 대한 불명확한 규정이나 규정이 없는 경우로 인해 갈등이 나타나고 있다고 볼 수 있다.

각 사례별 특징으로는, 먼저 NEIS 사례에서는 정보주체자가 미성년자이고 학생이기 때문에 부모의 열람이 가능하다는 이유에서 이들의 열람권을 보장하지 않고 있으며, 교육정보자원을 집적화하려는 계속된 시도에 따라 대규모 정보유출의 우려가 지속된다는 점이다. 다음으로 KICS 사례에서는 정보수집단계에서 정보수집자와 정보제공자 간의 관계가 대등하지 않은 경우가 많아 정보제공자의 선택권이 보장되지 않을 가능성과 수사자료의

특성상 정보수집자의 주관적 판단이 개입될 가능성이 있어 이들 자료 활용에 의한 선의의 피해자가 발생할 우려가 있다. 또한 형사사법에 대한 정보를 활용하고 저장하는 기관들의 특성과 관할범위가 다름으로 인해 한 기관에서 정보가 폐기되어도 다른 기관에서 정보를 가지고 있을 가능성이 있어 완전한 폐기가 어렵다는 특징이 있다. 마지막으로 보건의료정보통합 사례에서는 법령에 나타나고 있는 진료기록부 이외의 정보를 수집하는 기관이 다수 있어서 정보 수집 측면에서 문제가 나타나고 있으며, 공공기관 내부자의 의한 정보의 무단열람과 공유, 유출이 빈번하게 이루어지고 있어 개인정보보호에 대한 문제가 매년 지적되고 있다는 점이다. 폐기에 있어서는 보건의료기관에서 기 확보한 정보자료를 영구적으로 보관하여 이를 연구자료 등으로 활용하려고 하고 있어 정보주체의 폐기에 관한 권한을 침해하고 있다는 문제를 가지고 있다.

이와 같은 문제로 인해 갈등이 발생하는 근본적인 이유는 정보자원에 대한 인식에서 차이 때문이다. 앞서 언급했던 바와 같이 정부는 정보자원을 도구적 합리성 차원에서 다루고 있지만, 정보자원은 효과적 관리를 위한 도구인 이전에 정보주체에 대한 다양한 측면을 보여준다는 점에서 인권적 요소를 담고 있다. 자원 활용의 효율을 높이기 위해 예외 규정을 넓게 설정하는 등의 정부의 정보자원 관리로 인해 현재 부각되고 있는 정보인권이 보장되고 있지 못하면서 정보자원과 관련한 갈등이 지속되고 있다. 그리고 전자정부 이후, 국가통합DB를 구축하고자 하는 시도가 증가하면서 이러한 갈등은 점차 증가하고 있다. 이러한 갈등을 완화시키기 위해서는 정보자원 관련 법 규정에 있어 정보인권을 보장할 수 있는 명확한 법령을 제정하고 개인정보보호를 위한 기구를 상설화함과 동시에 정보주체가 자기 정보의 사용 · 공유 · 폐기를 확인 할 수 있도록 정보주체의 열람권을 보장해주도록 해야 할 것이다.

〈표 6-6〉 각 사례의 정보자원 생애주기에 따른 특징적 이슈

	정보자원생애주기				
	수집/생성	저장	분배/공유	사용	폐기
공통이슈	▪ 정보수집에 대한 명확한 법적 근거 미비 ▪ 정보주체의 동의 없이 개인정보를 집적	▪ 정보의 저장 및 보관과 관련하여 보다 엄격한 규정 필요	▪ 목적외 사용의 우려	▪ 정보주체의 알권리 행사의 어려움 ▪ 목적외의 사용을 폭넓게 인정	▪ 정보주체의 알권리 행사의 어려움 ▪ 폐기 규정의 미비
교육 행정정보 시스템	▪ 자기정보 통제권, 선택권 침해	▪ 정보자원 집적에 따른 대규모 유출의 우려	▪ 행정상 편의를 위해 공유 ▪ 정보주체의 알권리 행사의 어려움	▪ 관리주체의 자의적 정보사용 ▪ 사용과 관련한 명확한 법규정의 미비	▪ 자료의 사용 후 폐기를 확인하기 어려움
형사사법 통합정보 체계	▪ 정보수집의 대등하지 않은 관계 ▪ 수자기록에 주관적 판단 개입 ▪ 수집에 대한 포괄적 예외 조항	▪ 공공기관 종사자 개인 수준에서의 취약한 보안관리 ▪ 저장에 대한 포괄적 예외 조항 적용 가능	▪ 정보의 이용 및 제공의 제한과 관련하여 예외규정 ▪ 범죄해결을 이유로 공유에 대한 사전조치 미흡	▪ 개인적 이유로 제3자에 정보제공	▪ 결재된 서류는 수정 및 삭제불가 ▪ 한 기관의 삭제로 정보가 폐기되지 않을 우려
보건기관 통합정보	▪ 법령외의 정보를 수집	▪ 내부자에 의한 정보유출	▪ 내부자에 의한 무단정보 열람과 공유	-	▪ 정보보유 기관의 의도적인 정보 미폐기

Ⅶ. 정부의 정보자원관리 실태분석

1. 설문조사 개요

현재 정부의 정보자원관리 실태를 파악하기 위해 정보자원의 관리자인 조직과 그 구성원들이 어떤 인식을 가지고 있는가는 매우 중요하다. 이러한 인식이 실제 행태로 이어지기 때문이다. 실제로 정부기관의 개인정보 유출 사건이 발생하는 배경에는 조직과 그 구성원들의 정보자원관리에 대한 낮은 인식 수준이 문제가 되었다.

따라서 정보자원의 관리과정에서 조직과 그 구성원들이 인권적 원칙에 관하여 어떻게 인식하고 있는지 조사하고 조직과 그 구성원들의 인식 수준이 법적 체계나 정보인권원칙 등과 얼마나 괴리되어 있는지, 어떤 정보자원관리 단계상에서 그 괴리가 가장 크거나 작은지 등을 확인하려 한다. 괴리가 큰 단계일수록 정보자원관리 상의 갈등이 더 높게 나타날 수 있으며, 이러한 괴리 상태가 지속된다면 아무리 좋은 인권적 관리원칙을 수립하더라고 갈등은 계속 발생할 수밖에 없을 것이다.

따라서 조직과 그 구성원의 인식과 정보자원관리상의 원칙이 어느 정도 차이가 있는지를 확인하는 것은 인권적 정보자원관리 체계 구축을 위해 필수적인 과정이다. 이를 통해 정부 정보자원의 인권적 관리 프레임을 구축 시 조직과 그 구성원의 관점에서 어떤 부문이 강화되거나 조정되어야 하는지를 확인하고 이에 기반을 둔 정보자원관리 원칙을 도출할 수 있는 것이다.

이를 위해서 본 장에서는 중앙 및 지방 정부의 각 부서별로 정보자원의 직접적 관리를 담당하는 정보부서 및 현업부서 공무원들을 대상으로 정보자원의 관리 실태에 관한 설문을 실시하고 그 결과를 분석하였다.

1) 조사 대상 및 방법

정부 조직의 정보자원 관리 실태 분석이 연구의 초점이므로 중앙 및 지방정부의 부서를 분석 단위로 하여, 부서 단위에서 이뤄지는 개인정보 관리 실태에 대하여 조사하였다. 중앙 및 지방 정부의 부서들 중에서 개인정보 목록을 구축 및 관리를 주로 담당하고 있는 부서 리스트를 작성한 후, 국가인권위원회를 통해 공문 협조를 구하여 총 346개 과를 대상으로 온라인 설문지를 발송하였다.

총 346개 부서의 정보관리 담당자들 및 일반 현업부서 담당자들에게 발송한 온라인 설문지는 2011년 9월 말부터 10월 둘째 주까지 3주 이상 진행되었으며, 총 126개 부서로부터 응답을 받았다. 약 35%대의 수거율이었으나, 중앙 및 지방정부 전체를 대상으로 정보자원관리 실태에 관한 설문조사를 진행하였다는 점에서 의의가 크다. 특정 부처나 중앙정부 수준에서 진행되었던 기존 연구과는 달리, 중앙과 지방을 포괄한 정부 전 부서를 대상으로 하였다는 점에서 정부의 정보관리 실태를 보다 전반적으로 파악할 수 있을 것이다.

설문문항은 개인정보의 수집부터 폐기까지 각 단계별 관리 실태와 정부 정보관리의 효과성 및 위험성 등으로 구성되었으며 5점 척도의 선택문항들로 구성하였다(구체적인 문항은 부록 1 참조).

2) 표본의 특성

수거된 표본의 속성을 살펴보면 아래의 <표 7-1>와 같다. 총 126곳으로부터 답변을 받았으며 이 중 정보 부서로부터 90개가 현업 부서로부터 36개가 수거되었고, 중앙정부 소속 부서로부터는 27개, 지방정부 소속 부서로부터는 87개 등이 수거되었다.

업무 구분에 따라, 개인정보보호 및 정보화를 담당하는 정보부서가 전체 표본의 71.4%를, 일반 현업 부서는 28.6%를 구성하고 있으며 주로 정

보 부서를 관리 실태를 중심으로 파악되었다고 볼 수 있다. 각 부처에서 정보보호책임을 담당하는 부서에서 관리 실태에 관하여 응답한 만큼, 다른 부서에 비해 답변이 보수적, 긍정적으로 이루어졌을 가능성을 고려해야 할 것으로 보인다.

또한 중앙-지방 정부 구분에 따라서, 중앙정부 소속 부서가 21.4%를, 지방정부 소속 부서가 69%를 차지하고 있으며 중앙-지방 소속 구분에 응답하지 않은 설문이 약 9.5%으로 나타났다. 지방 정부 소속 부서에 편중된 구성으로 보이나 모집단 자체가 중앙보다 지방의 비중이 더 크다는 점을 고려하면 추출된 표본의 왜곡 우려는 크지 않을 것으로 보인다.

따라서 중앙정부 및 지방정부의 부서에서 벌어지고 있는 정보관리의 현 주소를 파악하기 위하여 진행된 설문조사는 총 126개의 중앙 및 지방의 정보관리 담당부서를 통해 확인되었으며 추출된 표본의 특성 상 일반화에 어려움이 있을 수 있으나 정부 전반의 포괄적 관리 실태를 확인할 수 있는 규모와 구성이라는 점에서 의의가 있다고 할 것이다.

<표 7-1> 표본의 특성

	중앙-지방 구분			업무 구분	
	중앙정부 소속 부서	지방자치단체 소속 부서	구분불가*	정보 부서	현업 부서
빈도	27개	87개	12개	90개	36개
%	21.4%	69%	9.5%	71.4%	28.6%
전체	총 126개(100%)				

주: *구분불가는 중앙정부와 지방자치단체의 구분이 불명확한 설문응답을 말하며 중앙과 지방을 비교하기 위한 분석에서는 제외하였음.

2. 정부 정보자원관리에 관한 실태 인식

설문조사를 통해 나타난 정부의 정보자원 관리 실태에 대한 응답 수준(n=126)은 평균 3점대로써 보통 수준으로 평가되었다. 앞서 언급하였듯이 정보관리를 담당하는 부서로 관리 실태에 대해 긍정적인 평가 및 위험 여부에 대해 보수적인 평가를 할 여지가 있다는 점을 감안한다면, 이러한 결과는 관리 실태를 다소 부정적으로 평가하는 편이라고 볼 수 있다. 대체로 응답 수준은 크게 부정하거나 긍정하기보다 보통 수준을 중심으로 집중되어 있다. 따라서 평균 점수에 대한 해석과 함께 항목간의 순위 비교에 초점을 두고, '높다/낮다'에 대한 1차적 해석보다는 경향성의 발견에 주목하여 특징을 찾아야할 것으로 보인다.

1) 정보관리의 효과성에 관한 인식

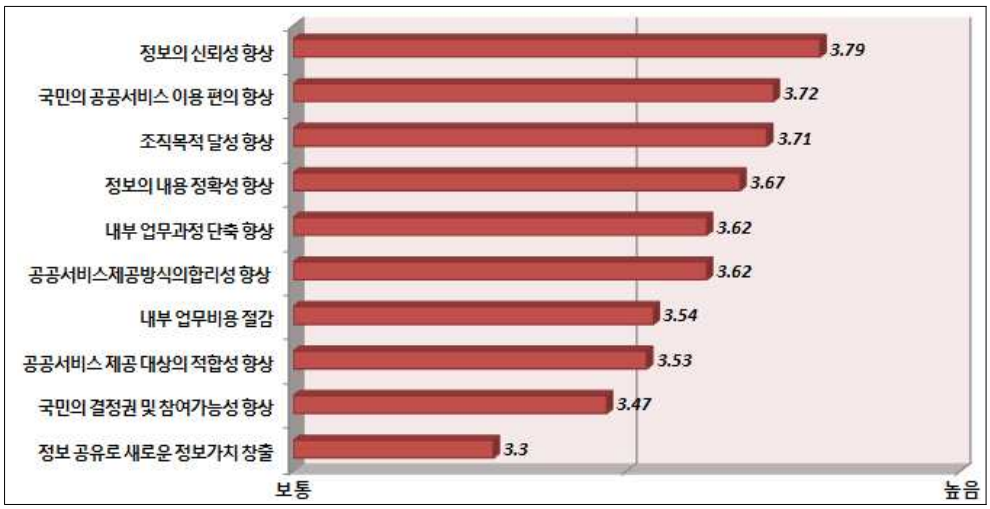
먼저, 정부 정보관리의 효과성에 관한 부서별 응답을 살펴보면, 정보자원의 관리를 통해 조직목표를 달성하는 것을 돕고 국민이 정부에 쉽게 접근할 수 있도록 하였으며 정부 정보의 신뢰성을 높였을 것이라는 점을 긍정적으로 꼽았다. 반면, 국민이 정부 정보관리 과정에 개입하거나 국민맞춤형 공공서비스를 받는 등의 적극적 효과는 상대적으로 낮게 평가하고 있었다. 일반적으로 정보관리를 통한 효과성을, 공공서비스 제공의 효율성, 이용편의성, 정보신뢰 향상, 조직목적 달성, 시민참여 등으로 다양하게 고려할 수 있는데, 그동안 우리 정부에서는 정보의 신뢰성, 이용편의성, 조직목적 달성에는 상대적으로 효과가 있었고 새로운 정보가치 창출, 시민참여 가능성, 고객맞춤형 서비스 제공 등은 효과가 상대적으로 낮았다는 것이다.

정보관리의 효과성에서 높은 점수를 보인 항목들을 구체적으로 살펴보면, '우리 부서는 정보관리 과정에서 보유하는 정보의 신뢰성을 높이고 있다'는 응답이 평균 3.79점으로 가장 높게 나타났으며 이어서 '우리 부서는 정보수집, 공유, 사용으로 국민의 공공서비스 이용편의를 향상

시키고 있다’ 는 응답이 평균 3.72점이며, ‘우리 부서는 정보수집, 공유, 사용을 통해 조직목적 달성을 돕는다’ 는 응답이 평균 3.71점이었다.

〈표 7-2〉 정보관리의 효과성에 관한 인식

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부서는 정보 관리 과정에서 보유하는 정보의 신뢰성을 높이고 있다	0 (0)	2 (1.6)	37 (29.4)	73 (57.9)	14 (11.1)	**3.79**
우리 부서는 정보 수집, 공유, 사용으로 국민의 공공서비스 이용 편의를 향상시키고 있다	0 (0)	6 (4.8)	37 (29.4)	69 (54.8)	14 (11.1)	**3.72**
우리 부서는 정보 수집, 공유, 사용을 통해 조직목적 달성을 돕는다	1 (0.8)	2 (1.6)	43 (34.1)	66 (52.4)	14 (11.1)	**3.71**
우리 부서는 정보 관리 과정에서 보유하는 정보의 내용 정확성을 높이고 있다	1 (0.8)	3 (2.4)	44 (34.9)	66 (52.4)	12 (9.5)	**3.67**
우리 부서는 정보 수집, 공유, 사용으로 내부 업무과정을 단축시키고 있다	1 (0.8)	4 (3.2)	50 (39.7)	58 (46)	13 (10.3)	**3.62**
우리 부서는 정보의 수집, 공유, 사용으로 보다 공공서비스 제공방식의 합리성을 높이고 있다	1 (0.8)	4 (3.2)	48 (38.1)	62 (49.2)	11 (9.7)	**3.62**
우리 부서는 정보 수집, 공유, 사용으로 내부 업무비용을 절감하고 있다	1 (0.8)	5 (4.0)	57 (45.2)	51 (40.5)	12 (9.5)	**3.54**
우리 부서는 정보의 수집, 공유, 사용으로 공공서비스를 제공받을 적합한 대상을 찾는다	1 (0.8)	6 (4.8)	56 (44.4)	51 (40.5)	12 (9.5)	**3.53**
우리 부서는 정보 수집, 공유, 사용 과정에서 국민의 결정권 및 참여가능성을 높이고 있다	2 (1.6)	7 (5.6)	58 (46)	48 (38.1)	11 (8.7)	**3.47**
우리 부서는 다른 부서, 부처, 민간기관 등과의 정보 공유로 새로운 정보가치를 창출시키고 있다	2 (1.6)	15 (11.9)	61 (48.4)	39 (31)	9 (7.1)	**3.3**



반면, 상대적으로 낮은 점수를 보인 항목으로는, ‘우리 부서는 다른 부서, 부처, 민간기관 등과의 정보 공유로 새로운 정보가치를 창출시키고 있다’는 응답이 평균 3.3점으로 가장 낮게 나타났으며, 이어서 ‘우리 부서는 정보 수집, 공유, 사용 과정에서 국민의 결정권 및 참여가능성을 높이고 있다’는 응답이 3.47점이며, ‘우리 부서는 정보의 수집, 공유, 사용으로 공공서비스를 제공받을 적합한 대상을 찾는다’는 응답이 3.53점이었다.

이는 현재 정부가 개인정보 관리를 통해서, 이전에 비해 국민들이 정부 정보에 대한 접근이 용이해졌고 정부 정보에 대한 신뢰가 높아졌을 것이며 정부 스스로도 조직목표 달성에 도움을 주었다고 자체적으로 실태 인식하는 것이며, 반면에 아직까지는 국민의 자기정보결정권이나 정보 활용을 통한 새로운 가치 창출 등 적극적 정보관리 단계에는 이르지 못한 것으로 평가하고 있는 것이다.

2) 정보관리상의 참여가능성에 관한 인식

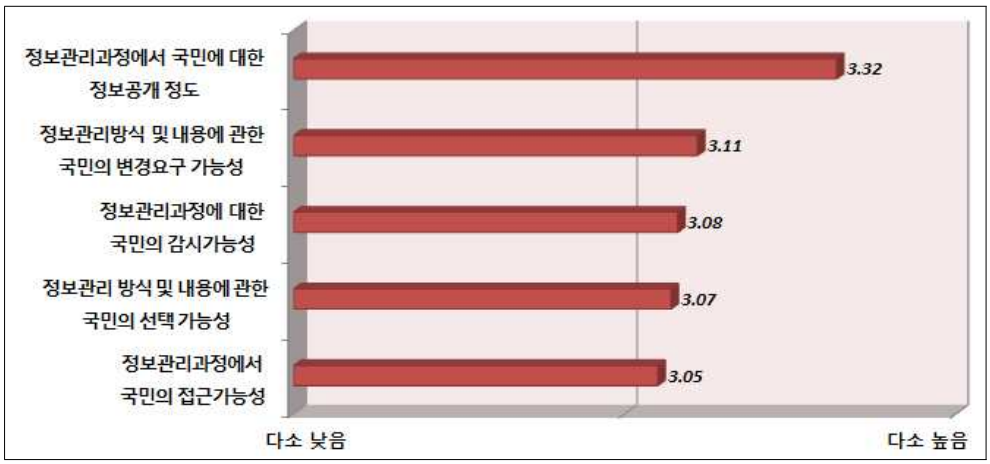
최근 정부의 개인정보관리에 대해 국민의 참여 및 통제가 강화되어야 한다는 사회적 요구를 고려할 때, 정부 내부에서는 현재 정보관리 과정상 국민의 참여가능성을 어느 정도로 평가하고 있는지를 살펴볼 필요가 있다. 국민의 참여가능성이란 소극적 측면에서 볼 때 국민의 참여는 접근가능성, 정보공개정도, 감시가능성 등이며 적극적 측면에서는 정보 내용에 대한 국민의 수정요구 가능성, 선택가능성 등으로 볼 수 있다.

