총 목 차

발제문

1 · 전자정부에서 정보프라이버시의 실현과제 ……1
2 · 공공기관 보유 개인전자정보의 학술적 이용에 대한 고찰 ……45
3 · 수사와 범죄 예방 활동에서의 감시기술의 활용과 그에 대한 통제 ……63
4 · 인터넷과 인권 ……89

토론문

1 · 「公共機關의 個人情報保護法改正案」說明資料 ……105
2 · 정보화 사회에 있어서 개인정보보호 현황 및 대책 ……111
3 · 프라이버시 보호와 관련 법제도 개선 필요성 ……121
4 · 개인정보 보호시스템과 관련된 기술적 조치에 대해서 ……129
5 · 정보화사회에서의 인권 [토론요지문] ……133
6 · 한국사회의 정보인권의 현실 ……141

전자정부에서 정보프라이버시의 실현과제

李 仁 皓
(중앙대학교 법과대학 교수)

순 서

I. 머리말 ·····3
II. 자유민주국가의 정보법질서와 정보인권 ·····4
III. 개인정보처리의 위험성에 대한 이해 ·····7
IV. 위험성에 대한 안전장치 : 정보인권으로서의 개인정보자기결정권 ··12
V. 현행 공공부문 개인정보보호법제의 문제점 분석 ·····23
VI. 체계정비를 위한 몇 가지 제언 ·····40
VII. 맺는 말 ·····44

전자정부에서 정보프라이버시의 실현과제

李 仁 皓
(중앙대학교 법과대학 교수)

I. 머리말

오늘날 놀라운 정보기술의 발전으로 인해, 디지털화된 개인정보가 정보주체도 인식하지 못한 채 타인의 수중에서 무한대로 수집·축적·처리·가공·이용·제공될 수 있게 되었으며, 그리하여 개인의 실존인격과 분리된 또 하나의 총체적 인격상이 타인의 수중에서 쉽게 획득되고 조작될 수 있는 가능성이 점차 현실화되고 있다. 개인정보자기결정권은 이러한 정보환경에서 그 정보주체의 인간존엄과 민주적 가치질서를 확보하기 위해 필수불가결하게 요구되는 헌법적 요청이다.

종래의 사생활권이 은둔으로서의 사생활보호(privacy as seclusion)라는 소극적 성격의 것이었다면, 이 개인정보자기결정권은 참여로서의 사생활보호(privacy as participation)라는 적극적 성격을 지닌다. 정보주체는 자신에 관한 정보가 누구에 의해 어떤 목적으로 어떻게 이용되는지를 명확하게 인식하고 그러한 정보처리의 과정에 함께 참여할 수 있어야 한다. 이러한 참여로서의 사생활보호 모델은 특히 정부가 개인정보처리의 남용을 통해 국민을 감시하고 통제하고자 하는 위험을 차단시키는 역감시의 기능을 수행한다.

그러나 현재 우리의 공공부문 개인정보보호법제는 아직 참여로서의 사생활보호 모델을 완전하게 구현하지 못하고 있는 것으로 평가된다. 여러 개별 법률에서는 비밀보호라는 관점에서 처벌조항을 두고 있을 뿐이고, 개인정보자기결정권을 구체화하는 일반법인 공공기관의개인정보보호에관한법률은 여러 가지 한계와 문제점을 가지고 있는 것으로 분석된다. 장차 이 법의 개정방향을 어떻게 모색할 것인지는 우리 전자정부의 기본이념과 가치를 어떻게 설정할 것인지와 직결되어 있는 문제이다.

전자정부에서 개인정보 보호의 문제는 두 가지 상이한 측면에서 제기된다. 하나는 정부기관 상호간 또는 국민에 대한 정부업무의 효율성을 위해 개인정보를 수집·처리·이용하는 측면(“개인정보이용의 측면”)이고, 또 하나는 정부의 투명성을 확보하기 위해 정부 보유의 공공정보를 국민에게 공개하는 가운데 개인정보가 공개되는 측면(“정보공

개의 측면")이다. 전자의 측면에서는 '정부의 효율성 가치'와 '개인정보보호의 가치'가 충돌하고, 후자의 측면에서는 '정부의 투명성 가치'와 '개인정보보호의 가치'가 충돌한다. 이 양 측면에서의 개인정보보호의 법리는 완전히 동일할 수 없다. 전자의 측면에서 개인정보보호는 참여로서의 사생활보호 모델이 중심이 되고, 후자의 측면에서 개인정보보호는 은둔으로서의 사생활보호 모델이 중심을 이루기 때문이다.

그런데 현재의 공공부문 개인정보보호법제는 각 측면에서 상충하는 가치간의 균형이 다소 일그러져 있다는 판단이다. 즉, 개인정보이용의 측면에서는 정부의 효율성 가치가 개인정보보호의 가치를 압도하고 있는 반면, 정보공개의 측면에서는 개인정보보호의 가치가 정부의 투명성 가치를 상회하고 있는 것으로 보인다.

이 글은 개인정보이용의 측면에 초점을 맞추어 정부의 효율성 가치에 압도된 개인정보보호의 가치를 재평가하고 양 가치간의 깨어진 균형을 회복할 필요가 있음을 역설하면서 그 방향을 제시해보고자 한다.

II. 자유민주국가의 정보법질서와 정보인권

1. 정보 · 권력 · 자유의 상관관계

'아는 것이 힘이다'라는 베이컨(1561-1626)의 고전적 명제는 원래 그가 사용했던 것보다 훨씬 더 보편적인 의미를 지니고 있다. 베이컨의 이 명제는 경험과학적 지식을 통해 인간이 자연에 도전하고 그것을 정복한다고 하는 제한된 전략적 함의를 가지고 제시되었었다.[1] 그러나 이 명제는 情報의 지배와 權力의 상관관계를 설명하는 보다 확대된 의미로 재구성될 수 있다. 즉 '정보통제는 곧 권력이다.' 이 명제는 중세시대 라틴어로만 쓰인 경전을 성직자만 읽고 해석할 수 있었다는 사실 그 자체가 곧 교회권력을 유지하는 필수 조건이었음을 상기하는 것으로 충분히 이해될 수 있다.

실로 정보는 단순한 데이터나 지식이 아니라 그 자체가 곧 힘(power)인 것이다. 일정한 정보를 누가 받고 누구는 받지 못하게 조정할 수 있을 때 그의 권력은 강화되게 마련이다. 따라서 정치공동체 내에서 정보를 누가 얼마만큼 장악하고 지배하느냐는 그 공동체의 권력

1) 미셸 푸코는 近代社會에서 '과학'이 중세의 신을 대신하는 권위를 지니고 인간의 의식과 행태를 통제하기 위한 권력의 주요한 원천임을 규명하고 있다. Christopher Arterton/한백연구재단(편역), 『텔레데모크라시』(거름, 1994), 11쪽.

구조 및 개인의 자유를 결정하는 핵심조건이 아닐 수 없다. 다시 말해서, 정보의 지배는 권력의 원천이자 자유의 조건인 것이다. 문제는 누가 정보를 지배하느냐에 있다.

예를 들면, 오늘날의 정보사회에서 개인정보의 지배는 그 정보주체에게는 인격의 존엄과 자유의 불가결한 조건이 되지만, 동시에 타자(정부나 기업체)에 의한 개인정보의 지배는 정보주체를 통제할 수 있는 권력의 기초가 된다. 최근에 정보사회로 진입하면서, 개인정보를 중심으로 한 자유와 권력의 이항대립이 정부 대 시민사회 사이에서, 그리고 시민사회 내부에서 첨예하게 나타나고 있다. 개인정보의 지배권을 누가 장악하느냐에 따라 종래의 국가권력과 시민사회의 관계는 재조정될 것이며, 동시에 시민사회 내부에서는 새로운 권력관계가 형성될 수도 있다. 이는 자유민주주의체제의 운명을 결정지을 중대한 사안이다. 자유민주체제는 한 마디로 개인의 존엄과 자유의 조건을 확보하는 체제이기 때문이다. 개인정보보호의 문제를 단순히 인격보호의 관점에서만 바라볼 수 없는 이유가 여기에 있다. 한편, 정보사회에서 무한한 정보자원에 접근할 수 없는 사람들에게 그것은 단순한 지식의 결여만을 의미하는 것이 아니라 곧 권력과 자유의 조건을 상실한다는 것을 의미한다. 오늘날 정보격차(digital divide)의 문제가 단순히 복지차원의 문제로 그칠 수 없는 이유도 또한 여기에 있다.

2. 헌법상 정보법질서의 기본이념

자유민주주의를 지향하는 현행 헌법상의 정보법질서는 자유로운 정보유통의 이념에 입각하여, 정보유통에 대한 통제권을 상이한 두 가지 차원에서 개인에게 부여함으로써 개인의 자유와 민주주의를 확보하고자 하는 기본정책을 표방하고 있다.