조사 결과, 전반적인 참여가능성은 보통 수준이라고 평가하면서 항목별로는 국민에 대한 정보공개, 정보관리 방식 및 내용에 관한 변경 요구 가능성을 상대적으로 높게 생각하고 있었다. 반면, 부처의 정보관리 과정에 국민의 접근 가능성, 정보관리 방식 및 내용에 관한 선택 가능성을 상대적으로 낮게 인식하고 있었다. ‘현재 우리 부처의 정보관리 과정에서 국민에 대한 정보공개 정도’에 관한 질문에는 평균 3.32점으로 응답하여 가장 높게 인식하였으며 ‘현재 우리 부처의 정보관리 과정에서 국민의

접근가능성’에 관한 질문에는 평균 3.05점으로 가장 낮게 인식하였다. 이는, 신청된 정보는 절차에 따라 공개되고 있다는 점에서 보다 긍정적으로 평가하는 반면, 국민들이 정보에 접근하기 위한 절차 및 과정은 상대적으로 용이하지 않을 것으로 평가한다고 해석할 수 있을 것이며, 전체적으로 국민의 적극적 참여가능성은 낮다고 평가하고 있었다.

〈표 7-3〉 정보관리의 국민 참여가능성에 관한 인식

진 술 문	매우 낮다	낮다	보통 이다	높다	매우 높다	평균
현재 우리 부처의 정보관리 과정에서 국민에 대한 정보 공개 정도	1 (0.8)	9 (7.1)	74 (58.7)	33 (26.2)	9 (7.1)	**3.32**
현재 우리 부처의 정보관리 방식 및 내용에 관한 국민의 변경 요구 가능성	1 (0.8)	17 (13.5)	82 (65.1)	19 (15.1)	7 (5.6)	**3.11**
현재 우리 부처의 정보관리 과정에 대한 국민의 감시 가능성	1 (0.8)	19 (15.1)	80 (63.5)	21 (16.7)	5 (4)	**3.08**
현재 우리 부처의 정보관리 방식 및 내용에 관한 국민의 선택 가능성	2 (1.6)	18 (14.3)	82 (65.1)	17 (13.5)	7 (5.6)	**3.07**
현재 우리 부처의 정보관리 과정에서 국민의 접근 가능성	5 (4)	19 (15.1)	75 (59.5)	19 (15.1)	8 (6.3)	**3.05**



3) 정보관리의 위험성에 관한 인식

현재 정부의 정보관리 실태가 얼마나 우려할 만한 수준인가에 대해 정

부 각 부서 스스로는 어떻게 평가하고 있는지를 살펴볼 필요가 있다. 이는 특히, 현재 정부의 정보관리 안전성에 대한 사회적 우려가 높아지고 있는 상황에서 정부와 사회의 인식상의 괴리를 파악할 수 있다는 점에서 중요할 수 있다.

이를 위해 국민의 프라이버시 침해가능성, 국민 감시가능성, 운영상의 불투명성, 보안사고의 위험, 잘못된 내용으로 인한 피해, 오남용으로 인한 피해, 공유상의 사고위험 등 다양한 측면에서 어느 정도 위험 수준에 있다고 여기는지 질문하였다.

조사결과, 정부 부서들은 전반적으로 정보관리의 위험성을 크게 인지하지 못하고 있는 상태로 나타났지만, 정부가 국민의 프라이버시를 침해할 가능성을 다른 위험성에 비해 가장 높게 꼽고 있었다. 프라이버시 침해가능성에 대한 질문에 평균 2.63점으로 응답하고 있어 가장 높은 수준이었으며 이어서 국민의 접근 가능성이 낮은 불투명한 운영을 2.49점으로, 국민에 대한 감시가능성을 2.46점으로 응답하여 이러한 분야에 대한 위험성을 높게 꼽았다. 반면, 정보오류로 인한 국민의 피해에 대해서는 평균 2.21점으로 위험성 수준이 가장 낮다고 응답하였고 이어서 정보 오남용 등으로 인한 피해, 정보공유 과정상의 정보유출 등의 위험성을 상대적으로 낮게 인식하고 있었다.

이러한 결과는 현재 정부 정보관리상의 위험에 대한 사회적 우려와 비교할 때, 전반적으로 사회의 우려와 괴리되는 인식수준으로 볼 수 있지만 국민 프라이버시 침해에 대한 위험성은 공무원들 역시 우려하고 있는 것이었다. 그러나 프라이버시 침해에 대해서는 우려하고 있지만, 정보내용의 오류나 정보유출에 대한 위험성 인식은 상대적으로 낮은 수준으로 나타났는데 정부의 정보유출 사고가 증가하고 있으며 정보내용의 오류를 수정하기 위한 특별한 내부 조치가 없음을 고려할 때, 이러한 인식은 현 실태와는 어느 정도 괴리되고 있다고 볼 수 있을 것이다.

〈표 7-4〉 정보관리의 위험성에 관한 인식

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
현재 우리 부서의 정보 수집 및 생성 수준은 국민의 프라이버시를 침해할 가능성이 있다	9 (7.1)	56 (44.4)	39 (31)	17 (13.5)	5 (4)	**2.63**
현재 우리 부서의 정보 관리는 국민의 접근이 어려워 불투명하게 운영될 가능성이 있다	13 (10.3)	54 (42.9)	45 (35.7)	12 (9.50	2 (1.6)	**2.49**
현재 우리 부서가 보유하고 있는 정보를 통해 국민에 대한 감시가 가능하다	20 (15.9)	46 (36.5)	44 (34.9)	14 (11.1)	2 (1.6)	**2.46**
현재 우리 부서는 정보가 제때 폐기 되지 않아 국민이 피해를 볼 수 있는 잠재적인 위험이 있다	18 (14)	62 (49.2)	35 (27.8)	11 (8.7)	0 (0)	**2.31**
현재 우리 부서는 개인정보 유출, 분실, 도난 등 보안 사고의 위험이 있다	18 (14.3)	67 (53.2)	31 (24.6)	9 (7.1)	1 (0.8)	**2.27**
현재 다른 부서 및 부처와의 정보 공유 과정에서 정보유출 및 오남용 등 사고의 위험이 있다.	20 (15.9)	63 (50)	35 (27.8)	7 (5.6)	1 (0.8)	**2.25**
현재 우리 부서는 목적 외 정보 이용, 정보의 오남용 등으로 국민이 피해를 받을 위험이 있다	24 (19)	62 (49.2)	29 (23)	9 (7.1)	2 (1.6)	**2.23**
현재 우리 부서가 보유하고 있는 정보 중 잘못된 내용으로 인해 국민이 피해를 받을 위험이 있다	26 (20.6)	58 (46)	34 (27)	6 (4.8)	2 (1.6)	**2.21**

4) 정보관리 체계에 관한 인식

정부가 정보자원을 어떠한 체계적 구조로 관리하고 있는지는 정보관리의 기본적 속성을 결정지을 수 있다는 점에서 중요하다. 따라서 현재 정부 정보관리 체계의 집권성, 자율성, 공식성 등 구조적 차원의 특징이 무엇인가를 살펴볼 필요가 있다.

조사결과는 현재 정부의 정보관리 체계는 부처를 중심한 운영체계로서, 부서별 자율성은 낮은 편이고 부서 간 조정 체계 역시 미흡한 편으로 볼 수 있었다. 한편, 법제나 절차상의 부족 및 혼란은 그다지 높지 않게 나타났다.

우선, 집권적 관리체계 측면에서, 전 부처를 포괄하는 중앙집권적 운영 여부, 부처별 책임운영 여부, 부서별 책임운영 여부를 각각 질문한 결과, 부처별 책임으로 정보가 관리되고 있다는 응답이 평균 3.81점으로 가장 높게 나타났다. 이어서 부서별 책임으로 운영된다는 응답이 3.75점, 전 부처 포괄적 운영이라는 응답은 3.27점 순이었다. 이는 전 부처를 포괄하는 중앙관리적 운영체계가 구축되지 못했음을 보여주며, 우리 정부의 정보관리 기본 단위는 현재 부처가 되고 있는 것이다.

<표 7-5> 정보관리 체계에 대한 인식: 집권성

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리나라 정보 관리는 **부처별** 책임으로 운영되고 있다	0 (0)	8 (6.3)	27 (21.4)	72 (57.1)	19 (15.1)	**3.81**
우리나라 정보 관리는 **부서별** 책임으로 운영되고 있다	1 (0.8)	10 (7.9)	27 (21.4)	70 (55.6)	18 (14.3)	**3.75**
우리나라 정보 관리는 **전 부처**를 포괄하는 중앙집권적으로 운영되고 있다	2 (1.6)	25 (19.8)	48 (38.1)	39 (31)	12 (9.5)	**3.27**
우리 부처에는 정보 관리 과정에서 발생하는 부서 간 문제를 조정하는 체계가 있다	4 (3.2)	34 (27)	46 (36.5)	35 (27.8)	7 (5.6)	**3.06**
우리 부처의 경우 부서별로 전담하는 정보가 따로 구별되어 관리되고 있다	1 (0.8)	10 (7.9)	25 (19.8)	73 (57.9)	17 (13.5)	**3.75**

한편, 부처 내에서 부서별로 전담 정보가 어느 정도 구별되어 있는가에 대한 질문에는 평균 3.75점으로 응답하고 있어 대체로 부서별 전담관리 체계로 운영됨을 알 수 있었다. 반면, 부처 내에 정보관리 과정상 발생하는 부서 간 갈등을 조정하는 체계가 어느 정도 구축되었는가에 대해서는 이보다 낮은 3.06점으로 응답하고 있었다. 즉, 부처 내에서 부서별로 구분된 정보를 담당하고 있지만 이들 간의 문제가 발생할 경우 부처 내에서 적절하게 조정할 수 있는 공식 체계는 미흡한 수준으로 평가되는 것이었다.

또한 자율적 관리체계 측면에서도, 역시 부처 중심의 관리 체계가 확인되고 있었다. 정보의 수집, 공유, 이용, 폐기에서 부서와 부처로 어느 정도 자율적으로 결정할 수 있는지에 대한 질문에, 부처별 자율성이 높다는 응답이 평균 3.25점, 부서별 자율성이 높다는 응답이 2.74점으로 나타나 부처별 자율성이 더 높았다.

이러한 차원에서 볼 때, 현재 정부의 정보자원은 각 부처를 중심으로 관리되고 있으며 부처 간의 배타성을 조정할 전 정부적 관리 구조가 미흡하며 부처 내부에서도 부서간의 갈등 발생 시 이를 해결할 공식 구조가 존재하지는 않는 것이다.

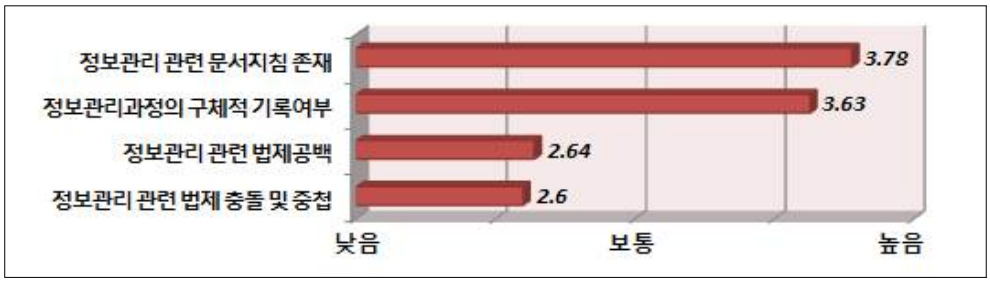
〈표 7-6〉 정보관리 체계에 대한 인식: 자율성

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 **부처**는 정보의 수집부터 공유, 저장, 이용, 폐기 등에 관해 자율적으로 결정할 수 있는 재량이 많다	3 (2.4)	26 (20.6)	46 (36.5)	39 (31)	12 (9.5)	**3.25**
우리 **부서**는 정보의 수집, 공유, 이용, 폐기 등에 관해 자율적으로 결정할 수 있는 재량이 많다	9 (7.1)	42 (33.3)	52 (41.3)	19 (15.1)	4 (3.2)	**2.74**

한편, 공식화된 관리체계 측면을 보면, 정보관리에 관한 구체적인 문서 지침 존재 여부, 구체적 기록관리 정도, 법제 간 충돌과 중첩 정도, 법제의 공백 정도 등을 통해 확인한 공식화 수준은 보통 수준으로 평가되고 있었다. 정보관리의 기준이 되는 구체적인 문서 지침이 있다는 응답이 평균 3.78점, 정보관리 과정이 구체적으로 기록 및 관리되고 있다는 응답인 3.63점으로 응답하고 있어 정보관리가 상대적으로 공식화된 편으로 평가하였다. 또한 정보관리 과정에서 관련 법제의 공백으로 문제해결의 어려움이 있는가에 대해 2.64점, 법제간의 충돌과 중첩으로 혼란이 있는가에 대해 2.60점으로 부정적으로 나타났다.

<표 7-7> 정보관리 체계에 대한 인식: 공식성

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부처에는 정보 관리에 기준이 되는 구체적인 문서 지침이 있다	0 (0)	7 (5.6)	36 (28.6)	61 (48.4)	22 (17.5)	**3.78**
우리 부처의 경우 정보 관리 과정은 구체적으로 기록되고 관리 된다	0 (0)	9 (7.1)	45 (35.7)	56 (44.4)	16 (12.7)	**3.63**
우리 부처의 경우 정보 관리 과정에서 법제의 공백으로 문제해결의 어려움이 있다	10 (7.9)	45 (35.7)	53 (42.1)	16 (12.7)	2 (1.6)	**2.64**
우리 부처의 경우 정보 관리 과정에서 법제 간 충돌과 중첩으로 혼란이 있다	10 (7.9)	49 (38.9)	51 (40.5)	14 (11.1)	2 (1.6)	**2.60**



이 결과는 정부는 정부의 정보관리 과정이 상대적으로 법제나 절차에 따라서 운영되는 편이라고 평가함을 보여준데, 이는 현재 정부의 개인정보보호에 관한 법제가 모호하거나 중첩되어 있어서 프라이버시 침해 등

정보인권 상의 문제를 낳고 있다는 사회적 비판과는 다른 현실 인식으로 보여 진다. 이는 개인정보보호법제가 있으나 예외 규정이 많아서 자의적 관리의 우려가 높다고 비판하며 구체적이고 통일적인 법제의 마련을 주장하는 시민사회 및 학계와의 인식 충돌을 보이고 있는 것이다.

정부 부서의 경우, 개인정보보호를 위한 법제와 지침이 존재하고 있다는 점에서 법제상 공백이 있다고 여기지 않을 수 있고, 법제상의 충돌이 있더라도 이미 부처 내부에서 관행적으로 적용해온 해석기준이 받아들여지고 있다면 혼란을 느낄 여지가 적을 수 있다는 점에서 이러한 인식 차이를 해석해볼 수 있을 것이다.

5) 정보자원의 생애주기별 인식

아래에서는 수집 및 생성, 저장, 분배 및 공유, 이용, 폐기라는 정보자원의 생애주기에 따라 각 단계별로 정부 부서들의 관리 실태 인식 수준을 확인하였다.

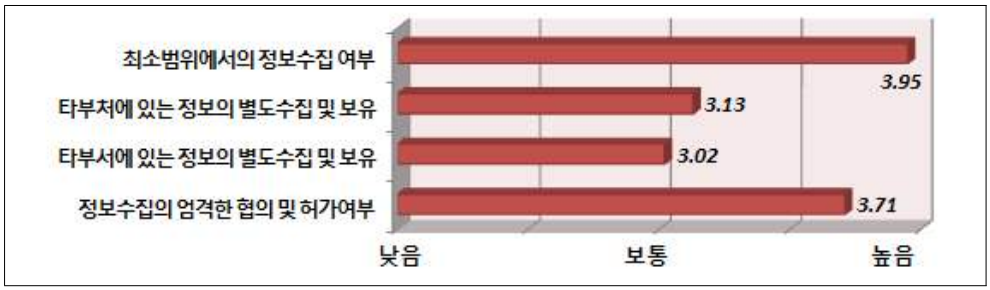
(1) 정보의 수집

먼저, 정보 수집 단계에 있어서 관리 상 강조되어온 바는, ‘최소한의 정보수집’, ‘책임 있는 정보수집’, ‘수집정보의 공개’, ‘정보주체의 동의’ 등으로, 업무에 필요한 최소한의 정보를 수집하고 중복하지 않는 효율적 수집을 지향하며 이 과정이 정보주체의 동의와 감시 아래 이뤄져야 한다는 것을 주요 내용으로 하고 있다.

조사결과, 업무에 필요한 최소한의 수집 및 보유에 대해서 평균 3.95점으로 응답하여 수집 분야에서는 상대적으로 가장 높은 점수를 보였다. 같은 정보를 다른 부처/부서가 가지고 있더라도 따로 수집 및 보유하고 있는가에 대해서는 부처의 경우 3.13점, 부서의 경우 3.02점으로 응답하여 부서보다 부처간의 정보수집의 배타성이 약간 더 높게 나타났다.

〈표 7-8〉 정보수집에 관한 인식: 수집최소성

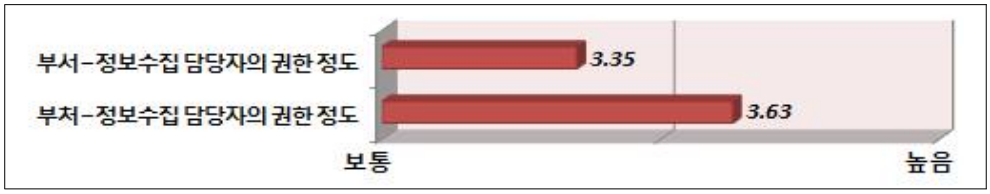
진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부서는 업무에 필요한 최소한의 범위에서 정보를 수집 및 보유하고 있다	1 (0.8)	2 (1.6)	25 (19.8)	72 (57.1)	26 (20.6)	**3.95**
다른 **부처**에서 같은 정보를 가지고 있더라고 우리 부처에서 따로 수집하여 보유한다	5 (4)	28 (22.2)	44 (34.9)	43 (34.1)	6 (4.8)	**3.13**
다른 **부서**에서 같은 정보를 가지고 있더라도 우리 부서에서 따로 수집 및 보유한다	9 (7.1)	28 (22.2)	45 (35.7)	40 (31.7)	4 (3.2)	**3.02**
우리 부서는 정보를 수집하는 과정에서 내부적으로 엄격한 협의 및 허가를 거친다	0 (0)	5 (4)	47 (37.3)	53 (42.1)	21 (16.7)	**3.71**



이는 앞서 정보관리 체계가 부처를 기본단위로 한다는 결과와 연결되는 실태 인식이다. 또한 정보수집 과정에서 내부적으로 엄격한 협의 및 허가를 거치는지에 대하여 평균 3.71점으로 응답하고 있어 상대적으로 수집상의 내부통제 절차에 따르고 있다고 평가하고 있었다.

〈표 7-9〉 정보수집에 관한 인식: 책임성

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 **부서**에는 정보 수집을 기획하고 책임지는 담당자의 권한이 크다	0 (0)	24 (19)	45 (35.7)	46 (36.5)	11 (8.7)	**3.35**
우리 **부처**에는 정보 수집을 기획하고 책임지는 담당자의 권한이 크다	1 (0.8)	15 (11.9)	29 (23)	65 (51.6)	16 (12.7)	**3.63**

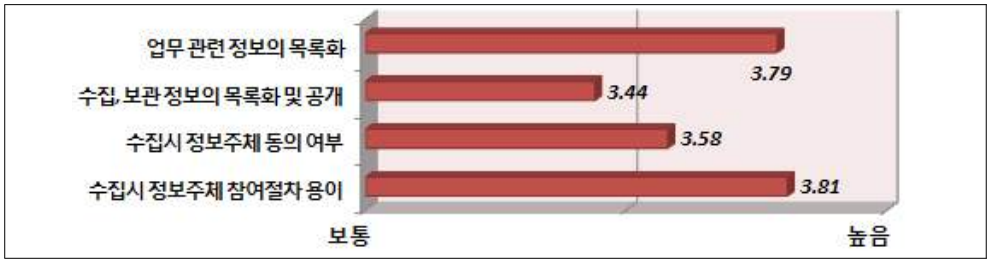


부처/부서에서 정보 수집 및 기획 담당자의 권한이 어느 정도인가에 대해 부처담당자의 권한은 3.63점, 부서담당자의 권한은 3.35점으로 응답하고 있어 정보수집에 있어서 담당자의 권한이 부서에 비해 부처 담당자의 권한은 상대적으로 더 큰 편으로 인식되었다. 이 역시 정보수집에서도 부처별로 운영 관리되고 있음을 보여주는 것이다.

정보수집의 공개성은 업무상 이용되는 정보가 목록화 되어 있는지, 그리고 구축된 목록이 어느 정도 공개되고 있는지를 의미한다. 부서 정보의 목록화 여부에 대한 응답 수준은 평균 3.79점으로 나타났으며, 목록의 공개 수준은 3.44점으로 나타났다. 목록화 수준에 대한 평가보다 목록공개 수준에 대한 평가가 더 낮게 나타나는 것으로 보아 목록화 된 정보에 비해 국민에게 공개되는 정보는 이보다 적은 것으로 평가되고 있었다.

<표 7-10> 정보수집 실태에 대한 인식: 공개성 및 참여성

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부서에서 업무상 이용되는 정보의 대부분이 목록으로 구축되어 있다	0 (0)	10 (23)	29 (23)	64 (50.8)	23 (18.3)	**3.79**
우리 부서에서 수집, 보관하는 정보의 목록은 국민에게 공개되고 있다	1 (0.8)	11 (8.7)	56 (44.4)	48 (38.1)	10 (7.9)	**3.44**
우리 부서는 정보를 수집하는 과정에서 정보주체의 동의를 구하고 있다	1 (0.8)	9 (7.1)	50 (39.7)	48 (38.1)	18 (14.3)	**3.58**
우리 부서는 정보를 수집하는 과정에서 정보주체의 참여 절차가 용이하다	0 (0)	4 (3.2)	37 (29.4)	64 (50.8)	21 (16.7)	**3.81**



또한 정보수집상 정보주체의 동의 및 참여에 대한 응답을 보면, 정보수집 과정에서 정보주체의 동의를 구하고 있는가에 대해 3.58점, 정보주체의 참여절차가 용이한가에 대하여 3.81점으로 나타났다. 정보수집상 정보주체의 동의나 참여 용이성을 약간 긍정하는 수준이며, 정보주체의 참여절차는 상대적으로 용이하지만, 정보주체에게 직접 동의를 구하는 것은 이보다 미흡한 것으로 평가되었다.

(2) 정보의 저장

정보의 저장 단계에서는 안전한 정보의 관리가 중심이 되는데 정보유출, 해킹 등을 대비하는 보안관리 체계와 기술적 조치 등이 마련되어 있어야 한다. 이에 대한 정부의 실태 인식은 전반적으로 정보의 보안 관리에 대해 상대적으로 긍정적 평가를 내리고 있어, 최근 연이은 정부의 개인정보유출 사고에 대한 사회적 우려와는 인식의 차이를 보여주었다.

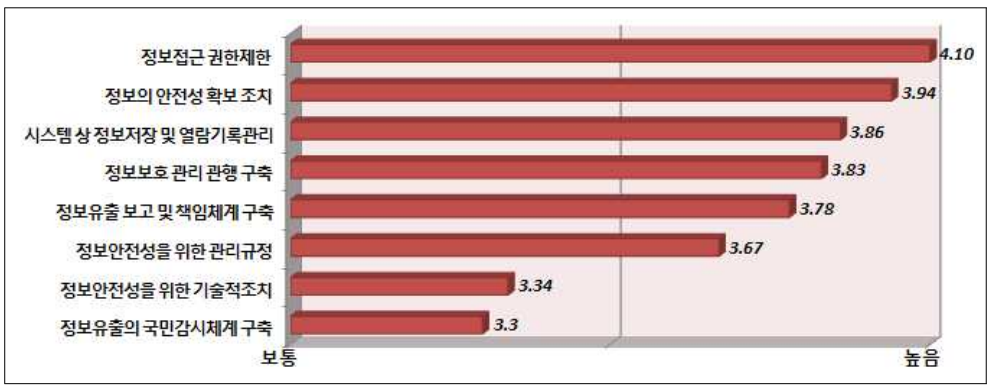
우선, 정보 접근 권한을 내부적으로 제한하는 수준에 대해 평균 4.10점으로 가장 높은 평가를 내리고 있었고, 정보저장 및 정보파일 송수신시 암호화는 3.94점, 정보저장 및 열람에 관한 기록의 시스템 상 관리는 3.86점 등으로 응답하였다. 그 외에도 정보보호 및 보안을 위한 관리관행, 책임체계, 기술적 조치 등도 각각 3.83점, 3.78점, 3.67점 등으로 나타났다. 이러한 결과는 응답의 대상자가 주로 정보 부서였기에 정보보안에 관한 직접적 책임과 관리를 담당하고 있어서 접근제한이나 암호화 등 기술 조치 등에 대해 보다 긍정적 평가를 할 수 있었을 것으로 보인다.

반면, 상대적으로 낮은 평가를 하는 분야는 정보유출에 대해 국민이 감시할 수 있는 체계의 구축으로, 정보유출에 대한 외부감시 체계는 미흡한 편으로 평가하였다.

즉, 정보의 저장 실태에서는 전반적으로 정보에 대한 내부적 접근권을 제한하거나 기술적 조치를 지키는 편으로 인식하지만 저장 실태를 외부에서 관리 감독할 수 있는 통제체계는 미흡한 수준으로 볼 수 있었다.

〈표 7-11〉 정보저장에 관한 인식

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부처에서는 정보에 접근할 수 있는 권한을 업무 담당자로 제한하고 있다	0 (0)	2 (1.6)	17 (13.5)	74 (58.7)	33 (26.2)	**4.10**
우리 부처는 정보저장 및 정보파일 송수신시 안전성 확보를 위한 조치(암호화 등)를 지키고 있다	0 (0)	4 (3.2)	30 (23.8)	61 (48.4)	31 (24.6)	**3.94**
우리 부처는 정보 저장 및 열람에 관한 기록을 시스템 상에서 관리하고 있다	0 (0)	6 (4.8)	32 (25.4)	62 (49.2)	26 (20.6)	**3.86**
우리 부처는 정보보호 및 보안을 위한 관리 관행이 구축되어 있다	2 (1.6)	5 (4)	26 (20.6)	73 (57.9)	20 (15.9)	**3.83**
우리 부처는 정보유출에 대한 내부 보고 및 책임체계가 구축되어 있다	0 (0)	8 (6.3)	36 (28.6)	58 (46)	24 (19)	**3.78**
우리 부처는 정보의 안전성을 위한 관리규정이 충분하다	0 (0)	7 (5.6)	44 (34.9)	58 (46)	17 (13.5)	**3.67**
우리 부처는 정보의 안전성을 위한 기술적 조치가 충분하다	1 (0.8)	8 (6.3)	41 (32.5)	61 (48.4)	15 (11.9)	**3.64**
우리 부처는 정보유출에 대해 국민이 감시할 수 있는 체계가 구축되어 있다	0 (0)	20 (15.9)	61 (48.4)	32 (25.4)	13 (10.3)	**3.30**



(3) 정보의 공유

정부는 부처 및 부서 간 정보의 공유를 통해서 정보관리의 효율성을 도모하는 한편, 국민들의 편의를 높이고자 하고 있다. 이런 측면에서, 부처 및 부서 간 정보의 공유 실태는 공유의 범위, 공유과정의 용이성, 공유절차, 공유과정의 통제 등의 측면에서 살펴볼 수 있다.

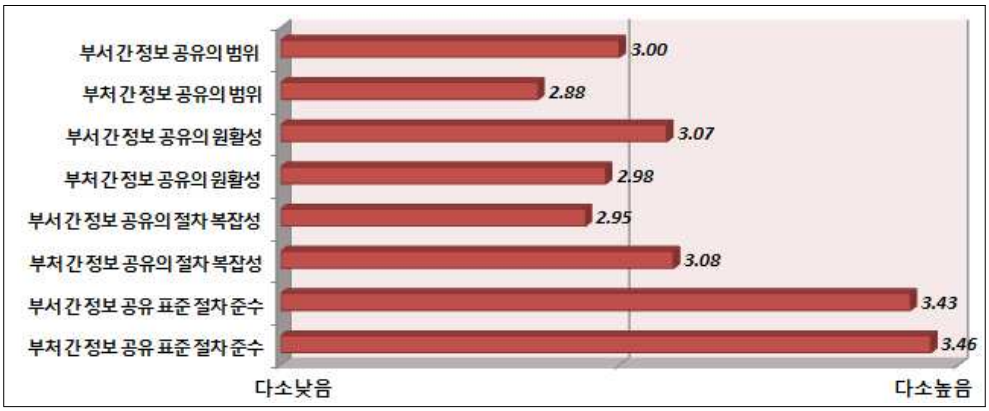
조사결과, 정부 부처 간 정보공유는 공유 범위 면에서도 부족하고 공유 절차상에서도 용이성이 미흡한 것으로 평가되고 있었다. 부처 간 공유범위가 넓은가에 대해 평균 2.88점, 부서 간의 공유범위가 넓은가에 대해서는 평균 3점으로 나타나 정보공유의 범위가 넓지 않다고 평가하였다. 특히 부서간의 공유에 비해 부처간의 공유 범위는 더욱 좁다고 평가하고 있어 앞서 정보관리체계와 수집단계에서 확인하였던 부처간의 배타성을 공유에서도 확인할 수 있었다.

공유과정이 원활한가에 대해서도 부서 간의 정보공유에 대해서는 3.07점으로 응답하였으나 부처간의 정보공유에 대해서는 2.98점으로 응답하고 있어 공유과정이 그다지 원활한 편으로 평가하지 않으면서 부처 사이의 공유는 더 어려움을 알 수 있었다. 공유절차가 복잡한가에 대한 질문에서는 부처 간은 3.08점, 부서간은 2.95점으로 응답하고 있어 공유절차는 역시 부처가 부서에 비해서는 절차가 더 복잡한 상태로 평가되고 있었다.

정보 공유를 위한 표준 절차가 어느 정도 준수되고 있는가에 대해서는 부서 간 정보공유를 위한 표준 절차 준수 정도를 3.43점, 부처 간은 3.46점으로 응답하여 부처/부서 간 큰 차이 없이 보통 수준의 실태 인식을 보여주었다.

<표 7-12> 정보공유에 관한 인식: 공유의 범위와 원활성

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
부서 간 정보 공유의 범위(공유 부서 수, 공유 정보 수 등)가 넓다	1 (0.8)	31 (24.6)	64 (50.8)	27 (21.4)	3 (2.4)	**3.00**
부처 간 정보 공유의 범위(공유 부처 수, 공유 정보 수 등)가 넓다	5 (4)	37 (29.4)	55 (43.7)	26 (20.6)	3 (2.4)	**2.88**
부서 간 정보 공유가 원활하게 이뤄지고 있다	1 (0.8)	27 (21.4)	62 (49.2)	34 (27)	2 (1.6)	**3.07**
부처 간 정보 공유가 원활하게 이뤄지고 있다	4 (3.2)	31 (24.6)	57 (45.2)	32 (25.4)	2 (1.6)	**2.98**
부서 간 정보 공유의 절차가 복잡하다	2 (1.6)	27 (21.4)	74 (58.7)	21 (16.7)	2 (1.6)	**2.95**
부처 간 정보 공유의 절차가 복잡하다	1 (0.8)	26 (20.6)	69 (54.8)	22 (17.5)	8 (6.3)	**3.08**
부서 간 정보 공유를 위한 표준 절차가 준수되고 있다	1 (0.8)	4 (3.2)	67 (53.2)	48 (38.1)	6 (4.8)	**3.43**
부처 간 정보 공유를 위한 표준 절차가 준수되고 있다	1 (0.8)	6 (4.8)	62 (49.2)	48 (38.1)	9 (7.1)	**3.46**



한편, 정보공유는 효율성과 이용편의성을 주요 목적으로 하지만 공유의 확대로 인하여 정보 유출, 정보 오남용, 프라이버시 침해가 증가할 수 있다는 우려가 동시에 존재한다. 따라서 이를 방지하기 위한 통제 체계, 공유 권한의 제한, 공유 절차의 엄격한 운영, 공유 과정에 대한 외부 통제 등이 요구된다. 이에 관한 실태 인식을 보면, 공유 시 정보유출과 오남용을 막기 위한 공유 권한자를 제한하고 있다는 평가가 평균 3.75점으로 가

장 높게 나타났다. 또한 정보유출과 오남용을 막기 위한 절차를 엄격하게 운영하고 있는가에 대해서 3.63점, 조치가 충분하다는 응답이 3.51점 등으로 나타나 정보 공유 상의 문제를 막기 위한 노력을 비교적 긍정적으로 인식하는 편이었다.

한편, 공유 과정을 기획 및 통제할 제도가 구축되어 있는가에 대해 부서의 경우 3.25점, 부처의 경우 3.21점으로 상대적으로 낮은 점수로 응답하고 있어, 정보 공유 과정의 일반적 통제 체계는 미흡한 것으로 평가하고 있다. 또한 정보공유 과정에서 국민에 의한 감시 및 통제 체계에 대한 인식도 3.25점으로 나타나 외부적 통제 체계 역시 미흡한 것으로 평가되고 있었다.

위의 결과는, 현재 정부가 정보공유의 범위를 확대시키고 절차를 개선해나가야 함과 동시에, 정보공유와 함께 증가할 유출과 오남용을 막기 위한 통제 절차를 동시에 마련해 나가야할 단계임을 보여준다고 할 것이다.

<표 7-13> 정보공유에 관한 인식: 공유과정의 통제 체계

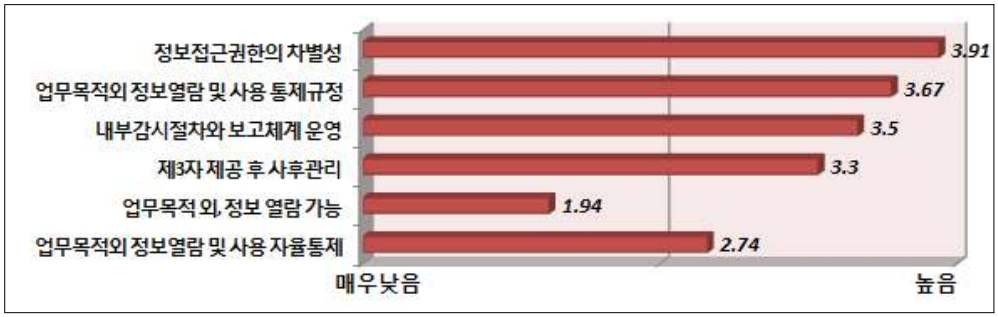
진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
정보 공유 시의 정보유출, 오남용 등을 막기 위해 공유 권한자를 제한하고 있다	1 (0.8)	5 (4)	35 (27.8)	68 (54)	17 (13.5)	**3.75**
정보 공유로 인한 정보유출, 오남용 등을 막기 위해 공유 절차를 엄격하게 운영하고 있다	2 (1.6)	8 (6.3)	41 (32.5)	58 (46)	17 (13.5)	**3.63**
정보 공유 시의 정보유출, 오남용 등을 막기 위한 조치가 충분하다	1 (0.8)	7 (5.6)	57 (45.2)	49 (38.9)	12 (9.5)	**3.51**
정보 공유의 내역이 기록 및 공개되고 있다	2 (1.6)	12 (9.5)	58 (46)	43 (34.1)	11 (8.7)	**3.39**
부서 간 공유 과정을 기획 및 통제할 제도가 구축되어 있다	1 (0.8)	15 (11.9)	66 (52.4)	39 (31)	5 (4)	**3.25**
부처 간 공유 과정을 기획 및 통제할 제도가 구축되어 있다	2 (1.6)	14 (11.1)	69 (54.8)	37 (29.4)	4 (3.2)	**3.21**
정보 공유 과정에서 국민에 의한 감시 및 통제 체계가 마련되어 있다	3 (2.4)	14 (11.1)	66 (52.4)	35 (27.8)	8 (6.3)	**3.25**

(4) 정보의 사용

정부의 정보사용 과정에서 주목해야하는 것은 목적 외 사용을 통제하고, 정보의 질 관리로서, 업무 외 목적으로 정보의 열람 등이 이뤄지지 않도록 통제하고 목적 외 사용이나 오남용을 막기 위한 관리체계가 운영되어야 한다는 것이다.

<표 7-14> 정보의 사용에 관한 인식: 목적외 사용 통제

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부서는 정보에 접근하는 권한이 업무관련성에 따라 차별적으로 부여된다	1 (0.8)	4 (3.2)	27 (21.4)	67 (53.2)	27 (21.4)	**3.91**
우리 부서에서는 업무 외 목적으로 정보를 열람 및 사용하는 것을 통제하는 관리규정이 구축되어 있다	1 (0.8)	8 (6.3)	39 (31)	62 (49.2)	16 (12.7)	**3.67**
우리 부서의 경우 정보의 목적 외 사용, 오남용을 막기 위한 내부 감시절차와 보고체계가 운영되고 있다	3 (2.4)	9 (7.1)	47 (37.3)	57 (45.2)	10 (7.9)	**3.50**
우리 부서는 정보를 외부위탁기관 등 제3자에게 제공한 후 그 사후관리를 하고 있다	7 (5.6)	20 (15.9)	36 (28.6)	54 (42.9)	9 (7.1)	**3.30**
우리 부서에서는 업무 외 목적으로 정보 열람이 가능하다	38 (30.2)	64 (50.8)	17 (13.5)	7 (5.6)	0 (0)	**1.94**
우리 부서에서는 업무 외 목적으로 정보를 열람 및 사용하는 것을 자율적으로 제한하는 관행이 존재한다	16 (12.7)	39 (31)	34 (27)	36 (28.6)	1 (0.8)	**2.74**



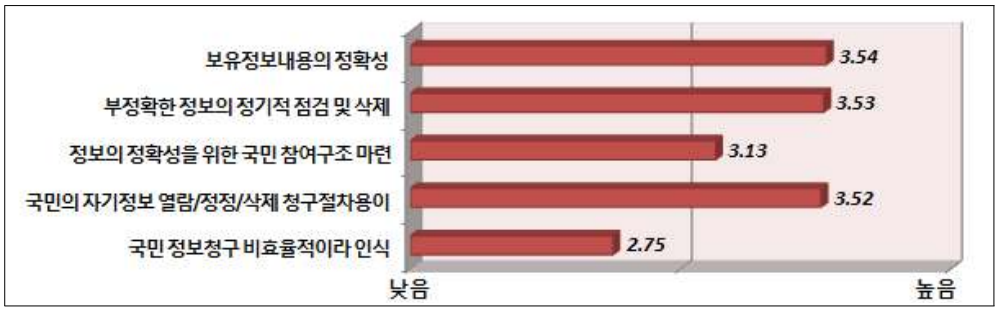
조사결과, 정보에 접근하는 권한을 업무 관련성에 따라 차별적으로 부여하고 있다는 응답이 평균 3.91점으로 가장 높게 나타났다. 정보사용상의 다른 측면에 비해서 접근의 제한적 관리는 비교적 잘 이뤄지고 있는 편으로 평가하였으며, 업무 외 목적으로 정보 열람 및 사용을 통제하는 규정이 있는가에 대해서 3.67점으로 나타나 통제 규정이 마련되어 있음을 알 수 있었다.

업무 외 목적으로 정보열람이 가능한가에 대한 질문에 1.94점으로 부정적으로 응답하고 있어 정보의 오남용에 대한 조직 차원의 관리 체계는 어느 정도 구축되어 있다고 평가하였다. 외부위탁기관 등 제3자에게 정보를 제공한 후 사후관리 수준에 대해서는 3.30점으로 응답자의 약 50.1%가 보통 이하의 사후관리 수준으로 응답하였다.