헌법은 제21조 제1항에서 언론·출판의 자유와 집회·결사의 자유를 보장하고, 제2항에서 검열금지의 원칙을 선언하고 있으며, 제22조 제1항에서는 학문의 자유[2]와 예술의 자유[3], 제26조는 청원권, 제27조 제3항은 공개재판을 받을 권리, 제31조는 교육을 받을 권리와 대학의 자율성을 보장하고 있다. 그리고 제45조는 국회의원의 면책특권을 보장하고, 제50조에서는 국회회의공개의 원칙, 제109조는 재판의 심리·판결의 공개원칙을

2) "학문의 자유는 진리를 탐구하는 자유를 의미하는데, 그것은 단순한 진리탐구에 그치지 않고 탐구한 결과에 대한 발표의 자유 내지 가르치는 자유 등을 포함하는 것이다."(헌재 1992. 11. 12. 89헌마88, 판례집 4, 739, 756). 이러한 학문의 자유에는 진리탐구에 필요한 정보의 자유로운 수집과 탐구결과의 자유로운 전파라고 하는 자유로운 정보유통의 이념이 내재되어 있다.

3) "예술의 자유의 내용으로서는 예술창작의 자유, 예술표현의 자유, 예술적 집회 및 결사의 자유가 포함된다." (헌재 1993. 5. 13. 91헌바17, 판례집 5-1, 275, 283).

선언하고 있으며, 나아가 제127조에서는 국가의 정보개발의무를 규정하고 있다. 이들 헌법규정에는 사회 내 자유로운 정보유통이 촉진되어야 한다는 기본정책이 담겨 있다. 이에 더 나아가, 정부가 보유하는 정보에 대한 접근권인 정보공개청구권의 헌법적 보장의 확인[4] 및 이를 구체화하는 공공기관의정보공개에관한법률은 자유로운 정보유통의 이념을 보다 적극적으로 구현하고 있는 것이다. 결국 이들 기본권과 원칙들은 "公的 性格의 情報"를 정부가 독점하거나 지배하지 못하도록 함으로써 사회와 개인의 권력과 자유를 확보하는 기능을 수행한다.

그러나 반면에, 현행의 정보법질서는 특정한 목적을 위해 일정한 정보에 대해서는 위와 같은 헌법상의 개인의 통제권을 박탈하거나 제한함으로써 자유로운 정보유통을 억제하기도 한다. 예컨대, 헌법 제21조 제4항은 타인의 명예·권리 및 공중도덕의 보호를 위한 언론·출판의 한계를 밝히고 있고, 이에 따라 형사 및 민사의 명예훼손법은 타인의 명예를 훼손하는 정보의 유통을 금지시키며, 음란처벌법 및 미성년자 보호를 위한 규제입법들은 일정한 표현내용의 제작 또는 유통을 금지시키고 있다. 이 외에도 국가안보를 위협하는 정보나 기업비밀에 해당하는 정보의 유통을 금지하는 여러 입법들이 존재한다. 또 헌법 제22조 제2항은 저작자·발명가·예술가 등의 권리를 인정함으로써 그 보호범위에 드는 정보의 유통에 대한 통제권을 그 정보생산자에게 부여하고 있고, 그 한도 내에서 자유로운 정보유통은 제한을 받게 된다.

그렇지만, 이러한 정보유통의 억제는 결코 그 자체가 목적이 될 수 없다. 단지, 국가안보나 타인의 권리보호 또는 기술혁신과 사회진보의 달성이라고 하는 정당하고도 구체적인 목적을 위해서 예외적으로 허용되는 수단으로서의 성격을 가진다는 점에 유의하여야 한다. 그러므로 예외적인 정보유통의 억제수단이 헌법적으로 정당화되기 위해서는 비례의 원칙과 법률유보의 원칙을 준수하여야 한다. 즉 정당하고도 구체적인 목적이 존재하여야 하고, 그 목적 달성을 위해 필요한 최소한의 범위 내에서 정보유통을 억제하여야 한다(비례의 원칙). 또 그러한 억제정책은 민주적 정치과정인 입법절차에 의해 명확하게 표명되어야 한다(법률유보의 원칙).

---

4) 헌법재판소는 일찍이 정보공개청구권이 헌법상의 기본권적 성격을 가지고 있다는 점을 인정한 바 있다. 헌재 1989. 9. 4. 88헌마22, 판례집 1, 176; 헌재 1991. 5. 13. 90헌마133, 판례집 3, 234. 이후 이들 결정에서 제시된 정보공개청구권의 헌법적 근거 및 이론구성에 대해 상당한 비판이 제기되었다. 예컨대, 강경근, "국민의 정보공개청구권", 법률신문 제1881호, 1989. 10. 16; 홍준형, "정보공개청구권과 정보의 자유",『현대법의 이론과 실제』(김철수교수화갑기념논문집, 1993); 경건, "정보공개청구제도에 관한 연구"(서울대 법학박사학위논문, 1998) 등 참조. 그러나 긍정적 평가도 없지 않았다(이승우, "국민의 알권리에 관한 헌법재판소 결정의 평석",『사법행정』 1990년 4월호). 이들 결정에 대한 최근의 예리한 분석으로는, 전광석, "정보화사회의 헌법구조",『헌법학연구』 제5권 제2호 (한국헌법학회, 1999), 289-301면 참조.

한편 이와는 다른 차원에서, 헌법은 "私的 性格의 情報"에 대한 통제권을 당해 정보주체에게 줌으로써 정부나 타인의 자의적인 지배가능성으로부터 정보주체의 권력과 자유를 확보하고자 한다. 예컨대, 헌법 제12조 제1항의 압수·수색·심문의 법정주의, 동조 제2항의 불리한 진술거부권, 동조 제3항의 압수·수색의 영장주의, 제16조 제2문의 주거에 대한 압수·수색의 영장주의, 제17조의 사생활비밀의 보장, 제18조의 통신비밀의 보장 등이 그것이다. 나아가, 최근에 논의되고 있는 개인정보자기결정권은 타인(정부 또는 사기업체)이 축적·처리하고 있는 개인정보에 대해 정보주체에게 그 수집·이용 및 유통에 대한 통제권을 부여함으로써 더욱 적극적으로 개인의 자유를 확보하고자 하는 것이다.

물론 이 경우에도 국가안보나 형사사법의 집행 등 정당하고도 구체적인 목적을 위해 정보주체의 통제권을 제한함으로써 사적 성격의 정보의 유통을 예외적으로 허용할 수 있다. 그러나 그것은 어디까지나 예외적으로 채택되는 수단적 성격의 것이기 때문에, 그것이 헌법적으로 정당화되기 위해서는 비례의 원칙과 법률유보의 원칙, 그리고 일정한 경우에는 영장주의를 준수하여야 한다.

이상을 요약하면, 현행의 정보법질서는 자유로운 정보유통의 이념 하에 公的 性格의 情報에 대해서는 "모든 개인"에게 그 유통에 대한 통제권을 인정함으로써 개인의 존엄과 자유의 조건을 확보하고 동시에 민주적 정치과정을 촉진하고자 하는 기본정책을 채택하고 있다. 한편, 私的 性格의 情報에 대해서는 "당해 정보주체"에게 그 유통에 대한 통제권을 부여함으로써 개인의 존엄과 자유의 조건을 확보하고자 하고 있는 것이다. 이 두 가지 방향의 기본정책은 개인의 존엄과 자유를 보장하고 민주적 정치과정을 확보하고자 하는 모든 자유민주국가에서 그 정보법질서의 근간을 이루는 것이라고 할 것이다.

III. 개인정보처리의 위험성에 대한 이해

1. 서언

디지털 정보혁명으로 촉발된, 개인정보의 지배를 둘러싼 자유와 권력의 이항대립은 이미 우리 사회에 두드러진 현상이 되고 있다. 그런데 이러한 대립 속에는 결코 무시할 수 없는 개인정보처리의 이익과 가치가 그 위세를 떨치고 있음을 부인하기 어렵다. 현

대의 정부는 단순히 물질적 생산조건의 확보라는 기능을 넘어서서 복지나 사회정책 등 사회적 재생산조건을 보장하기 위한 기능을 담당하게 되었고, 이러한 기능을 효율적으로 수행하기 위해서는 무엇보다 개인정보의 수집과 처리가 불가결한 요소가 되고 있다. 특히 최근에는 정보기술의 활용을 통하여 대국민 고객지향성이라는 이념 하에 작고 효율적인 시민위주의 질 좋은 행정서비스를 제공한다고 하는 전자정부의 개념이 구체화되고 있다.[5] 이 전자정부의 핵심요소 중의 하나는 개인정보를 포함한 행정정보의 공동이용이다.[6] 한편, 시장에 있어서도 기업에 의한 고객의 개인정보처리는 자원배분의 효율성을 극대화할 뿐만 아니라 소비자인 정보주체에게는 거부할 수 없을 정도의 달콤하고 편리한 이익을 안겨준다.

그러나 개인정보처리가 가져다 줄 이익과 가치 못지않게 그 위험성 또한 무시할 수 없을 정도로 커서 이른바 사이버 원형감옥(Cyber-Panopticon)의 우려를 낳고 있다.[7] 사이버 원형감옥에서의 국민은 국가과정에 적극적으로 참여하는 능동적 시민으로서의 국민이 아니라, 정부가 구축하는 개인정보처리시스템에 의해 국가작용의 내용과 형식이 결정되어지는 소외된 수동적 시민으로서의 국민으로 전락하게 될 것이다.[8]

이제 고도정보사회로 진입하는 길목에서 이러한 위험성을 최소화하면서 개인정보처리의 이익과 가치를 극대화할 수 있는 규범적 척도를 찾아내는 것이 우리 사회의 시급하고도 절실한 과제가 되었다.