그러나 목적외 사용 등을 자율적으로 제한하는 관행이 존재하는가에 대해서는 2.74점으로 응답하고 있어 아직까지 부서 수준에서 자율적으로 관리하는 관행은 마련되어 있지 못한 것으로 평가하고 있었다. 정보를 업무 외 목적 등으로 사용하기 어렵도록 규정을 마련하고 있으나 이에 따른 자율적 관리 관행이 공무원들에게 안착되지 못했음을 보여준다고 할 수 있다.

<표 7-15> 정보의 사용에 관한 인식: 정보의 정확성 관리

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부서에서 보유하고 있는 정보의 내용은 오류 없이 정확하다	0 (0)	3 (2.4)	59 (46.8)	57 (45.2)	7 (5.6)	**3.54**
우리 부서는 부정확한 정보를 정기적으로 검점하여 정정 또는 삭제하고 있다	1 (0.8)	7 (5.6)	53 (42.1)	54 (42.9)	11 (8.7)	**3.53**
우리 부서는 정보의 정확성을 높이기 위해 국민이 참여하는 구조를 마련하고 있다	1 (0.8)	28 (22.2)	58 (46)	32 (25.4)	7 (5.6)	**3.13**
우리 부서는 국민이 자신에 관한 정보내용을 열람, 정정, 삭제 청구하는 절차가 용이하다	0 (0)	7 (5.6)	59 (46.8)	48 (38.1)	12 (9.5)	**3.52**
우리 부서는 정보에 대한 국민의 열람, 정정, 삭제 청구는 업무효율을 낮춘다	8 (6.3)	41 (32.5)	54 (42.9)	21 (16.7)	2 (1.6)	**2.75**



한편 정보 사용 상 또 다른 중요한 측면은 정보의 내용이 오류 없이 정확한 상태에서 사용되고 있는가 여부로, 이에 관한 응답을 보면 정보의 내용이 오류 없이 정확한가에 대해서 3.54점, 부정확한 정보를 정기적으로 점검하여 정정 및 삭제하고 있는가에 대해서 3.53점, 국민의 열람 및 정정 청구 절차의 용이성에 대해서는 3.52점 등으로 평가되었다. 정보의 정확성을 높이기 위해 국민이 참여하는 구조를 마련하고 있는가에 대해서는 3.13점으로 응답하고 있어 정보내용의 정정 및 삭제를 요구할 수 있는 국민 참여구조는 상대적으로 낮다고 인식되었다. 한편, 정보내용에 대한 국민의 열람, 정정, 삭제 등에 관한 청구가 업무의 효율을 낮추는가에 대한 질문에는 2.75점으로 부정하고 있었다. 즉, 대체로 국민의 참여가 업무 효율에 큰 장애를 주지 않을 것으로 인식함에도 앞서 살펴본 대로 정보내용에 대한 국민의 참여 구조는 상대적으로 부족한 것으로 평가되고 있었다.

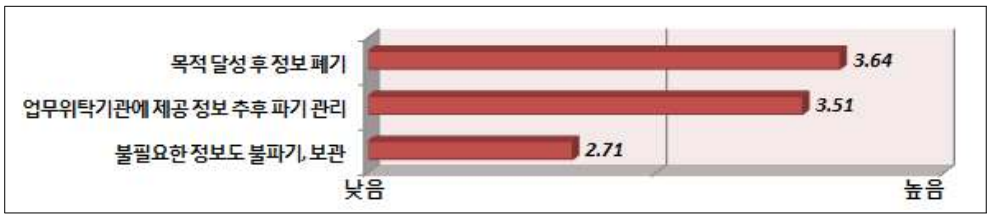
(5) 정보의 폐기

정보의 폐기 단계에서는 보유기간이 지나거나 목적 달성한 정보를 보관하지 않고 즉각 폐기하는 것이 중요하다. 정부 부처에서 정보는 오랫동안 부처의 권력 기반으로 인식되어왔기에, 정보를 확대, 확장하려는 경향이 강하지만 이를 합리적으로 폐기하려는 모습을 보이기 어렵다고 비판받아왔다.

정보의 폐기 실태에 대한 조사 결과를 보면, 정보의 보유기간이 지나거나 목적달성 한 후 정보를 규정대로 폐기하는가에 대해 평균 3.64점으로 평가하였다. 한편, 불필요한 정보라도 파기보다는 보관하려는 경향에 대해서는 2.71점으로 응답하고 있었는데, 앞서 규정대로 폐기하는가에 대한 응답보다 낮게 나타나고 있었는데, 이는 폐기가 규정된 상황에서는 폐기하는 편이지만 필요에 따르는 경우라면 폐기보다는 보관을 지향하는 경향이 있는 것으로 해석할 수 있었다.

〈표 7-16〉 정보의 폐기에 관한 인식: 폐기 실태

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부처는 정보의 보유기간이 지나거나 목적 달성 후 정보를 규정대로 폐기한다	2 (1.6)	6 (4.8)	46 (36.5)	53 (42.1)	19 (15.1)	**3.64**
우리 부처는 업무 위탁기관에 제공한 정보를 추후 파기하도록 관리한다	5 (4)	9 (7.1)	40 (31.7)	61 (48.4)	11 (8.7)	**3.51**
우리 부처는 당장 불필요한 정보라도 파기하기보단 보관한다	11 (8.7)	38 (30.2)	54 (42.9)	22 (17.5)	1 (0.8)	**2.71**



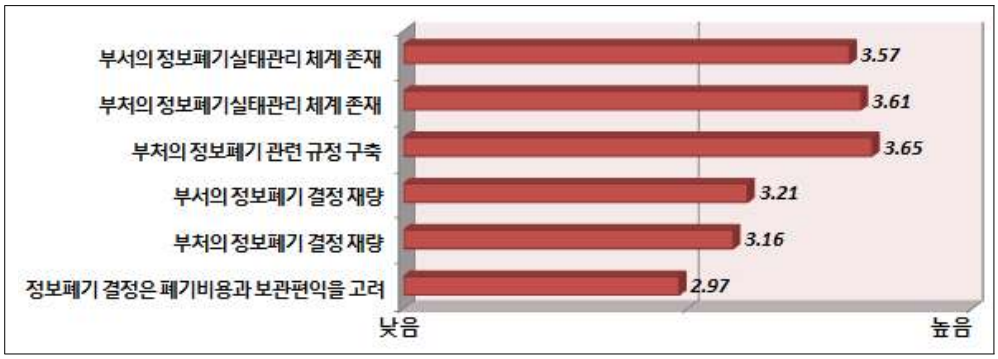
또한 업무 위탁기관에 제공한 정보를 추후 파기하도록 관리하는가에 대해서는 3.51점으로 응답하여 긍정하는 편으로 나타나, 최근 외부 위탁

기관으로 정보 제공 후 관리 부실 실태가 드러나고 있는 상황과는 괴리되는 인식으로 보여주었다.

한편 정보의 폐기를 관리하는 체계에 관한 질문에 대해, 부처 단위에서 정보폐기를 관리하는 체계가 존재한다는 응답이 3.61점으로 나타나 부서 단위 체계 인식인 3.57점보다 높게 나타났다. 폐기 관련 규정이 구축되어 있다는 인식이 3.65점 수준으로 나타났으며 정보 폐기에 관련된 부서 및 부처의 재량 수준은 3.21점 및 3.16점으로 상대적으로 높지 않게 인식하고 있었다. 또한 정보폐기 결정시에 폐기 비용이나 보관시의 편익 등을 고려할 수 있느냐는 질문에 2.97점으로 응답하면서 폐기 재량 수준을 낮게 평가하고 있었다.

<표 7-17> 정보의 폐기에 관한 인식: 폐기 체계

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 **부서**의 정보폐기 실태를 관리하는 체계가 존재한다	1 (0.8)	12 (9.5)	45 (35.7)	50 (39.7)	18 (14.3)	**3.57**
우리 **부처**의 정보폐기 실태를 관리하는 체계가 존재한다	0 (0)	13 (10.3)	43 (34.1)	50 (39.7)	20 (15.9)	**3.61**
우리 부처에는 정보폐기와 관련된 규정이 구축되어 있다	1 (0.8)	8 (6.3)	42 (33.3)	58 (46)	17 (13.5)	**3.65**
정보폐기 결정은 **부서**의 재량이 크다	4 (3.2)	25 (19.8)	44 (34.9)	47 (37.3)	6 (4.8)	**3.21**
정보폐기 결정은 **부처**의 재량이 크다	4 (3.2)	25 (19.8)	49 (38.9)	43 (34.1)	5 (4)	**3.16**
우리 부처의 경우 정보폐기 결정은 폐기비용과 보관 시 편익을 고려하여 결정할 수 있다	6 (4.8)	30 (23.8)	55 (43.7)	32 (25.4)	3 (2.4)	**2.97**

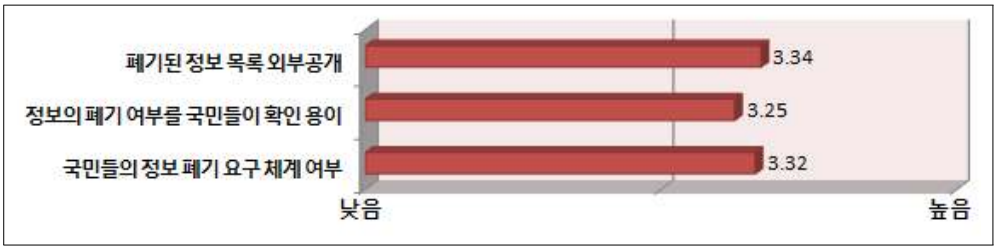


특히, 정보의 폐기와 관련해서는 불투명한 운영 가능성이 높기에, 규정에 따라 폐기한 목록을 구축하여 외부에 공개하거나 폐기 여부에 대한 국민의 확인을 위한 접근이 가능해야 하며 나아가, 국민이 정보폐기를 요구할 수 있는 가능성도 보장할 필요가 있을 것이다.

이에 대한 조사 결과, 부처에서 폐기된 정보 목록이 외부에 공개되고 있다는 응답이 3.34점 수준이었으며, 정보 폐기 여부의 확인 용이성 정도가 3.25점, 국민의 정보폐기 요구 체계 여부가 3.32점으로 응답하고 있어 전체적으로 정보폐기 상 국민의 통제 가능성은 상대적으로 낮게 나타나고 있었다.

<표 7-18> 정보의 폐기에 관한 인식: 외부 통제

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다	평균
우리 부처의 폐기된 정보 목록은 외부에 공개되고 있다	1 (0.8)	14 (11.1)	60 (47.6)	43 (34.1)	8 (6.3)	**3.34**
우리 부처의 경우 정보의 폐기 여부를 국민들이 확인하기 용이하다	1 (0.8)	18 (14.3)	63 (50)	36 (28.6)	8 (6.3)	**3.25**
우리 부처에는 국민들이 정보 폐기를 요구할 수 있는 체계가 있다	0 (0)	13 (10.3)	70 (55.6)	33 (26.2)	10 (7.9)	**3.32**

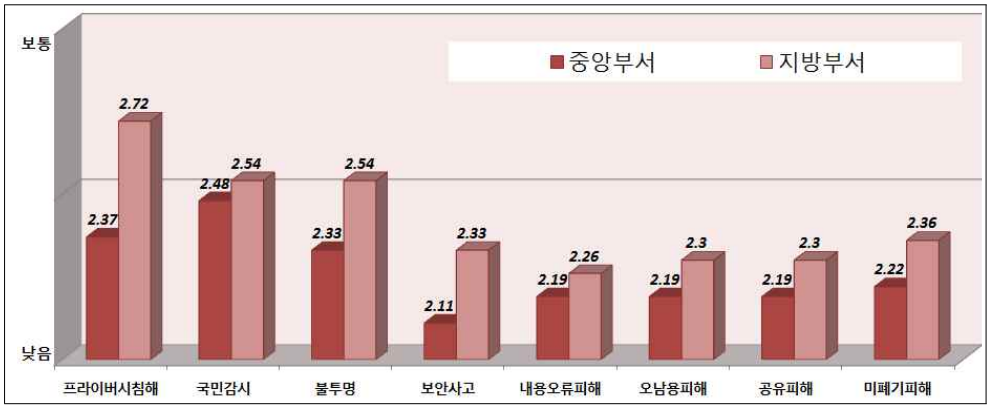


3. 중앙부서 및 지방부서 간 인식 차이

정보관리에 관한 중앙정부와 지방정부 사이의 인식 차이가 존재하는가를 살펴본 결과, 정보관리의 위험성과 참여가능성 등에서 인식의 차이를 발견할 수 있었다.

<표 7-19> 정보관리의 위험성에 대한 인식 비교: 중앙 vs. 지방

	프라이버시 침해	국민 감시	불투명	보안 사고	내용오류 피해	오남용 피해	공유 피해	불폐기 피해
중앙 부서	2.37	2.48	2.33	2.11	2.19	2.19	2.19	2.22
지방 부서	2.72	2.54	2.54	2.33	2.26	2.30	2.30	2.36



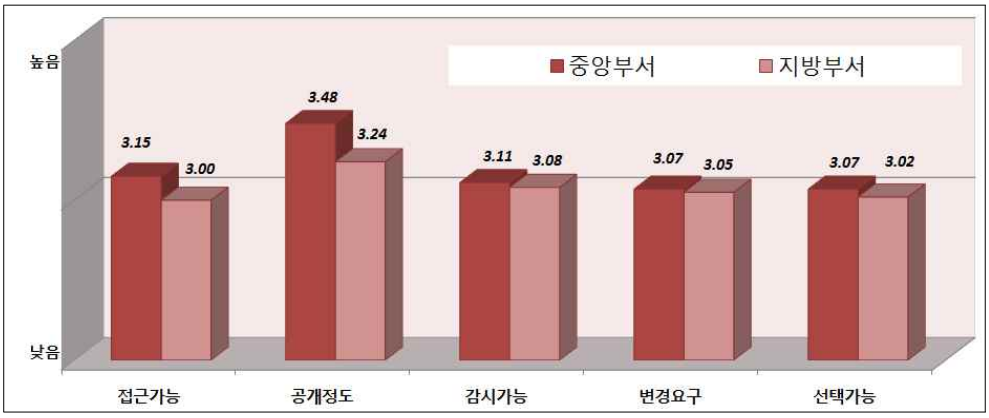
먼저, 정보관리의 위험성에 대해 지방 부서들이 중앙 부서들에 비해 더 위험하다고 평가하는 경향이 나타났다. 위의 <표 7-19>에서 보듯, 지방정부의 부서들은 프라이버시 침해, 국민에 대한 감시가능성, 불투명한 관리, 보안사고의 우려, 내용오류로 인한 피해, 오남용으로 인한 피해, 공유과정상 피해, 미폐기로 인한 피해 등 위험성 전반에 대해서 중앙정부의 부서들에 비해 위험성이 더 높다고 평가하였다. 위험성 인식 순위는 국민의 프라이버시를 침해할 가능성을 가장 높게 꼽았고 국민 감시가능성, 불

투명한 관리 등으로 중앙정부의 부서들과 별다른 차이를 보이지 않았다. 즉, 중앙정부의 부서들에 비해 지방정부의 부서들이 국민의 프라이버시 침해 등 정보관리 실태의 문제를 더 심각하게 느끼고 있는 것으로 보아, 중앙정부 수준에 비해 지방정부 수준에서 이뤄지고 있는 정보관리 실태가 더 열악한 수준임을 짐작할 수 있다.

또한, 정보관리상의 참여가능성에 대한 인식에 있어서도 지방 부서들이 중앙 부서들에 비해 국민의 참여가능성이 낮다고 평가하는 경향을 보였다. 아래의 <표 7-20>에서 보듯이 국민의 접근가능성, 정보공개 정도, 국민의 감시가능성, 정보내용 및 방식의 변경 요구 가능성, 선택가능성 등 참여가능성 전반에 있어서 중앙 부서에 비해 지방부서의 평가가 일관되게 낮게 나타나고 있다. 이러한 결과 역시, 중앙 정부에 비해 지방 정부 수준에서 정보의 수집과 저장, 공유, 사용, 폐기 등 정보관리 과정을 폐쇄적으로 운영하면서 참여가능성이 상대적으로 낮을 수 있음을 보여주고 있다.

<표 7-20> 정보관리의 국민 참여가능성 인식 비교: 중앙 vs. 지방

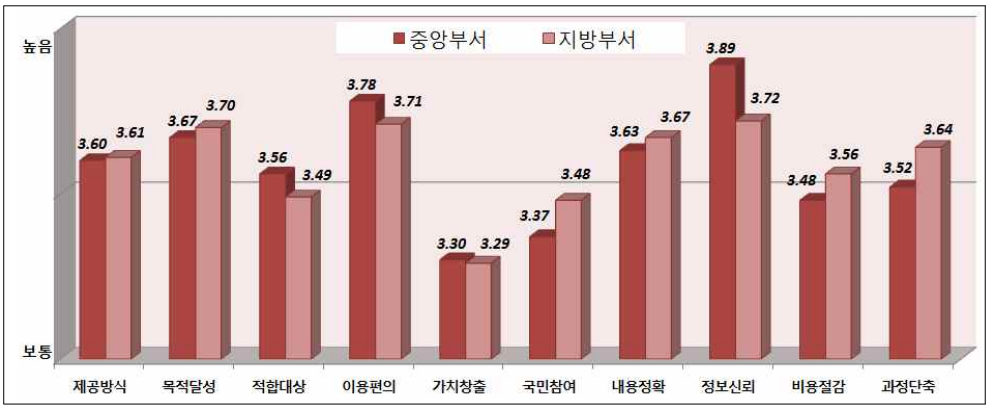
	접근가능	공개정도	감시가능	변경요구	선택가능
중앙부서	3.15	3.48	3.11	3.07	3.07
지방부서	3.0	3.24	3.08	3.05	3.02



한편, 정보관리의 효과성에 대해서는 지방과 중앙 부서 간의 인식 차이가 크게 나타나진 않았으나 지방부서가 중앙 부서에 비해 서비스제공방식의 합리성, 조직목적 달성 효과, 국민참여 가능성 향상, 정보의 내용 정확성 향상, 업무비용의 절감, 업무과정의 단축 등의 측면에서 더 긍정적으로 평가하고 있었다. 아래의 <표 7-21>에서 보듯이 중앙과 지방부서 사이 인식 차이는 크게 나타나지는 않았으나 위의 항목들에 비해서는 약간 더 긍정적으로 인식하고 있었다.

<표 7-21> 정보관리의 효과성에 관한 인식 비교: 중앙 vs. 지방

	제공 방식	목적 달성	적합 대상	이용 편의	가치 창출	국민 참여	내용 정확	정보 신뢰	비용 절감	과정 단축
중앙 부서	3.60	3.67	3.56	3.78	3.30	3.37	3.63	3.89	3.48	3.52
지방 부서	3.61	3.70	3.49	3.71	3.29	3.48	3.67	3.72	3.56	3.64



이러한 중앙과 지방부서 사이의 인식 차이는, 중앙에 비해 지방정부에서 정보관리 실태가 더욱 열악함을 의미하는 것일 수 있다. 정보관리 수준이 국민의 프라이버시 등을 침해할 위험성이 전반적으로 높다고 응답했다는 것은 그만큼 정보관리가 제대로 이뤄지고 있지 못함을 의미하며, 국민의 참여 가능성도 중앙에 비해 지방부서가 더 낮은 편으로 나타나고 있어서 국민의 참여를 통한 정보관리 과정 통제 역시 그다지 효과를 못보고 있다고 보여 진다.

그럼에도 불구하고 효과성에 대해 지방부서가 중앙 부서와 비슷한 수준의 효과성을 평가하거나 부분적으로 더 높은 효과성 평가를 하는 결과가 나타나는 것은, 정보관리의 수준이 열악한 지방 부서들은 정보관리의 위험성에도 예민하게 인식하지만, 그와 함께 효과성에 대해서도 더 민감하게 느낄 수 있음을 의미한다. 열악한 정보관리 실태로 인해 정보관리의 영향력에 대해 민감한 상태라면 효과성에 대해서도 빠르게 평가할 수 있기 때문이다.

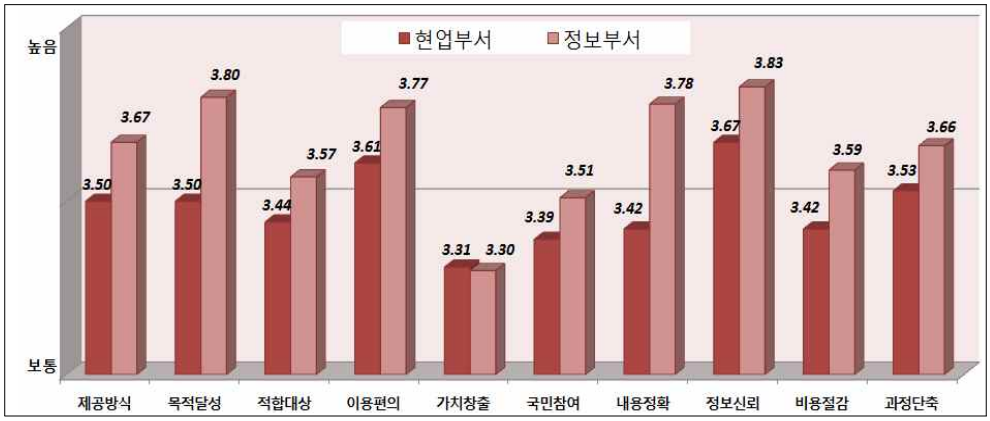
4. 정보부서 및 현업부서 간 인식 차이

정보부서와 현업부서 사이에는 정보관리 실태에 대해 어떠한 인식 차이가 나타나는가를 검토한 결과, 앞서와 같이 정보관리의 효과성, 참여가능성, 위험성 등을 다르게 평가하는 경향이 발견되었다.

먼저, 정보관리의 효과성에 관한 정보부서와 현업부서 사이 차이를 보면, 전체적으로 정보부서 담당자들이 정보관리의 효과성을 더 긍정적으로 평가하고 있었다. 서비스 제공방식의 합리성, 조직목적 달성, 서비스 적합대상 선택, 이용편의성, 국민 참여 가능성, 정보의 신뢰, 업무비용 절감효과, 업무과정 단축 효과 등 대부분의 효과성 측면에 대해 정보부서가 현업부서보다 더 긍정적인 실태평가를 내리고 있는 것이었다. 이 결과는 정보부서의 경우, 직접 부처의 개인정보 등을 맡아 처리하고 있어서 정보관리로 인한 효과를 직접 확인할 수 있어서 현업부서들에 비해서 정보관리로 인한 기대도 클 수 있다는 차원에서 설명할 수 있을 것이다.

<표 7-22> 정보관리의 효과성에 관한 인식 비교: 현업 vs. 정보

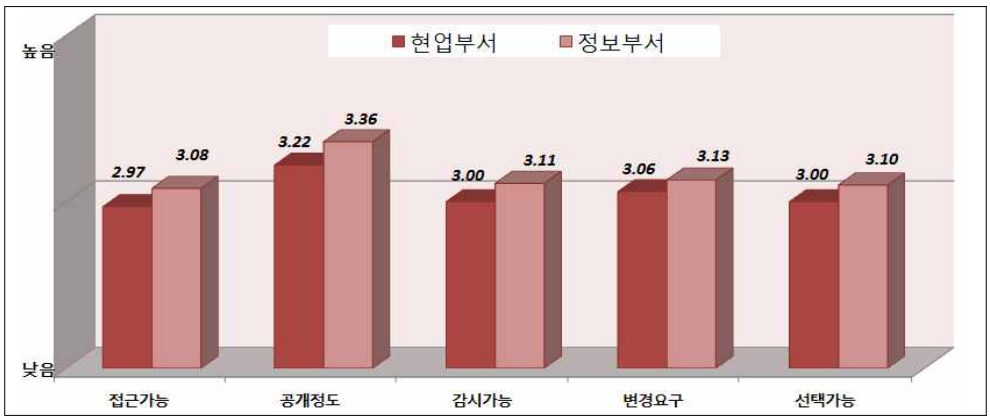
	제공 방식	목적 달성	적합 대상	이용 편의	가치 창출	국민 참여	내용 정확	정보 신뢰	비용 절감	과정 단축
현업 부서	3.50	3.50	3.44	3.61	3.31	3.39	3.42	3.67	3.42	3.53
정보 부서	3.67	3.80	3.57	3.77	3.30	3.51	3.78	3.83	3.59	3.66



국민의 참여가능성에 대한 인식에서도 정보부서와 현업부서의 인식 차이를 확인할 수 있다. 정보부서의 담당자들이 국민 참여의 가능성을 더 높게 인식하는 경향을 볼 수 있는데, 아래의 <표 7-23>에서 확인할 수 있듯이 정보부서의 경우, 현재 정보관리 과정에 국민이 참여할 수 있는 가능성에 대해 비교적 긍정하는 편으로 국민의 접근가능성, 정보의 공개정보, 국민의 감시가능성, 내용에 관한 변경요구 및 선택 가능성 등이 현업부서 공무원에 비해 약간 더 높게 나타나고 있었다.

<표 7-23> 정보관리의 국민 참여가능성 인식 비교: 현업 vs. 정보

	접근가능	공개정도	감시가능	변경요구	선택가능
현업부서	2.97	3.22	3.00	3.06	3.00
정보부서	3.08	3.36	3.11	3.13	3.10

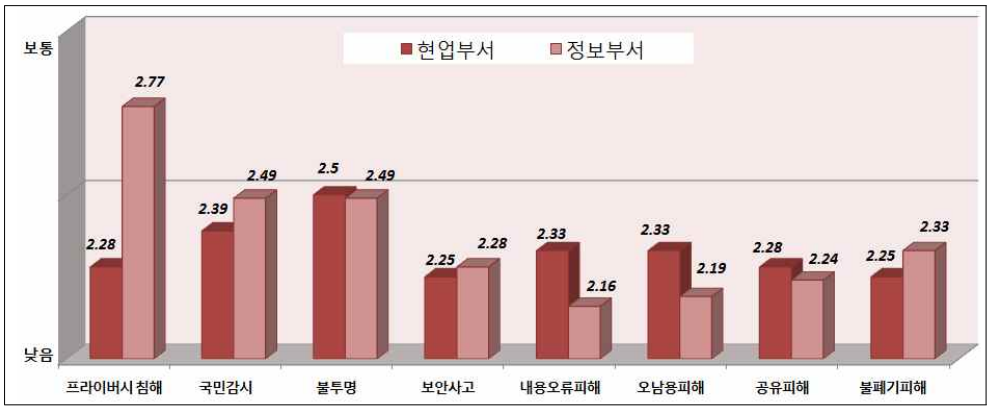


특히, 위험성에 관한 인식은 정보부서 담당자와 일반부서 담당자들 사이 차이를 보여주었다. 두드러진 차이점은 현재 정보관리 실태가 국민의 프라이버시를 침해할 가능성이 있는가에 대해 정보부서 담당자들이 일반부서 담당자들에 비해 더 높게 응답하였고 이는 통계적으로도 유의미한 차이($p<0.01$)를 보이고 있었다.

전체적으로 정보부서가 프라이버시 침해우려, 국민감시가능성, 보안사고의 우려, 정보 불폐기로 인한 피해의 위험성을 더 강하게 인식하고 프라이버시 침해 우려를 강하게 나타내고 있는 것이었다. 일반 현업 부서의 경우, 정보운영의 불투명성, 내용오류로 인한 피해, 오남용 피해, 공유시 피해 등의 항목에서 약간 더 높은 우려를 표현하고 있었다.

<표 7-24> 정보관리의 위험성에 관한 인식: 정보부서 및 현업부서 차이

	프라이버시 침해	국민 감시	불투명	보안 사고	내용오류 피해	오남용 피해	공유 피해	불폐기 피해
현업 부서	2.28	2.39	2.5	2.25	2.33	2.33	2.28	2.25
정보 부서	2.77	2.49	2.49	2.28	2.16	2.19	2.24	2.33



이 결과는 앞서 효과성 및 참여가능성에서 정보부서 담당자들의 인식이 상대적으로 높게 나온 것과 비교할 수 있는데, 정보부서 담당자들이 현재 정보관리의 효과성 및 참여가능성에 대해 상대적으로 높게 인식하면

서도 그 관리실태 상의 위험성을 동시에 높게 인식하고 있는 것이다.

즉, 정부가 정보관리를 통해서 다양한 효과를 낳고 있지만 그 현실적 관리 실태는 국민 프라이버시 침해의 가능성이 여전히 높은 것으로 평가하는 것으로, 현재 정보관리 과정에 대한 기대와 우려를 동시에 품고 있는 단계로 볼 수 있었다.

5. 종합분석

<표 7-25> 정부의 정보자원관리 실태 인식상 특징

구 분	특 징	
효과성 및 위험성	- 조직목표달성, 국민이용편의성 등 높게 평가 - 사회적 우려와 괴리된 실태 인식 수준; 낮은 위험 인식 - 프라이버시 침해에 대한 우려	
참여가능성	- 국민 참여를 통한 외적 통제 체계의 미흡: - 정보공개 수준은 높지만 접근절차와 적극적 참여보장 미흡 - 참여가 효율을 낮추지 않는다고 인식 - 국민의 적극적 참여 구조는 부족	
정보관리 체계	- 부처별로 분리된 배타적 관리 체계 - 범부처적 정보관리 통합조정 체계 미흡 - 미비한 법제에 대한 낮은 문제인식; 중첩 및 모호한 규정에 대한 부처의 관행적 적용 기준 존재	
정보관리 단계별	**수집/생성**	- 부처별 수집관리 구조 - 구축된 정보보다 낮은 수준의 공개
	저장	- 정보접근 권한 제한 - 외부 통제 체계의 미흡
	분배/공유	- 정보 공유의 범위와 절차상의 제약 - 정보 공유상의 문제점 대처 미흡
	사용	- 자율적 규제 관행의 미흡
	폐기	- 규정에 따른 폐기 but 규정 외 영역에서는 보관 경향; 명료한 규정의 필요성
정보관리 주체별	**중앙 vs. 지방 부서**	- 중앙 부서에 비해 열악한 지방부서의 관리 실태; 위험성 높고 참여가능성 낮음 - 중앙에 비해 지방에서 국민 접근의 어려움; 불투명, 절차와 과정의 어려움
	현업 vs. 정보 부서	- 정보부서가 현업 부서에 비해 프라이버시 침해 가능성 등 위험성 인식 높음

Ⅷ. 정부 정보자원의 인권적 관리 프레임[33]

정보자원생산주기의 각 단계에서 발생하고 있으며 또한 발생할 수 있는 정보인권 침해적 내용을 파악하고 정보인권 침해를 최소화하기 위한 방안을 검토하고 고안해야 한다. 정보의 생성 및 수집-저장-분배 및 공유-사용-폐기라는 일련의 정보자원생애주기에서 각 단계별 실태와 관리원칙에 기반을 둔 정보자원의 인권적 관리 프레임을 도출하려는 것이다. 즉 정보자원의 효율적 관리프레임과 인권적 관리 프레임을 결합한 새로운 프레임 도출을 시도하는 것이다.

앞서의 국내외의 법제 분석, 국내 갈등사례 분석, 정부 설문조사 결과 등에 근거하여 정부 정보자원의 인권적 관리 프레임을 제도적, 관리적, 기술적, 행태적 차원별로 설계해보고자 한다. 정보자원의 생애주기 단계별로 현재적 특징(As-Is)과 앞으로의 대안적 관리 방안(To-Be)을 제도-관리-기술-행태적 차원에서 제시함으로써 정부 정보자원의 인권적 관리가 지향하는 바를 보다 구체적으로 보여줄 수 있을 것이다.

1. 정보자원의 수집 및 생성

먼저, 현재 정부의 정보 수집 및 생성 단계에서 나타나는 대표적인 특징을 보면, 제도적 차원에서는 정보수집에 관한 포괄적 예외 조항이 적용될 수 있어서 정보보호를 위한 법규정을 무력화시키는 법적 혼란이 나타났다는 점이다. 관리적 차원에서는 중앙관리기구가 사전협의나 권고 수준의 권한에 머물면서 범부처적 정보관리 체계가 미약한 채 부처별로 배타적이며 불투명한 정보관리가 이뤄지고 있었다.

기술적 차원에서는 정보의 집적 및 통합으로 새로운 정보생성이 기술

33) 인권적 관리 프레임을 도출하는데 있어 본 연구진의 제안과 함께 장여경(진보네트워크), 이창범(한국법률문화연구원), A부의 전 정보화담당관 1인, B청의 전 정보화 관련 업무담당자 1인의 의견이 반영되었다.

적으로 가능해졌지만 이를 규제하는 특별한 규정이 없음으로써 사회적으로 우려를 낳았다. 한편 행태적 차원에서도 예외 규정의 무원칙적인 적용에 대해 문제로 인식하기보다 일종의 관행으로 여겨왔으며 정보수집 상의 주관적 판단이나 임의적 추가 수집에 대해서도 문제로 여기지 않았음을 알 수 있었다.

이러한 정보수집/생성 상의 관리 실태를 개선하는 주요 방향으로, 제도적 차원에서는 타 법에 의한 예외 조항 적용을 제한할 수 있도록 법제의 정비가 요구되며, 독일의 사례에서 살펴보았던 개인정보보호담당자와 같이 독립된 권한과 책임을 가지는 강한 내부통제 체계를 구축하는 것도 고려해 볼 수 있을 것이다.

관리적 차원에서도 범부처적 중앙관리기구를 강화하여 통합적이고 일관된 정보자원의 관리기반을 우선적으로 마련할 필요가 있다. 정보자원의 관리가 책임 있게 이뤄지려면 전 부처적으로 정보의 내용과 정보관리의 체계가 구축되어야 한다. 그 관리 중심이 범부처 기관이거나 부처별 조직일 수도 있지만 어떤 관리체계를 선택하든지 정보자원의 관리를 둘러싼 권한과 책임의 구조가 범 부처 차원에서 명료하게 정의되어야 할 것이다.

기술적 차원에서는 앞서 언급했던 정보생성에 관한 기술 규제 규정이 구체적으로 마련되어야 할 것이며, 행태적 차원에서는 정보수집 단계에서의 인권의식을 높여야할 필요가 보인다.

즉, 법제와 괴리된 수준의 현실 인식을 전환시키기 위한 조치가 필요하며, 예를 들어 정보관리의 입력 및 수집상의 자의성을 배제하기 위한 규정을 마련하거나 형사사법정보나 보건의료정보와 같이 정보수집자와 대상자가 대등하고 투명하기 어려운 비대칭적 상황을 수정하기 위한 조치가 마련되어야 할 것이다.

<표 8-1> 정부 정보자원의 수집생성과 관련된 인권적 관리 프레임

수집/생성		
	As-Is	To-Be
제도	- 수집에 대한 포괄적 예외 조항의 적용 가능 - 사전협의 수준의 중앙관리기구에서 법 개정으로 시정명령권 강화 - 개인정보영향평가제의 도입	- 예외 조항의 축소/명확화를 위한 법제 정리 - 독립적 개인정보보호책임자* 제도와 같은 내부통제 제도 강화 - 중앙관리기구의 권한 강화(시정명령권/과태료/허용취소) - 개인정보영향평가제도의 실천방안 구체화
관리	- 범부처적 정보관리 통합체계 미흡 - 부처별 배타적 정보관리 체계 - 관리지침의 약한 강제 - 법적 근거 없는 정보수집에 대한 제재 미비 - 정보공개 수준은 높지만 접근절차와 적극적 참여보장 미흡	- 구체적인 행동 매뉴얼 제시 - 불필요한 정보수집 제재 규정 마련 - 유효기간을 정한 수집 - 중앙관리기구의 사전 통제 강화
기술	- 통합DB을 통한 제3자의 정보수집 가능	- 정보통합으로 새로운 정보생성 규제
행태	- 미비한 법제에 대한 낮은 문제인식 - 정보수집자와 정보제공자 간의 대등하지 않은 관계(예:형사사법정보) - 추가정보를 수집하는 행위 - 정보생성의 불투명성	- 정보수집자와 수집대상의 대등한 관계 구조 마련 - 수집 및 입력 상의 자의성 배제 - 제재 수단도 명확히 명시

2. 정보자원의 저장

정보자원의 저장 단계에서 나타나는 현재적 특징들을 보면, 제도적 차원에서는 안전한 정보 저장을 위한 외부적 통제 감시 체계가 미비하고 관련 규정을 어겼을 때 개인에 대한 제재조치를 미약하여 정보보호 규정의 실효성이 낮게 나타나고 있었다.

관리적 차원에서도 개인정보의 보안 및 보호를 담당하는 부서가 이를 전담하여 책임 있게 운영하기보다는 다른 업무와 겸하면서 높은 업무 부담과 낮은 영향력으로 업무전문성을 확보하지 못했다고 평가되어 왔다. 정보에 대한 접근 권한을 제한하고 있지만 접근이 가능한 권한자를 어떻게 관리할 것인지에 대해서는 미비한 실정이다.

기술적 차원에서는 안전한 정보 저장과 관리를 가능하게 하는 여러 조치들이 부족해서 규정상으로는 금지되어 있으나 현실적으로는 개인별 저장장치를 통해 정보를 외부로 유출하는 것도 가능할 실정이었다. 행태적 차원에서는 보안의식보다 편리성과 효율성을 강조하는 것이 대부분 조직 구성원의 인식 수준이며 암호화 등 안전한 정보저장을 위한 관행은 구축되어 있지 못한 것으로 인식되었다.

이러한 정보 저장상의 관리 실태를 개선하는 주요 방향으로, 제도적 차원에서는 조직 외부 감시체계 및 조직 내부 통제체계를 강화하는 필요할 것이며 관리적 차원에서 개인정보 담당부서의 전문성을 강화시키고 정보 접근권자를 신중히 선발해 접근권자에 대한 관리도 이뤄져야 할 것이다.

기술적 차원에서는 망 분리, 개인저장장치를 사용한 정보반출 불가 등이 적극적으로 적용되어야 하며 보안기술 수준에 대한 잦은 정기 진단이 요구된다. 행태적 차원에는 취약한 정보보안 인식을 강화할 수 있는 교육과 함께 정보보안상의 사고에 대한 담당자의 책임을 높이는 방향을 고려해볼 수 있을 것이다.

〈표 8-2〉 정부 정보자원의 저장과 관련된 인권적 관리 프레임

저장		
	As-Is	To-Be
제도	- 권장수준의 내부통제 지침 - 미흡한 외부 감시 체계 - 자기정보열람권에 대해 낮은 수준의 보장	- 제재조치를 포함한 내부통제 강화 - 외부 감시 기구의 신설 - 자기정보열람권한의 적극적 보장
관리	- 개인정보보호 관련 부서의 비전문성과 높은 업무 부담, 낮은 영향력 - 접근권한은 제한하지만 접근가능자에 대한 감시 미흡 - 구성원의 양심에 의존하는 경향 - 정보보호 담당 인력 부족	- 개인정보보호 담당 부서의 업무전문성 강화 - 보안관리 상태의 정기적 검토 및 보고체계 운영 - 접근권한자의 신중한 선정 관리
기술	- 규정상 금지되지만 실제로 개인저장장치를 통한 외부반출 가능	- 개인 저장장치에 보관 및 외부 반출 규제 - 망 분리 - 보안기술수준의 정기적 진단 - 필요에 따른 열람만이 가능하도록 DB이외의 공간에서 저장 불가
행태	- 공공기관 종사자의 취약한 보안관리 인식 - 보안보다 편리성 중요시 - 정보보호를 위한 저장 관행 미흡	- 보안관련 정기적 교육 강화 - 업무 관련 개인정보에 대해 정보처리자의 책임성 부여

3. 정보자원의 분배 및 공유

정부 정보자원의 분배 및 공유 단계에서 나타났던 특징을 보면, 제도적 차원에서는 정보공유의 확대로 나타날 수 있는 개인정보관리상의 문제점을 소극적으로 다루고 있었으며 이에 대한 외부적 통제제도 역시 부재한 상황이었다.