2. 개인정보의 디지털화와 통합관리의 효율성

상호작용적이고 네트워크화된 사이버공간에서 컴퓨터의 키보드를 두드리는 것 자체가 내 자신을 드러내는 행위이고 그 행위는 사이버공간의 어딘 가에 디지털화된 형태로 흔적을 남긴다. 이처럼 정보사회로 진전되면 될수록 개인의 행위 하나 하나는 모두

---

5) 전자정부의 이념을 구체화하는 입법으로 전자정부구현을위한행정업무등의전자화촉진에관한법률이 2001년 3월 28일 법률 제6439호로 공포되고 2001년 7월 1일부터 시행되고 있다. 이 법에서 "전자정부"라 함은 "정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부"를 말한다(법 제2조 제1호).

6) 2000. 8. 30. 현재 중앙행정기관, 지방자치단체, 정부투자기관 등 전체 4,373개의 공공기관이 모두 452종, 8,421개의 개인정보화일을 보유하고 있고, 그 속에 담긴 개인정보의 전체양은 실로 엄청나다.

7) 사이버 원형감옥의 기술적 요소인 프라이버시침해기술(PITs)에 대한 소개는, 이인호, "온라인 프라이버시 침해기술과 보호기술의 법적 함축", 『법학논문집』 제25집 제2호 (중앙대학교 법학연구소, 2001), 53-76면 참조.

8) 한상희, "국가감시와 민주주의", 『개인정보의 국가등록·관리제도의 문제점』 (프라이버시보호네트워크 제2차 공동토론회 요지집, 2001. 8. 22), 1-2면.

디지털화되어 일정한 데이터베이스에 수록된다. 오늘날 모든 공·사의 기관들은 여러 가지 목적에서 개인에 대한 수많은 자료들을 디지털화된 형태로 가지고 있다. 인구학적 기본통계, 교육, 재정, 의료, 신용정보, 고용, 납세, 출입국, 치안관련자료, 사회복지, 군복무, 자동차관리, 백화점, 사회단체, 금융 등과 관련한 개인정보는 일부에 지나지 않는다. 사실 사회가 정보화된다는 것은 모든 사회활동이 디지털화된다는 것을 의미한다.

그런데 디지털화된 개인정보는 관리 및 이용의 측면에서 이전과 비교할 수 없는 효율성을 가지게 된다. 발전된 DBMS(Database Management System)의 활용으로 인해 개인에 대한 정보의 입력, 처리, 검색, 출력이 신속하고 정확하게 이루어질 뿐만 아니라 더 나아가 표준식별번호(universal identification number)에 의한 컴퓨터결합(computer matching)을 통해 분산되어 있는 개인정보들을 용이하고 효율적으로 통합·처리할 수 있게 되었다.

3. 수집·처리된 가상인격과 실존인격의 불일치에 따르는 위험성

이 같은 기술적 가능성 속에서 이제 개인은 자신의 실존인격 외에 또 하나의 가상인격을 가지게 되는 셈이다. 그런데 정보사회의 위험성은 바로 이러한 가상인격이 실존인격을 규정짓게 된다는 사실에 있다. 다시 말해서, 개인의 사회적 정체성이 디지털화된 개인정보에 의해 좌우될 위험성이 상존하고 있는 것이다. 일례로, 잘못된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인의 사회적 활동에 미치는 위험성은 지대할 뿐만 아니라, 나아가 개인의 인격 자체에도 치명적인 위해를 가할 수 있다.

그런데 이러한 위험성은 개인정보를 수집·처리·이용하는 각 국면에 따라 다양한 형태로 표출되어 나타난다. 여기서 이 같은 위험성을 체계적으로 인식하고 또 개인정보 보호를 위한 정책방안을 수립하기 위하여 다음의 몇 가지 개념을 구분하여 인식할 필요가 있다.[9]

첫째, 개인정보의 정확성(accuracy)의 문제이다. 데이터베이스에 수록된 개인정보가 실제와 다른 경우 그러한 틀린 개인정보에 기초해서 정책결정(정부부문)이나 경영결정(시장부문)이 행하여진다면 그것이 개인의 사회생활에 미치는 파장은 대단히 심각해진다.[10] 그렇기 때문에 개인정보는 정확하게 입력되어야 할뿐만 아니라 잘못된 정보에

9) 조동기, "정보화사회와 프라이버시",『정보화시대의 미디어와 문화』(한국언론학회·한국사회학회 엮음, 세계사, 1998), 432-436면 참조.

10) 개인정보의 정확성이 문제된 사례는 빈번히 일어나고 있다. 예컨대, 1996년에 발생한 고교 생활기록부

대한 수정이 신속하게 이루어져야 하는 것이다. 또한 시간이 경과하여 이미 입력된 자료의 내용이 時宜性을 가지지 못하는 경우에도 개인정보의 정확성을 해치게 된다. 그러나 문제는 개인정보의 오류를 발견하는 것이 용이하지 않고, 데이터베이스의 특성상 틀린 자료나 시의성이 없는 자료를 발견했다고 하더라도 그것을 수정하는 것이 쉽지 않다는 점이다.

둘째, 개인정보의 충실성(integrity)의 문제이다. 이는 주로 개인정보를 처리하는 과정에서 발생하는데, 예컨대 컴퓨터연결의 과정에서 적절하지 못한 방식으로 개인자료가 통합되거나 재분류되는 경우 출력된 개인정보는 정보주체를 정확하게 반영하는 충실성을 가지지 못하게 된다. 또한 처리프로그램의 내재적인 문제로 인하여 출력된 개인정보가 체계적으로 왜곡될 수도 있다. 이러한 문제는 하드웨어의 오작동이나 조작자의 실수에 의해 복합적으로 나타날 수도 있다. 이처럼 체계적으로 왜곡된 개인정보에 의하여 실존인격이 규정되는 경우 그 위험성은 더욱 커지게 된다.[11]

셋째, 개인정보의 보안성(security)의 문제이다. 이는 개인정보의 관리과정에서 발생하는 문제로서 외부 또는 내부에 의한 불법적인 침입에 의해 개인정보가 누출되는 경우이다. 정보통신망의 확산으로 인해 개인정보의 데이터베이스는 다른 물리적 공간에 존재하지만 상호 연결되어 있기 때문에 외부의 침입에 취약할 수밖에 없게 되었다. 최근 해킹이나 크래킹에 의한 불법적인 침입은 보안기술의 발달에도 불구하고 줄어들지 않고 있다. 또한 보안성은 내부자에 의해 의도적으로 침해될 수 있다. 즉 개인정보 데이터베이스에 합법적으로 접근할 수 있는 사람이 개인적인 이득을 취하기 위하여 개인정보를 외부에 유출하는 경우이다.[12]

전산화자료의 입력오류사건을 들 수 있다. 당시 교육부가 입시사정자료용으로 각 대학에 제공한 고교 3학년생 생활기록부 전산화 자료에 수험생의 내신석차, 주민등록번호, 재적학생수 등 일부 내용이 잘못 입력된 것으로 밝혀졌는데, 이러한 오류가 발견된 학교는 전체 1,889개 고교 중 0.4%인 70여개 학교에 달하였다. 이러한 부정확한 개인정보에 의해 개인이 입게 되는 피해는 결코 가벼운 것이 아니다.

11) 예컨대, 미국에서는 컴퓨터연결의 결과 메사추세츠주의 복지수혜자들이 사기행위를 한 것으로 드러나 법정에서 자신들의 무죄를 위해 싸워야 하는 사태가 발생하기도 하였다. 우리나라에서도 외교통상부의 여권발급전산망과 연결된 경찰청의 신원조회전산망이 세밀하지 못한 정보를 제공하여 범죄자와 이름이나 생년월일만 같아도 부적격자로 판정되어 2만여명이 여권발급을 받지 못한 경우가 있고, 또 주민등록번호의 잘못된 처리로 인하여 범죄피의자로 오인되어 수차에 걸쳐 경찰에 연행되어 조사를 받은 사례가 있다. 서유창, "개인정보보호법 제정배경과 시행성과", 『수사연구』(1996년 4월호), 17면.
이러한 사례들은 개인신상에 관한 자료의 입력과 관리가 완벽하게 이루어지더라도 자료를 처리하는 과정에서 문제가 생길 수 있음을 보여 준다. 때문에 미국에서는 정부측의 무분별한 컴퓨터연결로부터 개인정보를 보호하기 위하여 1988년에 컴퓨터연결 행위 자체를 규율하는 내용의 『컴퓨터연결과 프라이버시보호법』(Computer Matching and Privacy Protection Act)을 제정·시행하고 있다.

12) 예컨대, 백화점의 고객명단이 유출되어 범행의 대상선정에 이용된 사례가 있고, 의료보험 관련자료를 담당자가 유출하여 선거에 이용한 사례, 주민등록기록을 열람하여 가족상황을 파악한 후 독신녀의 주거지

넷째, 개인정보의 적합성(adequacy)의 문제를 들 수 있다. 이것은 개인정보의 수집 및 활용과정에서 수집목적의 정당성 및 이차적 이용의 타당성에 관련된 문제이다. 많은 비용과 시간이 요구되는 데이터베이스는 주로 특정한 목적을 위하여 구축되는데, 법률적 근거 없이 또는 정보주체의 명확한 인식 없이 불법적으로 수집되거나, 또는 수집된 개인정보가 본래의 수집목적이나 취지를 벗어나서 사용되는 경우 적합성의 위반문제가 발생한다.[13)]

요컨대, 자료입력의 정확성, 자료처리의 충실성, 자료관리의 보안성, 자료활용의 적합성이 확보되지 않는 경우 개인정보의 왜곡이 일어나게 되고, 그에 따르는 위험성은 실존인격에 치명적인 손상을 가하게 될 것이다.

4. 개인정보의 통합관리에 따르는 사이버 원형감옥의 위험성

개인정보를 장악하는 자는 물리력에 의한 권력 이상으로 그 개인을 통제하는 힘을 가지는 셈이다. 이러한 개인통제력은 또 다른 절대권력(Big Brother)을 낳게 될 것이고, 이는 결코 자유민주주의 정치질서와 양립할 수 없다.

개인의 모든 활동이 디지털화되는 정보사회에서 각 개인은 자신을 드러내고 싶지 않아도 사회적 관계를 맺기 위해서는 불가피하게 자신을 드러낼 수밖에 없는 상황에 놓여 있다. 이 거역할 수 없는 상황 속에서 그들 개인정보가 여러 가지 정보기술에 의하여 통합처리되는 경우, 개인은 문자 그대로 유리처럼 들여다 볼 수 있는 발가벗겨진 상태에 놓여 있게 된다. 이처럼 타인에게 노출하고 싶지 않은 사적 영역의 여러 측면들이 원하든 원치 않든 자신의 의지와 무관하게 노출될 수 있다는 사실만으로도 자유민주주

를 범죄의 대상으로 정한 사례, 자동차관리전산망을 통하여 외제 고급승용차의 차주를 확인하여 강도의 대상으로 삼은 사례 등 개인정보의 보안성이 침해되어 생겨나는 위험성은 결코 가벼이 넘길 수 없는 문제이다.

점차 개인정보의 불법유출 사례는 급증하고 있다. 국회의 국정감사에서 법무부가 국회 법사위에 제출한 '개인정보 유출 사범 단속실적'에 따르면 지난 94년 23건에 불과했던 개인정보 유출사범이 95년 38건, 96년 70건으로 증가한 데 이어 97년에는 3백26건으로, 94년에 비해 무려 13배나 늘어난 것으로 집계되었다. 한겨레 1998. 11. 3.자.

13) 예컨대, 경찰이 주민등록등·초본, 인감증명 등의 제반 서류발급신청인, 자동차등록신청인, 각종의 인·허가신청인 등의 명단을 입수하여 컴퓨터로 전과 및 수배사실을 조회하는 등 수배자 검거자료로 활용하는 사례를 들 수 있다. 이는 일반 시민들의 편의를 도모하기 위하여 내무행정기관에서 수집된 개인정보가 경찰의 수사목적으로 전용되고 있는 것이다. 또 지난 97년 서울시는 국민연금관리공단, 공무원연금관리공단, 사립학교교직원연금관리공단의 3개 기관에 의뢰해 지방세 체납자 245,348명의 개인정보를 넘겨받아 급여압류 및 압류예고장 발송 등의 조치를 취한 것으로 국정감사에서 밝혀지기도 하였다. 한겨레 1997. 10. 10.자.

의체제가 그 이념적 바탕으로 삼고 있는 인간존엄과 인격존중의 가치가 훼손될 수 있음은 물론이다.

더 나아가 개인정보를 축적·처리하는 공·사의 기관은 개인에 대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이다. 그리하여 이들 개인정보를 토대로 일정 부류의 사람들을 사회적으로 낙인화하는 일(예컨대, 신용불량자나 취업기피인물명단의 작성·유통)[14]이 얼마든지 가능해지게 되고, 그 결과 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수 있다.

IV. 위험성에 대한 안전장치: 정보인권으로서의 개인정보자기결정권

1. 개인정보자기결정권의 구체적 내용

개인정보자기결정권이란 자신에 관한 정보가 언제 어떻게 그리고 어느 범위까지 타인에게 전달되고 이용될 수 있는지를 그 정보주체가 스스로 결정할 수 있는 권리를 의미한다.[15] 따라서 개인정보의 수집·이용·제공이 정보주체의 결정권이 무시된 채 이루어지는 경우 개인정보자기결정권에 대한 제한이 있게 된다.

물론 이 기본권이 절대적인 것은 아니다. 타인이 행하는 정보의 수집·이용·제공에 대해 정보주체가 어느 정도 관여할 수 있을 것인지는 당해 개인정보의 성격, 수집목적. 이용형태, 처리방식에 따르는 위험성의 정도에 따라 다를 수 있다. 그러나 적어도 정보주체의 인격적 요소인 개인정보가 타인에 의해 마음대로 처리·조작되어서는 안 된다

---

14) 장영민, "정보통신망발전에 따른 개인정보보호",『형사정책연구』제26호 (한국형사정책연구원, 1996 여름), 9면.

15) 이러한 개념의 기본권을 독일 연방헌법재판소는 1983년의 인구조사판결(BVerfGE 65, 1)에서 "정보적 자기결정권"(Recht auf informationelle Selbstbestimmung)이라고 명명하였다. 이 판결에 대한 소개와 분석은, 정태호, "현행 인구주택총조사의 위헌성 -독일의 인구조사판결(BVerfGE 65, 1)의 법리분석과 우리의 관련법제에 대한 반성-", 『법률행정논총』제20집 (전남대학교 법률행정연구소, 2000), 202-218면; 김일환, "독일연방헌법법원의 인구조사판결", 『김계환교수회갑기념논문집』(1996), 66면 이하 참조. 그리고 미국은 정보프라이버시(information privacy)라고 부르고 있다.
한편, 우리의 경우 이 개념을 나타내는 용어가 통일되어 있지 않다. 예컨대, "자기정보관리통제권 또는 개인정보자기결정권"(권영성,「헌법학원론」, 법문사, 2001, 427면); "자기정보에 대한 통제권"(성낙인,「헌법학」, 법문사, 2001, 439면); "자기정보통제권"(차맹진, "프라이버시보호와 자기정보통제권", 인하대 박사학위논문, 1991); "정보자기결정권"(김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구",「공법연구」제29집 제3호, 한국공법학회, 2001); "정보의 자결권"(정태호, 같은 글) 등 다양하게 용어를 쓰고 있다.

는 것이 개인정보자기결정권의 기본정신이다. 그러므로 종래 정부가 법적 근거 없이 개인정보를 자유롭게 수집·처리해 온 관행은 개인정보자기결정권의 보장체계에서는 더 이상 용납되지 않는다.

이러한 정보주체의 자기결정권이 실질적으로 보장되기 위해서는 정보주체에게 다음과 같은 파생적 자유와 권리, 즉 익명거래의 자유, 정보처리금지청구권, 정보열람 및 갱신청구권이 보장되어야만 한다.

가. 익명거래의 자유

익명거래의 자유 또는 익명권은 정보주체가 정부 등의 타자와 온라인 교섭 또는 거래를 할 때 불필요하게 자신의 신원을 밝히지 않고 거래할 수 있는 자유를 말한다. 이 익명권이야말로 개인정보자기결정권의 헌법정신을 실현함에 있어 가장 전제되는 기본권이라고 하겠다. 오늘날 빠르게 발전하는 정보통신기술들은 정치적 및 시장의 요구와 필요에 따라 점차 모든 거래에 있어 놀라울 정도로 거래당사자의 신원확인을 가능하게 하는 방향으로 나아가고 있다. 이는 매우 우려할 사태이다. 이러한 신원확인의 흐름에 제동을 거는 법적 장치로서 익명거래의 자유가 보장되어야 한다.[16]

나. 정보처리금지청구권과 정보처리의 원칙

정보처리금지청구권은 기본적인 정보처리원칙이 충족되지 않는 경우에 개인정보의 수집·이용·제공 등의 정보처리를 금지하도록 요구할 수 있는 권리이다. 이러한 정보처리금지청구권의 인정 여부를 판단하기 위한 기준이 되는 정보처리원칙으로서 4가지 원칙을 들 수 있다.

첫째, 수집제한의 원칙이 요구된다. 개인정보자기결정권의 보장은 수집 단계에서부터 이루어져야 한다. 이것은 매우 중요한 출발점이다. 수집제한의 원칙이란 「(i) 정당한 수

16) 1994년 12월 6일 채택된 오스트레일리아의 프라이버시헌장(Privacy Charter) 제10조(익명의 거래)는 "사람들은 거래를 할 때 자신의 신원을 밝히지 않을 선택권을 가져야 하고, 이 선택권은 압도적인 공익 또는 사익에 의해 정당화되는 경우에 한하여 제한을 받는다." 고 선언하고 있음에 주목할 필요가 있다. <http://www.anu.edu.au/people/Roger.Clarke/DV/PrivacyCharter.html> 참조. 또한 1997년의 독일 정보통신정보보호법(TDDSG) 제4조 제1항은 인터넷에서 이용자의 익명성보호를 서비스제공자의 목표로 설정하고 있다. 즉 "서비스제공자는 기술적으로 가능하고 합리적인 범위 내에서 이용자가 익명 또는 가명으로 서비스를 이용하고 또 비용지불을 할 수 있도록 하여야 한다. 서비스제공자는 이러한 선택에 대해 이용자에게 고지하여야 한다."고 규정하고 있는 것이다. 그러나 우리의 현행 법제는 익명화기술이나 암호기술이 개발되고 활용될 수 있는 법적 조건을 확보하지 못하고 있는 것으로 보인다.