관리적 차원에서는 정보주체의 동의를 구하지 않아도 되는 정보공유의 범위가 넓어서 어떤 정보가 어디까지 공유되고 있는지 정보주체가 알기 어려웠다.

기술적 차원에서도 시스템 상 기록이 남는 공유는 확인이 가능하지만, 비공식적으로 분배되거나 공유되는 정보를 확인하기는 어렵다는 한계가 있었다. 행태적 차원에서는 부처간의 정보 공유에서는 공유 범위가 제한되어 있고 공유 절차도 원활하지 않은 것으로 인식되고 있었다.

이런 측면에서 볼 때 정보 공유가 확산될수록 공유과정에서 나타나는 인권 침해적 측면이 높아질 것이라는 인식으로 공유를 제한하기보다 원활한 부처 간 정보공유의 방안을 마련하면서 공유로 나타날 문제점을 해결하는 제도적 방안을 동시에 모색해야할 것으로 보인다.

또한 외부감시체계를 강화하고 정보공유 현황을 투명하게 공개 관리가 필요할 것으로 보인다. 기술적으로도 정보 분배 및 공유와 관련된 기록관리가 보다 철저히 점검 및 보고될 필요가 있으며 행태적으로도 정보공유에 배타적인 인식을 낮추는 동시에 개인적 필요에 의한 무단 열람 및 공유에 대한 처벌 조치를 강화해야할 것이다.

〈표 8-3〉 정부 정보자원의 분배 및 공유와 관련된 인권적 관리 프레임

분배 및 공유		
	As-Is	To-Be
제도	- 폭넓고 모호한 정보공유의 예외규정 - 정보공유에 대한 외부통제 미흡 - 정보공유상 문제점 대처방안 미흡	- 정보공유의 예외 사항을 구체적으로 제시 - 외부감시체제의 구성 - 공유 범위 및 절차의 합리적 확장
관리	- 정보주체자가 정보공유 현황에 대한 파악 어려움 - 정보주체의 동의를 구하지 않은 정보공유 - 공동이용 권한인정도 신청기관 내에서 결정하는 구조	- 투명한 정보공유 현황 공개관리 - 불가피한 정보공유 시 익명처리를 통해 사생활 침해를 최소
기술	- 정보공유에 대한 현황파악 미비	- 시스템상의 연계 기록 공개 및 보고
행태	- 내부자에 의한 정보의 무단열람과 공유 - 정보공유의 범위 및 절차 제한적	- 개인적 필요에 의한 무단열람 및 공유에 대한 처벌 조치 강화

4. 정보자원의 사용

정부 정보자원의 사용 단계에서 나타나는 특징들을 살펴보면, 제도적 차원에서는 목적 외 사용을 금지하면서도 목적 외 사용을 폭넓게 인정하는 예외 규정들이 존재하거나 모호하게 나타나고 있었다.

관리적 차원에서도 정보 사용 현황 및 실태에 대한 조사가 비정기적이거나 형식적으로 이뤄지고 있어 그 실효성이 낮았고, 부처별 정보 사용 내역에 대해서 정보주체자의 알권리가 적극적으로 보장되지 못하고 있었다.

기술적 차원에서는 사용하는 정보의 내용이 오류 없이 정확할 수 있도록 관리 가능해야 함에도 내용적 오류를 수정하는 기술적 메커니즘이 미흡하였다.

행태적 차원에서 나타난 특징을 보면 정보의 목적 외 사용 및 오남용을 막기 위한 여러 제약들이 존재했지만 정부 조직 내부에서는 잘못된 사용을 막기 위한 자율적 규제 관행은 여전히 미흡한 수준으로 평가되었다.

정보자원 사용상의 대안적 조치들로는 제도적 차원에서 정보 사용 범위를 명확히 규정하고, 관리적 차원에서는 정보 내용을 정확성을 보장할 수 있는 관리 체계를 마련하거나 기술적 차원의 지원이 필요할 것이다. 행태적 차원에서는 정보 사용 상 민감정보에 대한 주의 및 정보 사용의 자율적 관리 관행을 구축하기 위한 가이드라인 마련과 강제가 필요할 것으로 보인다.

〈표 8-4〉 정부 정보자원의 사용과 관련된 인권적 관리 프레임

사용		
	As-Is	To-Be
제도	- 목적외의 사용을 폭넓게 인정 - 공유 및 사용상 개인정보보호를 관리 감독하는 기구 미흡	- 정보사용 범위를 명확히 규정 - 모호한 예외규정의 수정이 필요
관리	- 정보사용 현황과 목적에 대한 관리 부재 - 부처 별 정보사용 내역에 대한 정보주체자의 알 권리 보장 미비 - 비정기적, 형식적 이용실태 감사	- 개인정보사용 내역에 대한 정보주체자의 접근을 용이하게 함 - 제3자에의 정보제공시 관리강화 - 정보의 질 관리 체계 마련
기술	- 정보의 내용적 오류 수정 미흡	- 정보사용 용도의 명확한 제시 - 정보사용에 대한 등급제 - 열람기록 보존 및 정기적 감사 강화
행태	- 자율적 규제 관행 미흡 - 업무 상 편의를 위한 무분별한 정보의 이용	- 업무 관련 필요 정보를 정리하여 가이드 라인을 제시 - 민감정보에 대한 차별적 관리

5. 정보자원의 폐기

마지막으로 정보자원의 폐기 단계에서 나타난 특징은 제도적 차원에서는 폐기에 관한 규정 역시 모호하고 예외 조항이 넓게 적용되고 있어 불확실, 불투명한 정보 폐기라는 우려를 낳고 있으며, 관리적 차원에서는 폐기기간이 명시되지 않은 채 운영되거나 기한이 끝나더라도 근거 규정을 조정하며 폐기하지 않고 정보를 지속하는 것으로 나타났다.

기술적 차원에서도 여러 기관에 걸쳐 공유된 후 폐기가 결정된 경우는 이를 연동해서 한 번에 폐기해주는 기술적 시스템이 부족하였다. 행태적 차원에서도 앞서 언급했듯이 규정에 따라 필요가 없어진 개인정보는 바로 폐기해야 하지만 계속해서 보관하려는 경향성을 보였다.

따라서 앞으로의 정보자원 폐기와 관련해서 제도적 차원에서는 정보주체의 삭제청구권을 적극적으로 마련하고 폐기의 예외 조항 적용을 줄이도록 법제의 정비가 필요할 것으로 보인다.

관리적 차원에서는 수집 시 정보 유효기간을 명시하고 폐기 정보의 투명한 관리를 위한 폐기 목록의 공개와 정기적 보고체계 마련이 요구된다. 또한 기술적 차원에서는 한번 삭제한 정보가 재생 불가능하도록 해야 하며, 정보폐기가 결정되었을 때 여러 기관으로 분배되어진 정보가 연동해서 삭제될 수 있도록 기술적 지원이 필요하다.

행태적 차원에서는 부처의 정보 폐기에 대한 민감성을 높이도록 하고 정보폐기에 대한 외부적 통제를 통해서 부처의 정보수집 욕구를 자제할 수 있도록 해야 할 것이다.

〈표 8-5〉 정부 정보자원의 폐기와 관련된 인권적 관리 프레임

폐기		
	As-Is	To-Be
제도	- 정보주체의 청구가 있어도 타 법률에 따라 보유해야 할 경우에 삭제를 거부 할 수 있음. 법률 제정에 따라 자료가 폐기되지 않고 영구보관 할 수 있는 가능성이 상존 - 영구보관이 가능하다는 예외조항이 지나치게 모호함 - 정보폐기에 대한 외적 감시 부족	- 삭제청구권 보장 - 영구보관의 예외 축소 - 정보폐기와 관련한 평가를 각 정부조직 평가에 반영하도록 함
관리	- 폐기기간이 명시되지 않은 경우가 많음 - 기관의 필요에 의해 폐기기간이 지난 정보도 영구 보관하거나 폐기하지 않은 경우 있음 - 정보주체자의 폐기 현황에 대한 열람을 보안 등의 이유로 거부하기도 함	- 모든 정보의 유효기간을 명시 - 폐기정보의 목록관리 및 정기적 보고체계 마련 - 개인정보의 폐기현황을 적극적 공개 - 수정 및 삭제 불가한 서류의 범위를 최소화함
기술	- 수정 및 삭제 불가한 서류가 존재함(예:형사사법정보) - 여러 기관에 걸친 정보의 일괄 삭제 불가	- 재생불가능한 기술 구현 - 한 기관의 삭제가 관련 기관에서 연동될 수 있어야 함
행태	- 필요가 사라진 개인정보의 미폐기 - 규정 전환을 통해서 보관 유지	- 필요가 사라진 개인정보 보유시 벌점 부여 등 인사평가에 반영하도록 함 - 부처의 정보폐기 의무 강화

6. 요약: 정부 정보자원의 인권적 관리 프레임

아래의 표는 앞서 분석한 정부 정보자원의 인권적 관리 프레임(To-Be) 부분만을 제시하고 있다.

<표 8-6> 정부 정보자원관리와 관련된 인권적 관리 프레임(To-Be)

수집/생성	
제도	- 예외 조항의 축소/명확화를 위한 법제 정리 - 독립적 개인정보보호책임자* 제도와 같은 내부통제 제도 강화 - 중앙관리기구의 권한 강화(시정명령권/과태료/허용취소) - 개인정보영향평가제도의 실천방안 구체화
관리	- 구체적인 행동 매뉴얼 제시 - 불필요한 정보수집 제재 규정마련 - 유효기간을 정한 수집 - 중앙관리기구의 사전 통제 강화
기술	- 정보통합으로 새로운 정보생성 규제
행태	- 정보수집자와 수집대상의 대등한 관계 구조 마련 - 수집 및 입력 상의 자의성 배제 - 제재 수단도 명확히 명시
저장	
제도	- 제재조치를 포함한 내부통제 강화 - 외부 감시 기구의 신설 - 자기정보열람권한의 적극적 보장
관리	- 개인정보보호 담당 부서의 업무전문성 강화 - 보안관리 상태의 정기적 검토 및 보고체계 운영 - 접근권한자의 신중한 선정 관리
기술	- 개인 저장장치에 보관 및 외부 반출 규제 - 망 분리 - 보안기술수준의 정기적 진단 - 필요에 따른 열람만이 가능하도록 DB이외의 공간에서 저장 불가
행태	- 보안관련 정기적 교육 강화 - 업무 관련 개인정보에 대해 정보처리자의 책임성 부여

공유	
제도	- 정보공유의 예외 사항을 구체적으로 제시 - 외부감시체제의 구성 - 공유 범위 및 절차의 합리적 확장
관리	- 투명한 정보공유 현황 공개관리 - 불가피한 정보공유 시 익명처리를 통해 사생활 침해를 최소
기술	- 시스템상의 연계 기록 공개 및 보고
행태	- 개인적 필요에 의한 무단열람 및 공유에 대한 처벌 조치 강화
이용	
제도	- 정보사용 범위를 명확히 규정 - 모호한 예외규정의 수정이 필요
관리	- 개인정보사용 내역에 대한 정보주체자의 접근을 용이하게 함 - 제3자에의 정보제공시 관리강화 - 정보의 질 관리 체계 마련
기술	- 정보사용 용도의 명확한 제시 - 정보사용에 대한 등급제 - 열람기록 보존 및 정기적 감사 강화
행태	- 업무 관련 필요 정보를 정리하여 가이드 라인을 제시 - 민감정보에 대한 차별적 관리
폐기	
제도	- 삭제청구권 보장 - 영구보관의 예외 축소 - 정보폐기와 관련한 평가를 각 정부조직 평가에 반영하도록 함
관리	- 모든 정보의 유효기간을 명시 - 폐기정보의 목록관리 및 정기적 보고체계 마련 - 개인정보의 폐기현황을 적극적 공개 - 수정 및 삭제 불가한 서류의 범위를 최소화함
기술	- 재생불가능한 기술 구현 - 한 기관의 삭제가 관련 기관에서 연동될 수 있어야 함
행태	- 필요가 사라진 개인정보 보유시 벌점 부여 등 인사평가에 반영하도록 함 - 부처의 정보폐기 의무 강화

Ⅸ. 결론

1. 연구요약 및 시사점

지금까지 한국 정부의 정보자원 관리 실태를 법제도, 갈등사례, 정부부서의 인식 등 세 차원에서 살펴보았으며, 연구결과를 간략하게 요약하면 다음과 같다.

1) 법제도 측면

법제도 측면에서 세계 여러 나라 가운데 단일한 전자정부법의 제정은 2001년 우리나라가 최초이며, 뒤이어 미국이 2002년 11월에 제정하였다(정충식, 2006) 우선 미국의 정보관리에 관한 법률은 우리나라의 법과 비교해 볼 때, 비교적 포괄적인 내용을 담고 있다. 우리나라의 전자정부법이 전자적인 문서처리를 기본관점으로 하여 기존의 사무관리 규정 조항들을 법령으로 승격시킨 것에 비해, 미국의 법은 전자정부 구현 및 개인정보보호에 있어, 관리예산처(OMB)의 역할을 규정하고, 연방정부의 조정력 강화에 초점을 맞추고 있다.

그러나 2011년 9월 시행되는 한국의 개인정보보호법 및 행정안전부의 공공기관 개인정보보호 지침에서 볼 수 있듯이 한국의 경우도 미국의 관리예산처(OMB)와 같이 행정안전부를 주축으로 각 부처에서 개별적으로 관리되고 있는 정보자원을 통합적으로 조정하고 통제하려는 노력을 보여주고 있다.

독일의 경우, 연방정보보호법은 독일 헌법의 “정보에 관한 자기 결정권”을 근거로 1990년 12월에 공포하여, 두 차례의 개정을 거쳐 현재에 이르고 있다. 이 법은 공공기관과 민간기관 모두에 적용되는 특징이 있다. 한국과 미국, 독일의 법률은 정보자원의 관리에 있어 정보의 수집, 생

성, 이용, 파기에 이르는 정보자원생애주기의 각 단계별 처리기준을 구체적으로 제시하고 있다.

2) 갈등사례 측면

갈등사례에서는 전체적으로는 정보자원 관리와 관련한 명확하고 엄격한 규정이 없거나 미비한 측면으로 인해 시민단체와 갈등을 불러 일으켰다. 정부는 전자정부를 실현하는 과정에서 기술의 도입과 효율적 관리에 중심을 두면서 정보인권과 관련한 법 · 제도적 측면을 부차적으로 고려하고 있다. 이에 정보인권에 대한 명확한 규정이 드러나 있지 않음으로 인해 이에 대한 정부의 조치나 활동이 부족하면서 이에 대한 시민단체의 우려가 갈등이라는 현상으로 나타났다. 따라서 정보자원 관리의 기술적 측면의 강화를 우선시 하면서 이에 대한 사회적 문제를 예방할 수 있는 법적, 제도적 측면에서의 조치가 부족하여 갈등을 일으켰다고 해석 할 수 있다.

각 정보자원생애주기별로, 수집 및 생성에서는 공통적으로 정보 주체의 동의 없이 개인 정보를 수집하거나 포괄적인 규정으로 인한 정보수집으로 인해 정보주체의 선택권이 부여되고 있지 않음이 나타나고 있다. 저장과 관련해서는 정보의 저장 및 보관과 관련한 보다 엄격한 규정의 필요성이 나타나고 있으며, 공유에 대해서는 정보자원의 목적외 사용에 대한 우려와 정보주체의 동의를 얻지 않은 공유가 문제로 나타났다. 사용에 대해서는 보유목적외의 사용을 폭넓게 인정하고 있는 점, 폐기와 관련하서는 폐기에 대한 불명확한 규정이나 규정이 없는 경우로 인해 갈등이 나타나고 있다고 볼 수 있다.

이와 같은 문제로 인해 갈등이 발생하는 근본적인 이유는 정보자원에 대한 인식에서 차이 때문이다. 앞서 언급했던 바와 같이 정부는 정보자원을 도구적 합리성 차원에서 다루고 있지만, 정보자원은 효과적 관리를 위한 도구인 이전에 정보주체에 대한 다양한 측면을 보여준다는 점에서 인

권적 요소를 담고 있다. 자원 활용의 효율을 높이기 위해 예외 규정을 넓게 설정하는 등의 정부의 정보자원 관리로 인해 현재 부각되고 있는 정보인권이 보장되고 있지 못하면서 정보자원과 관련한 갈등이 지속되고 있다. 그리고 전자정부 이후, 국가통합DB를 구축하고자 하는 시도가 증가하면서 이러한 갈등은 점차 증가하고 있음을 알 수 있다.

3) 정부 부서의 인식측면

효과성 및 위험성면에서 사회적 우려와 괴리된 실태 인식 수준과 낮은 위험 인식을 보여주고 있다. 정보관리 체계 면에서 부처별로 분리된 배타적 관리 체계, 범부처적 정보관리 통합조정 체계 미흡, 미비한 법제에 대한 낮은 문제인식, 중첩 및 모호한 규정에 대한 부처의 관행적 적용 기준 존재하는 것으로 나타났다.

정보관리 단계별로 수집 및 생성 부문에서는 부처별 수집관리 구조로서 구축된 정보보다 낮은 수준의 공개를 보이고 있다. 저장 부문에서는 정보접근 권한이 제한되고 있으며, 외부 통제 체계가 미흡한 것으로 인식하고 있었다.

분배 및 공유에서는 정보 공유의 범위와 절차상의 제약과 정보 공유상의 문제점 대처가 미흡한 것으로 인식하고 있었으며, 사용 부문에서는 자율적 규제 관행의 미흡한 것으로 나타났다. 폐기 부문에서는 규정에 따른 폐기하고 있으나 규정 외 영역에서는 보관 경향이 나타나고 있으며, 명료한 규정의 필요성을 인식하고 있는 것으로 나타났다.

정보관리 주체별에서 중앙과 지방부서 간을 보면 중앙 부서에 비해 열악한 지방부서의 관리 실태와 지방부서가 정보유출의 위험성이 높고 참여 가능성 낮은 것으로 인식하고 있었다. 또한 중앙에 비해 지방에서 국민 접근이 어렵다고 인식하고 있었다. 현업과 정보부서 간을 보면 정보부서가 현업 부서에 비해 프라이버시 침해 가능성 등 위험성 인식 높은 것으로 나타났다.

2. 제언: 정보인권을 위한 정보자원관리 거버넌스 설계

1) 정보인권을 위한 법체계 부문

공공부문과 민간부문에서 발생하는 개인정보 유출 등 정보인권 침해를 방지하고 실제적 보호를 위하여 2011년 9월에 개인정보보호법이 실행되었지만 여전히 정보인권을 관장하는 관련 기관간의 법이 충돌할 가능성을 배제할 수 없다. 개인정보보호법 제 6조는 동법과 다른 법률과의 관계에 있어 "개인정보 보호에 관하여는 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다"고 규정하고 있다. 그러나 이러한 일반법과 특별법의 소관부서가 다르다는 점이 문제가 될 가능성이 있다. 예를 들어 정보통신망과 개인정보보호법은 각각 방송통신위원회와 행정안전부의 소관이다. 이는 경우에 따라 관련 법률 규정을 집행하는데 있어 규제중첩이 발생할 수 있음을 의미한다.[34]

현재 정보자원을 관리하는데 있어 기본적으로 각 부처별로 관리하며, 매년 보유하고 있는 개인정보 목록을 공시하고 있다(행정안전부 홈페이지). 각 부처와 행정안전부는 사전협의 및 권고 관계로 부처는 개인정보의 수집 및 보유 목적 등을 고지하며 행정안전부는 상/하반기 1회씩 몇 개 기관을 선정해서 실태조사 후 개선을 권고하고 있지만 그 외 특별한 관리 및 보고 체계 없으며 사전협의나 권고도 강제력도 없다는 데 문제가 있다. 이러한 맥락에서 관련 기관간의 조직적 배열에 관심을 가져야 한다. 정보자원관리가 시간적(장기), 공간적(범부처)으로 상당한 노력이 필요하다는 점에서 정보자원을 일관성 있고, 체계적으로 운영할 수 있는 조직

34) 개인정보 보호법은 제34조에서 개인정보처리자는 개인정보가 유출되었음을 알게 되었을때에 지체없이 해당 정보주체에게 관련 사실들을 통보하여야 한다고 규정하고 있지만 정보통신망은 아무런 규정을 두고 있지 않다. 따라서 정보주체에 대한 통지문제가 포함된 개인정보 유출사고가 발생한 경우 원칙적으로 방송통신위원회가 사고조사를 수행하게 되지만 통지문제에 대해서 행정안전부가 재차 개입할 가능성이 있다는 것이다(심우민, 2011: 3-4).