집목적 하에 (ii) 필요한 범위 내에서 (iii) 공정하고 합리적인 방식으로 (iv) 정보주체의 분명한 인식 또는 동의 하에 수집되어야 한다」는 원칙이다. 수집목적의 정당성, 수집범위의 필요최소성, 수집방식의 합리성[17], 정보주체의 인식명확성[18] 요건의 판단은 관련되는 이익의 형량을 통해 결정되어야 할 것이다. 다만, 수집에 있어서의 동의권은 반드시 절대적일 수는 없다. 수집동의권의 인정 여부는 수집되는 개인정보의 민감성, 수집목적과 처리방식(예컨대, 분산관리냐 통합관리냐 등)에 따라 달라질 수 있을 것이다.

둘째, 목적구속의 원칙이 요구된다. 목적구속의 원칙이란 「개인정보를 수집하는 목적은 (i) 수집 당시에 명확히 특정되어 있어야 하고(목적의 특정성), (ii) 그 후의 이용은 이 특정된 수집목적과 일치되어야 한다(목적일치성)」는 원칙이다.[19] 이 원칙에서의 "이용"에는 "제3자 제공"은 포함되지 않고, 수집기관 내부의 자체 이용만을 의미한다. 제3자 제공의 경우에는 수집제한의 원칙과 목적구속의 원칙이 별도로 적용된다고 할 것이다.[20]

셋째, 시스템공개의 원칙이 요구된다. 시스템공개의 원칙이란 「개인정보처리시스템의 설치 여부, 설치목적, 정보처리방식, 처리정보의 항목, 시스템운영책임자, 처리시스템에 의한 자동결정이 이루어지는지 여부 등이 일반에게 투명하게 공개되어야 한다」는 원칙이다. 비밀리에 운용되는 개인정보처리시스템은 그 자체 개인정보자기결정권에 위협적인 요소가 되기 때문이다. 그리고 이 시스템공개의 원칙은 정보주체의 열람청구권과 갱신청구권 행사의 전제가 된다.

넷째, 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. 이것은 실존인격과 분리된 개인의 총체적인 인격상이 정부의 수중에 들어가는 것을 방지하기 위한 것이다.

이는 오늘날 컴퓨터결합(computer matching)이나 컴퓨터프로파일링(computer profiling) 등의 기법에 의한 정보통합이 기술적으로 용이하게 이루어질 수 있는 상황, 그리하여

---

17) 예컨대, 수집되는 개인정보에 기초해서 당해 정보주체에게 불이익한 행정결정이 내려질 수 있는 경우에는 가능한 한 당해 정보주체로부터 직접 수집되어져야 한다.

18) 자신에 관한 정보가 어떤 법적 근거 하에서 어떤 목적을 위하여 어떤 기관에 의해 어떻게 이용될 것인지를 당해 정보주체가 명확하게 인식할 수 있어야 한다. 독일에서는 이것을 연방헌법재판소의 결정(BVerfGE 65, 1)에 따라 일반적으로 규범명확성의 원칙이라고 표현하고 있다. 김일환, "개인정보보호법의 개정필요성과 내용에 관한 연구",『공법연구』제26집 제2호 (한국공법학회, 1998), 235면.

19) 독일에서도 "목적구속의 원칙"으로 불리어진다. 김일환, 위의 글, 235면; 김연태, "행정상 개인정보보호",『저스티스』제34권 제5호(한국법학원, 2001. 10), 210면 참조.

20) 김연태, 위의 글, 212면도 "정보제공의 경우에도 목적구속의 원칙이 적용되어야 함은 분명하다."고 설명하고 있다.

개인에 대한 광범위하고 엄청난 양의 정보를 소유하고 있는 정부가 개인의 총체적인 인격상을 마음만 먹으면 언제든지 획득할 수 있는 상황에서 요구되는 원칙이다. 그러므로 정부가 포괄적인 개인정보통합관리시스템을 구축하는 것은 이러한 개인정보분리의 원칙에 정면으로 반하는 것으로서 헌법적으로 허용되지 않는다고 하겠다.

물론 개인정보분리의 원칙이 절대적일 수는 없다. 그러나 개인정보의 통합이 허용되기 위해서는 기본권제한의 법리를 규정한 헌법 제37조 제2항 소정의 법률유보의 원칙과 비례의 원칙을 충족시켜야 할 것이다. 즉, 명시적인 법률의 근거 하에서 중대한 공익을 위해 불가피한 경우에 한하여 필요한 범위 내에서 개인정보의 통합이 허용될 수 있다고 하겠다.

다. 정보열람 및 정보갱신청구권

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 일거수 일투족에 관한 상세한 정보가 쉽고 값싼 비용으로 무한대로 저장·처리될 수 있고, 그러한 가상인격에 기초해서 실존인격에 영향을 미치는 결정이 이루어질 수 있는 정보사회에서 특히 위험한 요소는 한번 입력된 정보가 자동으로 지워지지 않는다는 사실에 있다. 낡고 틀린 정보가 지워지지 않은 상태로 계속 존재하면서 실존인격에 영향을 미칠 수 있는 가능성을 차단하기 위해서는 이 같은 정보열람청구권과 정보갱신청구권이 확실하게 보장되어야 한다.

2. 개인정보자기결정권의 헌법이론적 논거

가. 인간존엄의 보장 기능

개인정보자기결정권은 일차적으로 인간존엄의 존중과 개인의 인격보호라는 기능을 수행한다. 그 주된 목적은 각 개인의 존엄, 품위, 개성, 자율성을 촉진시키는 것이다. "사람은 자신의 인격, 신체 그리고 그 정신의 주권자이다."라고 J. S. Mill이 갈파한 바와 같이,[21] 개인의 존엄과 인격의 존중은 모든 자유사회의 기본원리이다.

---

21) John S. Mill, "On Liberty", in: Utilitarianism, ed. Mary Warnock (Glasgow: Fontana, 1962), p. 135.

자기의 정체성 및 인격의 완전성을 확보하고, 자기 나름의 독자적인 인간관계를 형성하며 자신만의 구원방법을 찾기 위해서는, 각 개인은 타자와 관계하는 영역을 한정적으로 설정하고 자신만의 고유영역을 확보할 수 있어야 한다. 무엇보다도 인간은 자기 자신만의 생각과 느낌, 믿음과 회의, 희망, 계획, 두려움과 환상을 자신의 내부에 비밀스럽게 간직할 수 있어야만 한다. 거기에는 다른 이유가 없다. 단지 그가 그러한 내면의 것들을 누구하고 어느 정도로 공유할 것인지를 자유로이 선택할 수 있기를 원하기 때문이다.[22]

개인의 행동과 그 역사는 그것을 행한 본인 자아의 한 부분이며, 그러한 자아의 부분은 그것을 함께 공유하기를 원하는 사람하고만 공유되어야 한다. 이러한 전제가 확보되지 않을 때 개인의 자아는 완전할 수 없고 인간존엄은 확보될 수 없다. 개인의 인격발현도 완전한 자아의 확보로부터 출발되어야 하는 것이다. "외부의 누군가가 나에 관한 무언가를 알고 있다"는 두려움과 불안감은 개인의 소외감을 형성시키고 자유의 습관을 대체하게 될 것이다. 더 나아가, 분산되어 있던 개인정보가 통합처리되고 그 결과 타자 앞에 알몸으로 드러나 있는 개인은 더 이상 자유로운 인격체로서 존립할 수 없으며 타자와의 의사소통관계도 온전할 수 없다. 상대방이 자기에 대하여 얼마만큼 아는지를 모르면서 개인이 자신의 결정을 자율적으로 행사한다는 것은 거의 불가능하다.[23]

결국, 개인정보에 대한 통제권의 상실은 필연적으로 인간으로서의 존엄과 자율성의 상실로 이어진다. 따라서 개인정보의 축적·처리가 무한대로 이루어지는 정보사회에서 개인정보자기결정권은 인간성의 본질적인 구성요소이며 인간존엄과 인격보호를 위한 핵심적인 기본권이 아닐 수 없다.

나. 자유민주적 기본질서의 유지 기능

두 번째의 논거는 정보기술이 독재의 도구로 전락될 수 있다는 가능성에 기초하고 있다. 권력제한적인 정부(limited government)에 대한 고전적인 자유주의적 신념은 권력에 대한 불신으로부터 생겨난 것이다. 정보기술은 시민 개인에 관한 방대한 양의 정보를 수집하고 조작할 수 있는 정부의 권력을 향상시킨다. 이제 개인정보를 장악하는 정부는 물리력에 의한 권력 이상으로 그 개인을 통제하는 힘을 가지는 것이다. 이러한 개인통제력은 또 다른 절대권력(Big Brother)을 낳게 될 것인바, 이는 결코 자유민주주

22) Justice(the British Section of the International Commission of Jurists), Privacy and the Law (London: Justice, 1970), p. 4.
23) BVerfGE(독일연방헌법재판소 판결집) 65, 1 [43].

의 정치질서와 양립할 수 없다.

자유민주주의체제 하에서 국가라고 하는 정치적 공동체는 일체론적(holistic) 구성체가 아니라 원자론적(atomistic) 구성체이다. 즉 국가란 그 구성원 개개인을 초월하는 어떤 존재가 아니다. 정부는 시민들에 의해서 구성되며 언제나 그들에게 책임을 져야 한다. 자유민주주의체제란 불가양의 인권, 권력제한적인 정부, 법의 지배, 국가의 정치영역과 시민사회의 영역의 분리를 의미한다. 즉 개인적 및 사회적 자율성의 확보야말로 자유민주주의질서의 기본적 전제조건인 것이다. 그리고 개인이 민주적인 정치적 결정과정에 적극적으로 참여하기 위해서는 누가, 무엇을, 언제 그리고 어떤 목적에서 자기에 관하여 얼마만큼 알고 있는지를 인식할 수 있어야만 한다. 그런데 정부가 개인정보의 통합처리를 통해서 개인의 일거수일투족을 빤히 들여다 볼 수 있는 상황에서는 개인의 정치적 의사형성과 사회적 자율성은 상실되어 버릴 것이다.[24] 결국 개인의 사적 영역을 국가의 감시와 통제로부터 보호하는 것은 바로 자유민주체제의 불가결의 전제조건인 것이다.

이미 1969년에 Stone과 Warner는 개인정보처리가 지닌 민주주의에 대한 위험성을 다음과 같이 경고한 바 있다: "컴퓨터는 정부의 손에 '아는 능력'(power to know)을 쥐어줌으로써 설령 全能(omnipotence)은 아니라 하더라도 全知(omniscience)의 힘을 부여한다. 기록되지 않는 사실이란 하나도 없고, 어떠한 사실도 잊혀지거나 소실되지 않으며, 그 어떤 것도 용서되는 것이란 없다."[25] 또한 미국 최초의 프라이버시보호법(Privacy Act of 1974)을 제정하는데 주도적 역할을 담당했던 Sam Ervin 상원의원은 "한정된 목적에서 시민들에 대해 결정을 내리는 이 나라의 모든 공무원들은 시민 개인에 관한 모든 가능한 정보를 수집하여 그 '개인의 전체상'(total man)을 알고자 하는 욕구에 사로잡혀 있는 것으로 보인다."고 공언하였다.[26] 사실 유럽에서도 개인정보보호법이 제정되게 된 주된 동기 중의 하나는 1930년대와 40년대 나찌정권과 파시스트 정권하에서의 경험의 재발을 방지하기 위한 것이었다.[27]

요컨대, 정보사회에서 개인정보자기결정권은 자유민주주의체제를 유지하기 위한 전제조건이다. 그밖에 개인정보자기결정권은 이러한 일반적인 역할 속에서 몇 가지 다른 기

24) 김일환, 『개인정보보호법제의 정비방안에 관한 연구』(한국법제연구원, 1997), 14면.

25) Britons Michael Stone & Malcolm Warner, "Politics, Privacy, and Computers", The Political Quarterly Vol. 40 (1969), p. 260.

26) Sam J. Ervin, Jr., "Privacy and Government Investigations", University of Illinois Law Forum (1971), p. 138.

27) Colin J. Bennett, Regulating Privacy : Data Protection and Public Policy in Europe and the United States (Ithaca : Cornell University Press, 1992), p. 30.

능을 수행한다: (1) 일상생활의 전면적인 정치화를 방지하며 (2) 종교적인 다원성과 관용을 뒷받침하며 (3) 자발적인 결사에의 참여를 보장하고 (4) 자유로운 학문적인 탐구를 보호하며 (5) 정부가 시민의 투표기록을 조사하는 것을 금지시킴으로써 선거과정을 보호하며 (6) 강제적인 自己負罪나 불법적인 수사행태를 차단시키는 방어벽으로서 기능하며 (7) 정부가 시민에 대해 책임을 질 수 있도록 활동하는 언론기관이나 기타 기관들의 활동을 보호한다.[28]

다. 다른 기본권의 보호 기능

개인의 존엄과 자유민주적 질서의 확보는 개인정보자기결정권의 직접적인 기능이다. 그밖에 개인정보자기결정권은 기타의 다른 기본권을 보장하기 위한 수단적인 기본권으로서의 기능을 수행한다. 개인정보보호에 대하여 경제적 분석방법을 적용한 Richard Posner는 개인정보보호를 다른 효용성을 획득하기 위한 중간매개로서의 경제적 재화로 분석한 바 있다.[29]

정보사회에서 개인은 자신의 실존인격 외에 사이버스페이스에 또 하나의 가상인격을 가지게 되는데, 개인정보처리의 위험성은 이러한 가상인격이 실존인격을 규정짓게 된다는 사실에 있다. 다시 말해서 개인의 사회적 정체성이 디지털화된 개인정보에 의해 좌우될 위험성이 상존하고 있는 것이다. 일례로 잘못된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인이 입게 되는 피해는 정확히 예측하기 힘들 정도로 그 파장이 크다. 범죄자로 오인되어 체포되는 경우 신체의 자유가 침해되고, 신용거래불량자명단에 잘못 이름이 기록되는 경우 경제적 생활에 치명적인 손상을 입는 것은 아주 비근한 예에 불과하다. 취업기피인물명단의 유통 등 고용에 있어서의 차별, 복지수혜자의 자격배제, 공동체생활에서의 명예의 상실 등 개인정보의 정확성(accuracy)과 충실성(integrity)이 확보되지 못한 결과로 오는 피해는 엄청나다. 나아가 개인정보의 보안성(security)과 적합성(adequacy)이 결여되어 강력범죄의 표적이 되는 경우 생명권마저도 위협받을 수 있다.

각국에서 개인정보보호법을 처음에 제정하게 된 이유 중의 하나도, 이처럼 개인의 인격과 분리될 수 없는 개인정보가 인격이 없는 기관의 시각으로 이것을 처리·사용하여 개인에 관한 불리한 경제적 및 사회적 결정을 내리게 된다는 사실에 있었던 것이다.[30]

---

28) Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967), pp. 24-25.

29) Richard A. Posner, "An Economic Theory of Privacy", in: Philosophical Dimensions of Privacy, ed. Ferdinand D. Schoeman(Cambridge: Cambridge University Press, 1984), pp. 333-345.

특히 봉급, 보험, 건강, 신용 등 수많은 영역에서 개인이 가지는 권리나 이익에 영향을 미칠 어떤 결정들이 자신의 개인정보에 기초해서 타인에 의하여 행하여지는데도 이러한 결정과정에 정작 정보주체인 자신은 참여할 수 없다는 사실이 사태를 더욱 어렵게 만든다.

요컨대, 개인은 자신의 개인정보가 정확하고 적절하며 시의성이 있어야 한다는 것, 그 정보는 정당한 권한을 가진 사람들에 의해서만 사용되어야 한다는 것, 그리고 그것을 알아야 될 필요가 있는 사람 이외의 사람에게 전달되어서는 안 된다는 것을 보장받을 권리를 가지며, 이러한 개인정보자기결정권이 확보되지 않고서는 가상인격이 실존인격을 규정짓는 정보사회에서는 여타의 다른 기본권도 온전하게 보장될 수 없다. 따라서 정보사회에서 개인정보자기결정권은 헌법상의 다른 기본권을 보장하기 위한 수단적 기본권으로서의 기능을 수행하는 것이다.

3. 개인정보자기결정권의 법적 성격과 의의

개인정보자기결정권과 종래의 사생활권은 어떻게 다른가? 개인정보보호와 사생활비밀보장은 구별되는 문제인가?

종래 사생활보호를 위한 헌법상의 보호장치, 즉 압수·수색에 있어서의 영장주의(헌법 제12조 제3항 및 제16조 제2문), 주거의 자유보장(헌법 제16조 제1문), 사생활의 비밀보장(헌법 제17조), 그리고 통신비밀침해금지(헌법 제18조) 등의 사생활권은 '사적인 사항이 공개되는 것을 원치 않는 이익'을 그 보호법익으로 하고 있었다.