이 필요하며, 범 정부적으로 공공기관에 대한 업무조정을 할 수 있는 능력과 인력이 확보되어야 할 것이다.

2) 정보인권을 위한 조직운영 부문

어떤 기술이든 과거에 비해 진화하는 속도가 매우 빨라져서 거의 대부분의 네트워크 영역에서 해킹가능성이 있다. 네트워크 영역에 대한 해킹 공격에 대한 위험성은 날로 높아지고 있고 각 국가들이 해킹에 의한 공격을 당하는 상황에서, 국민들의 개인정보를 집적하여 네트워크 망으로 연결할 경우, 한 기관의 전산망만 뚫리더라도 엄청난 양의 개인정보가 유출될 가능성이 상당하다. 문제는 이러한 피해가 국민 개개인에게 돌아간다는 점이다.

그러므로 정보자원을 정보인권 시각에서 관리하려는 노력이 무엇보다 중요하다고 할 수 있다. 사실 관리에 대한 패러다임이 아직은 전통관료제적 시각에서 이루어져 왔다. 하지만, 과거와는 달리 국민들의 인식틀에서 정부 정책은 국민들의 동의가 있어야 하는 것으로 생각하는 경향이 커지고 있다. 특히 정보의 주체인 국민들이 단순히 '관리의 대상이 아니다'라는 점을 간과한 채 형사사법통합체계 등과 같은 정보자원 통합 및 축적, 공유 등을 추진한다는 점은 국민들의 정보주체권에 대한 인식이 부족하다고 볼 수 있다.

정보주체권에 대한 인식이 부족하다는 것은 국민들은 관리의 대상이지 중요한 정책 파트너나 동의를 구해야 하는 중요 행위자로 인식하지 않고 있는 것이다. 물론 법제도가 존재하며 시스템 상 관리(서버관리, 로그기록 보존 등 대장관리)는 대체로 지침에 따라 지켜지지만, 정보보호의 개념이 잘 인식되어 있지 않을 뿐만 아니라 체계적으로 관리되지도 못하고 있는 형편인 것으로 보인다. 또한 개인정보보호는 조직에서 지켜야할 제도가 되지 못하고, 원칙대로 일일이 따르기 힘들고 불편한 비현실적인 원칙(현재 법제상의 공백, 중첩, 충돌 등)이 나타날 때 제도적으로 해결하기 보다

는 대부분의 개인들이 기존의 관행대로 처리하고 있음을 예상해 볼 때 정부 전체의 조직 운영에서 정보인권적 시각을 반영한 정보자원관리가 조직 전반적으로 내재화되고 일체화될 필요가 있다.

3) 정보인권에 대한 인식 부문

무엇보다도 국민에 대한 정보를 실질적으로 다루고 있는 정부조직과 그의 구성원이 정보인권에 대한 인식론적 전환이 필요하다. 지금까지 정부 관료는 정보자원을 보다 효과적인 관리를 위한 수단, 정보자원의 효율적 활용을 위한 규칙을 만드는 것에 치중했을 가능성이 높다. 정보에 대한 인식에 있어서 정부는 정보를 부와 성과를 만들어 내는 변화단계에서의 수단으로 여기는 측면이 강하기 때문에 인권 등 효율을 저해할 요소에 대해서는 최소한의 규정으로 이들 요인들로 인한 사용의 불편함을 줄이려고 하는 것이다.

또한 정보자원을 다룸에 있어 입력 오류 및 부주의한 관리, 자원의 미폐기 등의 문제가 야기 될 수 있음에도 이러한 문제들은 모두 통제 가능하다고 믿고 있었는지도 모른다. 이러한 점에서 그동안 정부는 정보자원과 관련된 사항은 단지 내부 관리방식의 변화라고만 인식하여 내부적 담론과정만을 거치면서 정책을 정당화하고 외부관계자들과의 의사소통은 거의 진행하지 않는 형편인 것이다.

특히 정보자원 집적을 통한 활용에 있어서 이에 따른 효용은 이를 집적하는 기관에서 얻게 되나, 이에 따르는 위험은 정보의 주체인 일반국민이 부담하게 된다. 정부입장에서는 정보유출로 인한 비난 여론으로 인한 뭇매는 통합에 따라 얻게 되는 이익보다 크지 않다고 인식할 수 있고, 자신들이 직접적인 피해자가 될 가능성이 적기 때문에 정보자원의 집적에 대해 집착하는 경향이 있다고 판단된다. 하지만, 일반국민들은 이러한 정보유출로 인해 금전적, 신체적 피해를 직접적으로 받지 않는 한 이러한 위험을 감지하지 못하는 경향이 크기 때문에 정보자원 집적에 대한 위험

에 대해 민감하지 못하며, 소수의 시민단체 만이 해당 문제를 제기하고 있는 형편이다.[35]

따라서 정보자원의 인권적 측면에서의 인식전환에 대한 초점은 위험이 잠재하지만 평소에는 직접적으로 느낄 수 없는 것들, 정보주체도 모르게 활용되어 정보주체에게 해를 끼칠 수 있는 부분에 대한 경각심과 인식론적 전환을 위한 교육, 훈련이 지속적으로 일관성 있게 추진되어야 할 것으로 보인다.

35) 일반국민들은 또한 정보자원 집적과 정보화에 따른 one-stop 서비스라는 편의성이라는 피부에 와 닫는 편의성에 대한 인식으로 정보화에 따르게 되는 부정적 부산물인 인권 침해에 대한 부분에 대해 둔감한 생각을 가지고 있을 가능성이 있으며, 단지 막연히 불쾌한 수준으로 인식하고 있을 가능성이 높다.

참고 문헌

국가인권위원회 (2006). 『헌법 및 국제인권법의 관점에서 본 개인정보의 취급기준과 그 한계: 전자정부와 개인정보의 공유 통합의 법적 문제점』.

국가인권위원회 (2006). 『개인정보 수집 · 저장 · 이용의 적법성과 한계(정보인권 관점 등에서 본 형사사법통합정보체계)』.

국가인권위원회 (2009) 『개인정보 수집 · 유통 실태조사』.

국가인권위원회 (2009). 『정보인권 관련 법제변화에 따른 시민의식 조사』.

교육인적자원부 (2003). "교육정보시스템(NEIS) 관련 자료집".

김동수 · 김민수 (2006). e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향 정보화정책 13원 4호 128~148

김상겸/김성준 (2008). "정보국가에 있어서 개인정보보호에 관한 연구 - 공공부문을 중심으로 독일의 법제와 비교하여", 《세계헌법연구》, 14(3): 87-116.

김선희 (2005). "국책사업 갈등분석 및 합의형성 방안", 국책사업 갈등분석 및 합의형성 방안, 국토연구원 1-25.

김성근 (2004).『행정정보자원관리 혁신방안 수립에 관한 연구』, 행정자치부 연구보고서.

김성태 (2003). 『전자정부론: 이론과 전략』. 법문사.

김일환 (2004). "행정정보의 공동이용으로부터 정보자기결정권의 보호에 관한 헌법상 고찰," 《공법연구》32(4).

김태형. (2007). 『학생의 사생활권 보호에 관한 연구: NEIS를 중심으로』. 인천대학교 석사학위논문.

나태준 (2006). "정책인식프레이밍 접근방식에 따른 갈등 분석: 교육행정정보시스템 도입 사례를 중심으로", 《한국정책과학학회보》, 297-325.

문신용 (1999). 『행정정보화와 조직운영의 혁신방안』, 한국행정연구원.
방송통신위원회 외 (2011). 『국가정보보호백서』.
박정훈 (2008). “정부신뢰와 정책수용: 전자주민카드정책을 중심으로,” 《행정논총》, 46(1): 93-122.
서진완 (1998). 『정보기술을 활용한 행정업무과정의 혁신지침』, 한국행정연구원.
심우민 (2011). “개인정보 보호법 시행과 당면과제,” 《이슈와 논점》 308호.
윤상오 (2009). “전자정부 구현을 위한 개인정보보호 정책에 관한 연구: 정부신뢰 구축의 관점에서”, 《한국지역정보화학회지》, 12(2): 1-29.
윤정수 (2005). “국내 공공기관의 정보자원관리 추진방안 연구: 서울시와 미 연방정부의 사례를 중심으로”, 《정보기술아키텍처연구》, 2(1): 67-83.
이은우 (2004). “지문 등 생체정보이용, 무엇이 문제인가,” 《국가인권위원회 토론회 자료집》.
이인호 (2005). 개인정보보호법제의 현대화방안에 관한 연구. 국회사무처 법제실.
임규철 (2002). “정보화사회에서의 개인정보자기결정권에 대한 연구 - 독일에서의 논의를 중심으로” 《헌법학연구》, 8(3): 231-260.
임규철 (2003). “각 국의 개인정보보호법제 비교연구 - 미국과 유럽연합의 개인정보보호법제를 주심으로”, 《공법연구》, 31(5): 71~90.
정국환 · 문정욱 · 홍필기 (2006). 『공공정보자원관리의 혁신방안 연구』, 정보통신정책연구원 .
정국환 외 (2005). 『공공정보화 성과평가 방법론 및 체계 연구』, 정보통신정책연구원.
정부혁신지방분권위원회 (2005). 『참여정부의 전자정부』.
정인숙 (2010). “행정정보공동이용과 정보인권”, 《인권복지연구》, 6:

97-127

정충식 (2007). 『전자정부론』. 서울경제경영.

조화순 (2004). 거버넌스의 관점에서 본 NEIS 갈등 사례 연구 《정보화정책》, 11(1): 36-50.

최재혁 (2008). 『형사법상 개인정보보호에 대한 연구: 사이버공간상의 개인정보보호를 중심으로』. 한양대학교 석사학위논문.

최진명 (2007). "EA와 정보자원관리의 관계," 《지역정보화》 45: 26-32.

최흥석·서진완 (2006). "한국 중앙정부의 정보자원관리 운영 분석," 《한국행정논집》 18(1): 129-148.

최흥석·이정준·구상회 (1999). "핵심성공요인에 기초한 중앙정부 정보자원관리모델," 《정책분석평가학회보》 9(1): 73-90.

한국보건의료연구원 외 (2011). 『보건의료 정보화 및 공익적 연구 활용을 위한 토론회 - 개인정보보호법 제정에 따른 의견 수렴』.

행정자치부 (2007). 『정부정보자원관리 프로세스 프레임워크』.

행정안전부 (2008). 『2008년도 공공기관 개인정정보호 기본지침』.

행정안전부 (2011). 『2011 국가정보화 백서』.

홍성욱 (2002). 『파놉티콘: 정보사회 정보감옥』, 책세상.

황성흠 (2001). "전자정부의 법과 국가," 《법과사회》 20.

황주성 · 임혜경 (2006). "공공부문의 정보자원관리의 문제점과 개선방향 연구". 《정부학연구》, 12(1): 195-229

황주성 외 (2006~2007). 『공공정보자원관리의 혁신방안 연구(Ⅰ,Ⅱ)』, 정보통신정책연구원.

Barendt, E. (2005). *Freedom of Speech*. Oxford University Press.

Cate, F. H. (1997). *Privacy in the Information Age*. Brookings Institution Press.

Der Bundesbeauftragter für den Datenschutz und Die Informationsfreiheit(편), Bundesdatenschutzgesetz - Text und Erläuterung, 제13판. 2007.

Gola/Schomerus, Bundesdatenschutzgesetz Kommentar, 제10판, 2010.

Henry, C. L. (2003). *Freedom of Information Act*. Novinka Books.

Keenan, K. M. (2005). *Invasion of Privacy: A Reference Handbook*. ABC-Clio.

Norris, P. (2001). Digital Divide: *Civic Engagement, Information Poverty, and the Internet Worldwide.* Cambridge University Press

Office of Management and Budget (2005). *FEA Consolidated Reference Model Document.*

Roberts, A. (2006). *Blacked Out: Government Secrecy in the Information Age.* Cambridge University Press

Subramanian, H. (2008). *Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions*. IGI Global.

부록 1. 설문조사지

Org Code		DP Code		Case ID			

정부 정보자원 관리 및 정보인권 인식에 대한 조사

안녕하십니까? 먼저 설문에 응해주셔서 감사합니다. 본 설문조사는 **국가인권위원회의 지원을 받아 진행되는 조사**로서 정보자원의 사용 및 관리에 대한 선생님의 경험과 의견을 수렴하여 이를 바탕으로 향후 제도발전과 정책개선에 도움이 되는 시사점을 모색하기 위한 것입니다.

본 연구의 성과는 바로 업무를 담당하시는 선생님 한 분 한 분의 귀중한 협조에 달려있습니다. 평소 선생님께서 진행하시는 사업에 대하여 생각하신대로 빠짐없이 기입해 주시면 본 조사에 큰 도움이 됩니다. 본 조사는 무기명으로 실시되며, 응답 내용은 통계적으로 처리되어 연구를 위한 참고자료로만 사용됩니다. 또한, 절대적으로 비밀이 보장됩니다. 바쁘신 와중에도 설문조사의 취지를 이해하시어 부디 끝까지 빠짐없이 응답해 주시기 바랍니다. 설문에 응답해 주셔서 감사드리며, 선생님의 건승을 기원합니다.

2011년 9월

고려대학교 행정학과 교수 최흥석
(02-3290-2279, hschoi@korea.ac.kr)

<설문응답 문의하실 곳>

■ 선임연구원: 고려대학교 행정학과 정부학연구소 이철주(leecjay@gmail.com)
고려대학교 행정학과 정부학연구소 한승주(sngjoo@korea.ac.kr)
■ 주소 및 전화번호: 서울시 성북구 안암동 1가 5번지 고려대학교 행정학과 02) 3290-2279

****본 설문에서 표현하는 '정보'는 각 부서에서 수집 및 보관, 관리하고 있는 행정정보DB를 의미합니다.**

Ⅰ. 정보의 수집, 저장, 분배 및 공유, 사용, 폐기 실태

<문 1> 다음은 선생님이 속한 부서의 **정보 관리 일반**에 관한 질문입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1)	우리 부처는 개인의 프라이버시를 고려한 정보 관리가 이루어지고 있다	①	②	③	④	⑤
(2)	우리 부처는 정부 정보가 민간 기관과 공유될 때 창출되는 부가가치 및 생산성을 고려한 관리가 이루어지고 있다	①	②	③	④	⑤
(3)	우리 부처는 행정 효율성 향상을 위한 정보 관리가 이루어지고 있다	①	②	③	④	⑤
(4)	우리나라 정보 관리는 **전 부처**를 포괄하는 중앙집권적으로 운영되고 있다	①	②	③	④	⑤
(5)	우리나라 정보 관리는 **부처별** 책임으로 운영되고 있다	①	②	③	④	⑤
(6)	우리나라 정보 관리는 **부서별** 책임으로 운영되고 있다	①	②	③	④	⑤
(7)	우리 부처에는 정보 관리 과정에서 발생하는 부서 간 문제를 조정하는 체계가 있다	①	②	③	④	⑤
(8)	**우리 부처의 경우 부서 별**로 전담하는 정보가 따로 구별되어 관리되고 있다	①	②	③	④	⑤
(9)	**우리 부처의 경우 부서 별**로 전담하는 정보에 관한 관리책임은 각 부서에 있다	①	②	③	④	⑤
(10)	우리 부처에는 정보 관리에 기준이 되는 구체적인 문서 지침이 있다	①	②	③	④	⑤
(11)	우리 부처의 경우 정보 관리 과정은 구체적으로 기록되고 관리 된다	①	②	③	④	⑤
(12)	우리 부처의 경우 정보 관리 과정에서 법제간 충돌과 중첩으로 혼란이 있다	①	②	③	④	⑤
(13)	우리 부처의 경우 정보 관리 과정에서 법제의 공백으로 문제해결의 어려움이 있다	①	②	③	④	⑤
(14)	우리 **부처**는 정보의 수집, 공유, 이용, 폐기 등에 관해 자율적으로 결정할 수 있는 재량이 많다	①	②	③	④	⑤
(15)	우리 **부처**는 정보의 수집부터 공유, 저장, 이용, 폐기까지 전반을 직접 관리하고 있다	①	②	③	④	⑤

<문 2> 다음은 정보의 **수집**과 관련된 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 O 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1)	우리 부처는 업무에 필요한 최소한의 범위에서 정보를 수집 및 보유하고 있다	①	②	③	④	⑤
(2)	다른 **부처**에서 같은 정보를 가지고 있더라고 우리 부처에서 따로 수집하여 보유한다	①	②	③	④	⑤
(3)	우리 **부처**에는 정보 수집을 기획하고 책임지는 담당자의 권한이 크다	①	②	③	④	⑤
(4)	우리 부처에서 업무상 이용되는 정보의 대부분이 목록으로 구축되어 있다	①	②	③	④	⑤
(5)	우리 부처에서 수집, 보관하는 정보의 목록은 국민에게 공개되고 있다	①	②	③	④	⑤
(6)	우리 부처는 정보를 수집하는 과정에서 정보주체의 동의를 구하고 있다	①	②	③	④	⑤
(7)	우리 부처는 정보를 수집하는 과정에서 정보주체의 참여 절차가 용이하다	①	②	③	④	⑤
(8)	우리 부처는 정보를 수집하는 과정에서 내부적으로 엄격한 협의 및 허가를 거친다	①	②	③	④	⑤
(9)	우리 부처는 정보를 수집 및 생성하는 과정에서 규정된 내용을 준수한다	①	②	③	④	⑤
(10)	우리 부처의 경우 CCTV, 지문 등 생체정보, 병력, 종교 등 민감한 정보를 처리하는 과정이 보다 엄격하다	①	②	③	④	⑤

<문 3> 다음은 정보의 **저장**과 관련된 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1)	우리 부처는 정보보호 및 보안을 위한 관리 관행이 구축되어 있다	①	②	③	④	⑤
(2)	우리 부처는 개인적으로 이동식 저장장치에 정보를 담아 외부에서 작업하고 있다	①	②	③	④	⑤
(3)	우리 부처는 정보저장 및 정보파일 송수신시 안전성 확보를 위한 조치(암호화 등)를 지키고 있다	①	②	③	④	⑤
(4)	우리 부처는 정보의 안전성을 위한 기술적 조치가 충분하다	①	②	③	④	⑤
(5)	우리 부처는 정보의 안전성을 위한 관리 규정이 충분하다	①	②	③	④	⑤
(6)	우리 부처에서는 정보에 접근할 수 있는 권한을 업무 담당자로 제한하고 있다	①	②	③	④	⑤
(7)	우리 부처는 정보 저장 및 열람에 관한 기록을 시스템 상에서 관리하고 있다	①	②	③	④	⑤
(8)	우리 부처는 정보유출에 대한 내부 보고 및 책임 체계가 구축되어 있다	①	②	③	④	⑤
(9)	우리 부처는 정보유출에 대해 국민이 감시할 수 있는 체계가 구축되어 있다	①	②	③	④	⑤