그러나 개인정보자기결정권이 인정되는 사회적 연관은 전혀 다르다. 즉 이 기본권에 대한 요구는 디지털화된 개인정보가 정보주체도 인식하지 못한 채 타인의 수중에서 무한대로 수집·축적·처리·가공·이용·제공될 수 있는 새로운 정보환경, 나아가 분산된 개인정보들을 단일의 기록파일에 의해 언제든지 통합관리함으로써 실존인격과 분리된 또 하나의 가상인격이 디지털화된 상태로 존재할 수 있는 정보환경에서 생겨난다. 그리하여 이 타인의 수중에 있는 디지털화된 가상인격에 의해 실존인격이 규정됨으로써 실존인격에 가해질 위험성이 극도로 높아지는 상황, 특히 정부나 민간에 의해 개인정보통합관리시스템이 구축됨으로써 개인이 정부나 기업 앞에 알몸으로 드러날 수 있

30) 독일의 연방데이터보호법(Bundesdatenschutzgesetz) 제1조도 개인정보가 저장, 전달, 수정 및 처리되는 과정에서 잘못 이용되지 않도록 함으로써 보호되어야 할 다른 개인의 권리와 이익이 침해되는 것을 막기 위한 것이 이 법의 목적임을 밝히고 있다.

는 상황에서 요구되는 기본권이다.

이처럼 전통적인 사생활권이 개인의 사적 영역을 외부의 침입이나 개입으로부터 소극적으로 보존하고자 하는 데에 초점이 맞추어져 있었다면, 개인정보자기결정권은 타인에 의한 개인정보의 무분별한 수집·축적·처리·가공·이용·제공에 대해 정보주체에게 적극적인 통제권을 부여하고자 하는 데에 그 핵심이 있다.[31] 즉, 종래의 사생활권이 "은둔으로서의 사생활보호"(privacy as seclusion)에 그 중심이 있었다면, 개인정보자기결정권은 "참여로서의 사생활보호(privacy as participation)"라는 가치를 담고 있다고 하겠다. 따라서 그 보호의 맥락과 보호범위, 그리고 보호내용이 동일하지 않다.

4. 개인정보자기결정권의 효력범위

개인정보자기결정권이 미치는 효력범위는 어디까지인가? 다시 말해서, 정보주체는 타인의 어떠한 개인정보처리에 대해 통제권을 행사할 수 있는가? 예컨대, 우편배달부가 새로 이사온 이웃사람의 이름을 물어보는 경우에도 개인정보자기결정권의 효력이 미치는가?

개인정보자기결정권은 개인인격의 구성요소들이 전자적 형태로 기록화됨으로써 정보주체의 총체적인 인격상이 타인의 수중에 들어가는 위험성을 사전에 차단하기 위해 요구되는 기본권이다. 따라서 이 같은 위험성이 없는 개인정보의 수집·처리에 대해서는 개인정보자기결정권의 효력이 미치지 않는다고 보아야 한다. 우선, 인간의 기억에 의해 입력·처리되는 경우와 같이 기록화되지 않는 개인정보의 수집은 효력범위에서 제외된다. 기록화되는 경우에도 다른 기록된 개인정보와 통합될 가능성이 없는 단편적인 기록화는 효력범위에서 제외된다고 보아야 할 것이다. 따라서 위 예에서처럼 우편배달부가 이웃사람의 이름을 단순히 물어보거나 메모하는 경우에는 개인정보자기결정권에 대한 제한 자체가 없다고 보아야 하고 따라서 이러한 수집에 대해서는 법률유보의 원칙이 적용될 여지가 없다.[32]

그러나 기록방식이 수기방식이라 하더라도 그것이 다른 수기기록 또는 전자기록과 통합될 가능성이 있는 경우에는 개인정보자기결정권의 효력이 미친다. 이 경우 통합가

31) 성낙인, "행정상 개인정보보호", 『공법연구』 제22집 제3호(한국공법학회, 1994), 288면.

32) 김연태, 앞의 글(각주 19), 208면은 국가에 의한 모든 개인정보의 수집·처리에 대하여 법적 근거가 필요한 것은 아니고, "법적으로 의미 있는, 정보의 자기결정권에 대한 침해를 가져오는 정보수집·처리의 경우에 법적 근거가 요구되는 것이다."고 하고, 독일 문헌을 인용하면서 위 우편배달부의 경우 정보의 자기결정권에 대한 "침해"가 아니라고 설명하고 있다.

능성은 그 수집목적과 처리방법 등을 기준으로 결정될 수 있을 것이다.

이러한 통합가능성이 있는 한, 정보주체로부터의 직접적인 수집·처리가 아니더라도 효력이 미치며, 또한 이미 공개된 개인정보를 수집·처리하는 경우에도 개인정보자기결정권의 효력이 미친다고 하겠다.

5. 개인정보자기결정권의 보호객체 : 개인정보의 개념

개인정보자기결정권의 보호객체는 "개인정보", 즉 "신원을 확인할 수 있는 개인에 관한 일체의 정보"이다. 따라서 신원을 확인할 수 없는 형태로 수집·처리되는 어떤 개인에 관한 정보는 여기의 개인정보에 해당하지 않는다. 그러나 이 같은 비신원확인정보라도 그 속에 개인의 신상정보가 담겨 있고, 다른 개인정보들과 결합하여 쉽게 신원확인이 가능한 경우가 많다. 그러므로 다른 개인정보들과 결합하여 쉽게 신원확인이 가능한 비신원확인정보도 개인정보자기결정권의 보호대상이 된다고 할 것이다. 예컨대, 인터넷상에서 비실명의 ID에 의한 기록파일은 그 ID가 다른 신상정보(주민등록번호, 이름 등)와 쉽게 연결될 수 있는 경우에 그 기록파일은 개인정보에 해당된다.

이 같은 맥락에서 공공부문의 개인정보보호에 관한 일반법이라고 할 수 있는 공공기관의개인정보보호에관한법률 제2조 제2호가 "개인정보"의 개념을 "생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)"[33]라고 정의하고 있는 것은 타당하다고 하겠다.

또한 1차 수집된 자료들을 분석하여 얻은 개인에 관한 2차 정보도 당연히 개인정보자기결정권의 효력이 미치는 개인정보에 해당된다.

한편, 개인정보자기결정권의 보호대상인 "개인정보"는 개인의 "비밀"정보만이 해당되는 것이 아니다. 여기의 개인정보는 헌법 제17조의 "사생활비밀의 불가침"조항 및 제18조의 "통신비밀의 불가침"조항에서 보호하는 개인의 "비밀"보다 넓은 개념이다.[34] 공

33) 이 개념규정 중 괄호 안의 이른바 '결합에 의한 식별정보'란 예컨대 성명이나 주민등록번호가 기록되지 않은 파일이라도 생년월일이 기록되어 있다면 생년월일 순으로 검색한 후 그 결과를 주민등록번호와 성명이 기록되어 있는 파일과 대조할 경우 정보주체를 식별할 수 있는 경우 등을 의미한다. 총무처, 「축조해설 개인정보보호법」, 1994, 34면.

34) 정태호, 앞의 글(각주 15), 206면도 같은 취지에서 헌법 제17조의 "사생활비밀"을 해석하고 있는 것으로 판단된다. 그는 "제17조의 조문에 충실하게 그 조문의 내용을 해석할 때 제17조를 통해서 미국에서 논의

개된 장소에서 개최되는 정치적 집회 등에 참여하는 경우와 같이 공개적으로 이루어지는 개인의 행동에 관한 정보도 국가에 의하여 지속적이고 체계적으로 수집·처리되고 나아가 이들 정보가 다른 개인정보들과 결합되는 경우 개인의 전체적인 인격상이 쉽게 드러날 수 있기 때문이다.

여기서 사생활비밀의 불가침조항(제17조), 통신비밀의 불가침조항(제18조), 그리고 개인정보자기결정권의 관계설정이 문제된다. 개인의 사생활비밀과 통신비밀은 모두 개인정보자기결정권의 보호대상이기도 하다. 그러나 사생활비밀과 통신비밀에 해당하는 개인정보에 대해서는 그 수집단계에서부터 더욱 철저한 보호가 요구된다는 것을 헌법이 천명한 것이라고 하겠다.[35] 중대한 국가이익의 보호를 위해 불가피하게 요구되는 경우 엄격한 절차적 보장 하에서만 사생활비밀과 통신비밀에 대한 수집이 허용될 수 있을 뿐이다.[36] 특히 개인의 인격실현에 중대한 침해를 야기할 수 있는 일정한 비밀정보에 대해서는 수집 자체가 금지되어야 할 것이다. 공공기관의개인정보보호에관한법률 제4조 본문이 "사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보"의 수집 자체를 금지하고 있는 것은 일응 타당하다고 하겠다.[37]

되는 프라이버시권이나 독일에서 논의되는 일반적 인격권을 우리 헌법에 모두 수용하는 데는 실패했다."고 평가하고 있다.

35) 한편, 사생활비밀과 통신비밀의 관계는 일반법과 특별법의 관계로 이해된다. 후자는 "통신", 즉 "비공개를 전제로 한 정보의 송신 또는 수신의 과정"을 제3자의 침해로부터 특별히 보호하고자 하는 것으로서, 그 통신내용·통신형태·통신내역이 특별히 "비밀"로 취급된다는 것을 헌법이 선언한 것이다. 사실 통신비밀의 보장은 사생활보호의 수단적인 의의를 가지는 것(허영, 『한국헌법론』, 박영사, 2001, 372면; 성낙인, 『헌법학』, 법문사, 2001, 446면)을 넘어서서, 헌법 제21조가 보장하는 언론·출판, 집회·결사의 자유를 보장하기 위한 불가결한 전제조건이기도 하다. 왜냐하면, 사회적 소수자의 비공개를 전제로 한 의사전달의 과정은 곧 헌법 제21조가 보장하는 헌법적 가치인 민주주의 실현의 중요한 한 요소이기 때문이다. 통신비밀보장의 이 같은 측면에 대한 상세는, 이인호, "방송·통신의 융합과 언론의 자유", 『공법연구』 제28집 제4호, 한국공법학회, 2000, 249-250면 참조.