<문 4> 다음은 정보의 **분배 및 공유**와 관련된 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
(1)	**부처 간** 정보 공유의 범위(공유 부처 수, 공유 정보 수 등)가 넓다	①	②	③	④	⑤
(2)	**부서 간** 정보 공유의 범위(공유 부서 수, 공유 정보 수 등)가 넓다	①	②	③	④	⑤
(3)	**부서 간** 정보 공유가 원활하게 이뤄지고 있다	①	②	③	④	⑤
(4)	**부처 간** 정보 공유가 원활하게 이뤄지고 있다	①	②	③	④	⑤
(5)	**부서 간** 정보 공유의 절차가 복잡하다	①	②	③	④	⑤
(6)	**부처 간** 정보 공유의 절차가 복잡하다	①	②	③	④	⑤
(7)	**부서 간** 정보 공유를 위한 표준 절차가 준수되고 있다	①	②	③	④	⑤
(8)	**부처 간** 정보 공유를 위한 표준 절차가 준수되고 있다	①	②	③	④	⑤
(9)	**부서 간** 공유 과정을 기획 및 통제할 제도가 구축되어 있다	①	②	③	④	⑤
(10)	**부처 간** 공유 과정을 기획 및 통제할 제도가 구축되어 있다	①	②	③	④	⑤
(11)	우리 부처는 정보 공유 시의 정보유출, 오남용 등을 막기 위한 조치가 충분하다	①	②	③	④	⑤
(12)	우리 부처는 정보 공유 시의 정보유출, 오남용 등을 막기 위해 공유 권한자를 제한하고 있다	①	②	③	④	⑤
(13)	우리 부처는 정보 공유로 인한 정보유출, 오남용 등을 막기 위해 공유 절차를 엄격하게 운영하고 있다	①	②	③	④	⑤
(14)	우리 부처는 정보 공유의 내역이 기록 및 공개되고 있다	①	②	③	④	⑤
(15)	우리 부처는 정보 공유 과정에서 국민에 의한 감시 및 통제 체계가 마련되어 있다	①	②	③	④	⑤

<문 5> 다음은 정보의 **사용**과 관련된 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1)	우리 부처에서는 업무 외 목적으로 정보 열람이 가능하다	①	②	③	④	⑤
(2)	우리 부처에서는 업무 외 목적으로 정보를 열람 및 사용하는 것을 자율적으로 제한하는 관행이 존재한다	①	②	③	④	⑤
(3)	우리 부처에서는 업무 외 목적으로 정보를 열람 및 사용하는 것을 통제하는 관리규정이 구축되어 있다	①	②	③	④	⑤
(4)	우리 부처의 경우 정보의 목적 외 사용, 오남용을 막기 위한 내부 감시절차와 보고체계가 운영되고 있다	①	②	③	④	⑤
(5)	우리 부처는 정보를 외부위탁기관 등 제3자에게 제공한 후 그 사후관리를 하고 있다	①	②	③	④	⑤
(6)	우리 부처는 정보에 접근하는 권한이 업무관련성에 따라 차별적으로 부여된다	①	②	③	④	⑤
(7)	우리 부처에서 보유하고 있는 정보의 내용은 오류 없이 정확하다	①	②	③	④	⑤
(8)	우리 부처는 부정확한 정보를 정기적으로 검점하여 정정 또는 삭제하고 있다	①	②	③	④	⑤
(9)	우리 부처는 정보의 정확성을 높이기 위해 국민이 참여하는 구조를 마련하고 있다	①	②	③	④	⑤
(10)	우리 부처는 국민이 자신에 관한 정보내용을 열람, 정정, 삭제 청구하는 절차가 용이하다	①	②	③	④	⑤
(11)	우리 부처는 정보에 대한 국민의 열람, 정정, 삭제 청구는 업무효율을 낮춘다	①	②	③	④	⑤

<문 6> 다음은 정보의 **폐기**와 관련된 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1)	우리 **부서**의 정보폐기 실태를 관리하는 체계가 존재한다	①	②	③	④	⑤
(2)	우리 **부처**의 정보폐기 실태를 관리하는 체계가 존재한다	①	②	③	④	⑤
(3)	우리 부처에는 정보폐기와 관련된 규정이 구축되어 있다	①	②	③	④	⑤
(4)	정보폐기 결정은 **부서**의 재량이 크다	①	②	③	④	⑤
(5)	정보폐기 결정은 **부처**의 재량이 크다	①	②	③	④	⑤
(6)	우리 부처의 경우 정보폐기 결정은 폐기 비용과 보관 시 편익을 고려하여 결정할 수 있다	①	②	③	④	⑤
(7)	우리 부처는 정보의 보유기간이 지나거나 목적 달성 후 정보를 규정대로 폐기한다	①	②	③	④	⑤
(8)	우리 부처는 업무 위탁기관에 제공한 정보를 추후 파기하도록 관리한다	①	②	③	④	⑤
(9)	우리 부처는 당장 불필요한 정보라도 파기하기보단 보관한다	①	②	③	④	⑤
(10)	우리 부처의 폐기된 정보 목록은 외부에 공개되고 있다	①	②	③	④	⑤
(11)	우리 부처의 경우 정보의 폐기 여부를 국민들이 확인하기 용이하다	①	②	③	④	⑤
(12)	우리 부처에는 국민들이 정보 폐기를 요구할 수 있는 체계가 있다	①	②	③	④	⑤

Ⅱ. 정보관리의 위험성 인식

<문 1> 다음은 정보 관리의 **위험성**에 관한 인식을 묻는 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1)	현재 우리 부처의 정보 수집 및 생성 수준은 국민의 프라이버시를 침해할 가능성이 있다	①	②	③	④	⑤
(2)	현재 우리 부처가 보유하고 있는 정보를 통해 국민에 대한 감시가 가능하다	①	②	③	④	⑤
(3)	현재 우리 부처의 정보 관리는 국민의 접근이 어려워 불투명하게 운영될 가능성이 있다	①	②	③	④	⑤
(4)	현재 우리 부처는 개인정보 유출, 분실, 도난 등 보안 사고의 위험이 있다	①	②	③	④	⑤
(5)	현재 우리 부처가 보유하고 있는 정보 중 잘못된 내용으로 인해 국민이 피해를 받을 위험이 있다	①	②	③	④	⑤
(6)	현재 우리 부처는 목적 외 정보 이용, 정보의 오남용 등으로 국민이 피해를 받을 위험이 있다	①	②	③	④	⑤
(7)	현재 다른 부처와의 정보 공유 과정에서 정보유출 및 오남용 등 사고의 위험이 있다.	①	②	③	④	⑤
(8)	현재 우리 부처는 정보가 제때 폐기 되지 않아 국민이 피해를 볼 수 있는 잠재적인 위험이 있다	①	②	③	④	⑤

Ⅲ. 정보관리의 효과성

<문 1> 다음은 정보 관리의 **효과성**에 관련된 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 그렇지 않다	그렇지 않다	보통이다	그렇다	'매우 그렇다
(1)	우리 부처는 정보의 수집, 공유, 사용으로 보다 공공서비스 제공방식의 합리성을 높이고 있다	①	②	③	④	⑤
(2)	우리 부처는 정보 수집, 공유, 사용을 통해 조직목적 달성을 돕는다	①	②	③	④	⑤
(3)	우리 부처는 정보의 수집, 공유, 사용으로 공공서비스를 제공받을 적합한 대상을 찾는다	①	②	③	④	⑤
(4)	우리 부처는 정보 수집, 공유, 사용으로 국민의 공공서비스 이용 편의를 향상시키고 있다	①	②	③	④	⑤
(5)	우리 부처는 다른 부처, 민간기관 등과의 정보 공유로 새로운 정보가치를 창출시키고 있다	①	②	③	④	⑤
(6)	우리 부처는 정보 수집, 공유, 사용 과정에서 국민의 결정권 및 참여가능성을 높이고 있다	①	②	③	④	⑤
(7)	우리 부처는 정보 관리 과정에서 보유하는 정보의 내용 정확성을 높이고 있다	①	②	③	④	⑤
(8)	우리 부처는 정보 관리 과정에서 보유하는 정보의 신뢰성을 높이고 있다	①	②	③	④	⑤
(9)	우리 부처는 정보 수집, 공유, 사용으로 내부 업무비용을 절감하고 있다	①	②	③	④	⑤
(10)	우리 부처는 정보 수집, 공유, 사용으로 내부 업무과정을 단축시키고 있다	①	②	③	④	⑤

<문 2> 다음은 **현재 정보 관리 과정의 국민 참여 가능성**과 관련된 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문		매우 낮다	낮다	보통이다	높다	매우 높다
(1)	현재 우리 부처의 정보관리 과정에서 국민의 접근 가능성	①	②	③	④	⑤
(2)	현재 우리 부처의 정보관리 과정에서 국민에 대한 정보 공개 정도	①	②	③	④	⑤
(3)	현재 우리 부처의 정보관리 과정에 대한 국민의 감시 가능성	①	②	③	④	⑤
(4)	현재 우리 부처의 정보관리 방식 및 내용에 관한 국민의 수정 요구 가능성	①	②	③	④	⑤
(5)	현재 우리 부처의 정보관리 방식 및 내용에 관한 국민의 변경 요구 가능성	①	②	③	④	⑤
(6)	현재 우리 부처의 정보관리 방식 및 내용에 관한 국민의 선택 가능성	①	②	③	④	⑤

Ⅳ. 정보기술과 정보관리자원에 대한 생각

<문 1> 다음은 **정보기술**에 대한 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1) 정보기술은 바이러스의 **확산** 가능성이 높다	①	②	③	④	⑤
(2) 정보기술은 개인정보의 **유출** 가능성이 높다	①	②	③	④	⑤
(3) 정보기술은 개인의 프라이버시 **침해가능성**이 높다	①	②	③	④	⑤
(4) 정보기술은 컴퓨터 **범죄의 발생**가능성이 높다	①	②	③	④	⑤
(5) 정보기술과 관련된 **위험**은 인간의 기술과 노력을 통해 **통제**할 수 없다	①	②	③	④	⑤
(6) 정보기술은 현재의 **사회문제를 해결**할 수 있다	①	②	③	④	⑤
(7) 정보기술하면 **좋은 이미지**가 먼저 생각난다	①	②	③	④	⑤
(8) 정보기술은 **인류 전체에 긍정적인 영향**을 미칠 것이다	①	②	③	④	⑤
(9) 정보기술은 인류에게 **편안한 생활**을 가져올 것이다	①	②	③	④	⑤
(10) 특정 정보기술이 막대한 경제적 이익이 있더라도 **윤리적인 문제**가 있을때는 절대 사용해서는 안된다	①	②	③	④	⑤
(11) 정보기술은 우리의 삶을 보다 **편리**하게 만들 것이다	①	②	③	④	⑤
(12) 정보기술의 발전 덕분에 지구의 자연자원은 **고갈되지 않을 것**이다	①	②	③	④	⑤
(13) 정보기술 덕분에 미래세대는 **더 많은 기회**를 가질 수 있을 것이다	①	②	③	④	⑤

<문 2> 다음은 **정보관리를 위한 자원**에 대한 질문들입니다. 각 주장에 대하여 선생님이 느끼시는 대로 해당되는 응답에 ○ 또는 V 표시 해주시기 바랍니다.

진 술 문	매우 그렇지 않다	그렇지 않다	보통 이다	그렇다	매우 그렇다
(1) 정보기술 전문인력이 많이 확보되어 있다	①	②	③	④	⑤
(2) 정보보안을 위한 필요인력은 확보하였다	①	②	③	④	⑤

(3) 정보부서 직원의 IT교육훈련(정보부서 IT교육훈련비/부서 전체교육훈련비):
_____원/_____원

(4) IT인력비율(IT인력/전체인력): _____명/_____명

<문 3> 다음은 **정보관리 담당자로서** 겪는 어려움과 현재 조직의 정보자원관리 상의 우려점이 무엇인지 선생님이 생각하시는 바를 자유롭게 적어주시기 바랍니다.

Ⅴ. 개인별 특성

1. 선생님의 소속부서와 직급은 어떻게 되십니까? (　　실·국) (　　과) (　　)

2. 귀하의 현재 계급은 몇 급(상당)이십니까?

1급 상당	2급 상당	3급 상당	4급 상당	5급 상당	6급 상당	7급 상당	8급 상당	9급 상당	10급 상당

3. 선생님의 연령은 만으로 어떻게 되십니까?

1	2	3	4	5
20-29세	30-39세	40-49세	50-59세	60세 이상

4. 선생님은 다음 중 어디에 속합니까?

1	2	3	4	5	6	7
행정직	기술직	별정직	기능직	전산직	계약직	기타_____

5. 선생님은 공직생활을 하신지는 몇 년 되십니까?

1	2	3	4	5	6	7
5년 이하	6-10년	11년-15년	16년-20년	21년-25년	26년-30년	31년 이상

6. 선생님의 성별은 무엇이십니까?

1) 남

2) 여

수고하셨습니다. 설문에 응해 주셔서 대단히 감사합니다.

부록 2. 정보자원관리 관련자 인터뷰 전문

○ 전 정보화담당관 인터뷰(女, 2011.8.23.3시, 국가인권위 회의실)

1. 정부의 정보 관리 거버넌스

기본적으로 각 부처별로 관리하며, 매년 보유하고 있는 개인정보 목록을 공시함(행정안전부 홈페이지). 각 부처와 행정안전부는 사전협의 및 권고 관계로, 부처는 개인정보의 수집 및 보유 목적 등을 고지하며 행정안전부는 상/하반기 1회씩 몇 개 기관을 선정해서 실태조사 후 개선 권고함. 그 외 특별한 관리 및 보고 체계 없으며 사전협의나 권고도 강제력이 없음.

2. 공무원의 정보 관리 실태

법제도가 존재하며 시스템 상 관리(서버관리, 로그기록 보존 등 대장관리)는 대체로 지침에 따라 지켜지지만, 개인의 업무상 정보자원 관리 실태는 심각하여 정보보호의 개념이 없고 체계적으로 관리되지 못함. 개인정보보호에 관한 무지, 무심, 둔감에서 나오는 실수들이 많으며 관행, 문화임. 개인정보에 대한 민감성이 매우 낮아서, 개인정보보호는 조직에서 지켜야할 제도가 되지 못하고, 원칙대로 일일이 따르기 힘들고 불편한 비현실적인 원칙. (현재 법제상의 공백, 중첩, 충돌 등이 나타날 때 이를 해결하는 것인 개인적인 판단으로 개인에게 달려있지만 대부분의 개인들이 기존의 관행대로 처리하고 있음).

1) 수집: 개인정보 대상이 뭔지 모르고 있음. 최소한 수집 원칙이 있지만 어디까지가 최소인지 담당자 개인의 판단에 달려있고 업무상 개인이 무엇을 수집하는지 옆에서 알 수도 없음. 기관에서 정보

수집 시 행정안전부에 보고, 협의 절차 있지만 사용목적만 적절히 고지하면 별다른 제약 없음. 개인이 업무적으로 필요한 것으로 따로 수집하는 것을 관리하기도 힘드니 개인한테 달려있는 셈인데 개인들은 현재 이를 문제로 인식하지 못하는 분위기.

2) 저장: 데이터를 개인 PC나 USB 등에 담아서 이동하는 것은 보통이고 아무 제약도 없고 문제라고 생각하지도 않음. 노트북에 담아서 밖에서 작업하다가 분실하는 경우도 발생하지만 큰 문제가 되지 않음. 서버 상 대장관리나 로그기록 같은 보안대책은 그나마 지켜지지만 개인별로 업무상 보안을 고려한 행동은 거의 없다고 봄.

3) 공유: 기관 대 기관 관계에서 정보를 보낼 때 비공식적으로 보내거나 하는 것은 많이 줄었음. 개인이 제3자에게 비공식적으로 제공하거나 외부 위탁한 정보를 신경 써서 관리하는 경우는 거의 없음. 행정정보 공동이용 과정에서 개인정보보호와 관련한 제한은 거의 없는 것으로 알고 있고 공동이용 사용권한 인정도 신청기관 내에서 결정하는 구조임.

4) 사용: 개인정보가 담긴 파일을 외부에 보내야할 경우 이메일로 보내는 것도 문제지만 암호화도 하지 않고 그냥 발송함. 암호화는 최소의 조치인데 이마저도 하지 않는 것이 현실임. 정보내용의 신뢰성, 정확성도 제때 제대로 업데이트하지 않으니까 떨어질 수밖에 없음.

5) 파기: 여태껏 어떤 부서에서 정보를 어떤 이유로 어떻게 파기했다는 소리를 들어본 적 없음. 정보폐기가 이뤄지고나 있는지 그와 관련된 기록 자체가 있는지 의심스러움. 없다고 봄.

3. 정부 정보관리 실태 개선을 위한 제언

시스템구축, 네트워크 관리, 보안 등의 업무를 맡지만 보안관련 업무는 업무자체가 10% 남짓일 정도로 적음. 개인정보보호는 중요하지만 업무의 비중이 낮고 우선순위에서 밀림. 물론 사고가 나면 크게 날 것이라는 불안감을 가지고 있지만 다른 일에 밀려 여력이 없으니 관심을 가지고 관리할 수 없음. 사고가 날까 불안감을 가지는 것조차 현재는 괜한 걱정을 하는 사람이라는 분위기임. 데이터가 유출되면 어떻게 흘러 다닐 것인지를 아니까 사고가 날 것이 우려되지만 큰 사고가 난 적이 없고 확률도 낮으니까 적극적으로 관리하게 되지 않음. 아마 큰 사고가 터져봐야 바뀌지 않을까. 새 개인정보보호법은 과태료 등 처벌 규정이 있으니까 이대로 시행된다면 앞으로 이런 문화가 나아질 것이라고 생각함. 원칙이 없는 것이 아니라 현실에서 엄격하게 적용되거나 지켜지지 않는 것이 문제니까.

업무상 취득한 개인정보는 목록화 되기 어렵고 통제할 수 있는 방법은 없다고 생각함. 그나마 네트워크 PC방식으로 공동DB를 구축하는 것이(은행처럼) 보안상 낫다고 생각하지만 서버구축 비용, 망 분리로 인한 불편초래 등을 생각한다면 보안만을 생각할 수는 없다고 봄.

○ 시민단체 담당자 인터뷰(女, 2011.6.20.6시)

1. 정부의 개인정보 관리 상 문제점

정부 스스로 인권적 관리할 것이라고 생각하지 않음. 인권위, 법원, 헌재가 중요한 통로이며 이들을 움직여서 정부의 인권적 정보관리 보장하는 방식으로 활동해야 함. 정부 공무원들의 인권적 관리 의식수준을 신뢰할 수 없으므로 법률유보를 강조하는 방향으로 활동해야 함.

현재는 다른 여러 법률에서 정보의 인권적 관리근거 찾을 수 있지만 산재되어 있어서, 정부는 이를 우회하여 적용하고 있는 것이 현실임. 예를 들어 형실효법이 있음에도 CIMS 상에서 정보는 폐기하지 않고 관리하는 것이 가능한 상황임.

공무원들의 정보관리 실태에 대한 구체적인 경험, 견해 등에 대해서는 듣지 못하지만, 공무원들이 개인정보의 관리를 중요하게 생각하지 않는 듯함. 다만, 정보시스템 감리업체와 공무원의 관계로 인해 형식적 감리관계에 그치는 정도의 문제는 알고 있음. 공무원의 시민단체 사이에는 실체적 피해와 잠재적 피해에 대한 인식 차이가 있음.

2. 정부 정보관리 실태 개선을 위한 제언

개선을 위해서는 공무원의 구체적인 관리실태보다는 조직단위의 행태로 접근해야 함. 2008년을 기점으로 정보공개에서는 행태가 확실히 다르게 나타남. 정보공개의 기준은 상당히 자의적이기에 대응행태 변할 수 있음. 특히, 경찰의 독립적 정보체계구축 욕구는 심각한 편으로 지문정보, 수사정보 등을 독점하여 불투명하게 보유, 이용하고 있음.

개인정보 보호를 둘러싸고 정부와 시민단체의 담론 경쟁을 하고 있음. 한때 진보넷은 정부의 효율성 담론에 따라 대응하기도 했지만 이제는 하지 않고 있는데, 효율성 프레임으로는 정보인권을 말할 수 없다고 판단했기 때문임.

시스템 도입 전에 이슈화하여 개입하려고 노력해야 하는데 정부에 특정 시스템이 일단 들어오면 철회는 어렵기 때문임. 최근에는 유전정보 DNA법, 패킷 감청, 전자주민증 등에 주목해서 활동하고 있음.

정부는 이중적 지위를 가지고 있음. 공공분야에서는 견제의 대상이지만 민간분야에서 개입이 요구되는데, 사회권적 차원에서는 정부개입을 요구하기에 자유권적 차원과 다름. 민간분야에서 기업의 정보관리에 대한 규제를 강화해야 하지만, 공공분야에서는 시민사회로부터 통제를 받고 투명해져야 함.