36) 통신의 "내용"을 보호하고자 하는 통신비밀보호법은 이러한 헌법원칙에 부합하는 것으로 일견 볼 수 있다(철저한 분석은 여기서 생략). 그러나 이와는 달리 통신의 이른바 "내역정보"(송·수신인, 통신시간 등 traffic data)는 헌법 제18조의 동일한 보호대상임에도 불구하고 전기통신사업법 제54조에서 별도로 규율하고 있고, 그 보호의 정도는 헌법적 요청에 충실하지 못한 것으로 판단된다.

37) 그렇지만 '사상·신조 등'의 예시가 너무 제한적이고 '기본적 인권을 현저하게 침해할 우려'의 개념이 불명확하다는 비판이 제기되고 있다(최영규, "공공기관의 정보관리와 개인정보보호", 『경남법학』 제13집, 경남대학교 법학연구소, 1998, 49면). 또한 그 단서에서 "다른 법률에 수집대상 개인정보가 명시되어 있는 경우"에는 예외를 널리 인정하고 있어 본문의 원칙이 크게 퇴색되고 있다고 하겠다.

V. 현행 공공부문 개인정보보호법제의 문제점 분석

1. 전자정부법상의 행정정보공동이용의 원칙

정보기술의 활용을 통하여 작고 효율적인 시민위주의 질 좋은 행정서비스를 제공하는 이른바 전자정부를 실현하기 위해 2001년 3월 28일 제정된 「전자정부구현을위한행정업무등의전자화촉진에관한법률」(이하 "전자정부법"이라 한다)은 전자정부의 운영원칙의 하나로서 행정정보공동이용의 원칙과 개인정보보호의 원칙을 선언하고 있다. 즉, 제11조(행정정보공동이용의 원칙)는 "행정기관은 수집·보유하고 있는 행정정보[38]를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다."고 규정하고 있고, 제12조(개인정보보호의 원칙)는 "행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다."고 선언하고 있다.

그러나 이 법상의 개인정보보호의 원칙은 선언에 불과할 뿐 이를 구체화하는 규정은 존재하지 않으며, 대신 행정정보공동이용의 원칙에 보다 초점을 맞추고 있다. 동법 제21조는 행정기관간에 행정정보를 공동이용하도록 의무지우고 있고, 특히 "공공기관의개인정보보호에관한법률 제10조 제2항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보"를 공동이용 대상정보의 하나로 규정하고 있다. 그리고 동법 제22조는 행정정보공동이용의 절차를 규정하고 있으나, 이 규정은 공동이용의 활성화를 위한 일반적 절차를 규정한 것일 뿐 달리 개인정보보호를 위한 절차적 제한을 가하고 있는 규율은 아니다.

결국, 전자정부법에 의한 개인정보의 공동이용을 통제할 수 있는 장치는 일반법인 공공기관의개인정보보호에관한법률에 일임되어 있다고 하겠다. 전자정부법상 의무적인 공동이용의 대상이 되는 개인정보의 범위도 또한 위 공공기관의개인정보보호에관한법률 제10조 제2항의 규율범위에 달려 있는 문제인 것이다. 그렇다면, 현재 공공부문에서 개인정보자기결정권이 어느 정도 보장되고 있는지의 판단은 공공기관의개인정보보호에관한법률의 규율체계의 분석에 달려 있다고 하겠다. 아래에서는 위에서 살핀 개인정보자기결정권에 담긴 헌법적 요청을 판단의 기준으로 삼아 위 법률의 한계와 문제점을 분석한다.

---

38) "행정정보"라 함은 "행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것"을 말한다(법 제2조 제4호). 따라서 개인정보도 여기의 행정정보의 개념에 속한다.

2. 공공기관개인정보법의 한계와 문제점

가. 서언

공공부문에서 개인정보자기결정권을 구체화하는 법률로서 공공기관의개인정보보호에 관한법률(이하 "공공기관개인정보법"이라 한다)[39]이 시행되고 있다. 이 법은 공공기관[40]의 컴퓨터에 의하여 처리[41]되는 개인정보[42]를 보호하기 위하여, 각 행정기관이 개인정보처리시스템 내지 개인정보DB, 즉 개인정보화일[43]을 보유[44]하고자 하는 경우에 그 보유범위 및 내부적 절차를 규율하고, 개인정보화일에 개인별로 수록된 개인정보(이른바 "처리정보")[45]를 이용하거나 제3자에게 제공하는 것에 대해 일정한 실체적 및 절차적 제한을 가하며, 정보주체에게는 열람 및 정정청구권을 인정하는 것을 주된 내용으로 하고 있다.

이 법은 공공기관의 컴퓨터에 의하여 수집·이용·제공되는 개인정보의 보호를 위한 일반법으로서, 다른 법률에 특별한 규정이 있는 경우에는 그 특별규정에 따른다(법 제3조 제1항). 그리하여 공공부문에서 개인정보의 수집·이용·제공을 규율하는 몇 가지 특별법이 존재하고 있다.

결론적으로, 개인정보자기결정권을 구체화하는 일반법인 공공기관개인정보법은 여러 가지 한계와 문제점을 가지고 있는 것으로 분석된다.

---

39) 법률 제4734호로 1994. 1. 7. 공포되어 1995. 1. 8.부터 시행된 이후 1998. 12. 24. 부분적으로 개정되었다. 미국 연방의 공공기관개인정보보호법인 Privacy Act가 1974년에 제정되었고, 독일의 연방데이터보호법이 1977년에, 프랑스의 「정보처리·축적 및 자유에 관한 법률」이 1978년에, 일본의 「행정기관이 보유하는 전자계산기처리에 따른 개인정보의 보호에 관한 법률」이 1988년에 제정된 것과 비교하면, 공공부문에서의 우리의 입법적 대응은 매우 뒤늦은 것이다.

40) 이 법의 규율대상인 공공기관에는 '국가행정기관, 지방자치단체, 각급 공·사립학교, 정부투자기관, 특별법에 의해 설립된 특별법인(단, 금융기관 제외)'이 속한다(법 제2조 제1호 및 시행령 제2조).

41) "처리"라 함은 "컴퓨터를 사용하여 정보의 입력·저장·편집·검색·삭제 및 출력 기타 이와 유사한 행위를 하는 것"을 말한다(법 제2조 제3호).

42) "개인정보"라 함은 "생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)"를 말한다(법 제2조 제2호).

43) "개인정보화일"이라 함은 "특정개인의 신분을 식별할 수 있는 사항에 의하여 당해 개인정보를 검색할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 컴퓨터의 자기테이프·자기디스크 기타 이와 유사한 매체에 기록된 것"을 말한다(법 제2조 제4호). "개인정보화일"이라는 용어는 적절하지 못하며, "개인정보처리시스템" 내지 "개인정보DB"라는 용어가 이해하기 쉬운 것으로 보인다.

44) "보유"라 함은 "개인정보화일을 작성 또는 취득하거나 유지·관리하는 것(개인정보의 처리를 다른 기관·단체 등에 위탁하는 경우를 포함하되, 다른 기관·단체 등으로부터 위탁받은 경우를 제외한다)"을 말한다(법 제2조 제6호).

45) 법률상의 "처리정보"라는 용어의 사용은 적절하지 않은 것으로 보인다. 개인정보DB에 개인별로 수록되는 "개인기록"(record)과 이 개인기록상의 여러 항목(field)에 담긴 개인정보들을 구별하지 않고 있다.

나. 규율범위에 있어서의 한계

(1) 보호대상의 제한

우선, 이 법의 규율대상은 '컴퓨터에 의하여 처리되는 생존하는 자연인의 개인정보'로 한정되어 있다. 여기서의 개인정보는 '신원확인이 가능한 개인에 관한 일체의 정보'를 가리키는 것으로 그 범위가 대단히 넓다. 즉 개인의 신상정보 내지 인격적 특성에 관한 정보뿐만 아니라 재산상황, 채권채무관계, 친구관계, 구매습관이나 취향 기타 각종의 사회경제적 활동에 관한 모든 정보가 포함된다.[46] 이 법이 이처럼 개인정보의 범위를 넓게 잡은 것에 대해 강경근 교수는 의미 있는 평가를 내리고 있다. 즉 "이는 개인정보의 보호에 관한 우리의 최초의 실정법이 이미 인격권적 의미의 프라이버시라는 전제를 극복하고 정보사회에서의 개인정보가 지니는 함의 즉 그 다양성과 대량적 이용가능성 등에 따른 정보의 재산적 성격도 배제한 것은 아니라는 점을 지적할 수 있다."고 한다.[47]

사실, 정보사회에서 개인정보의 처리와 관련한 사생활보호의 모델은 산업사회에서와 같이 은둔으로서의 사생활보호(privacy as seclusion)를 뛰어 넘어 민주적 참여의 가치를 담고 있는 사생활보호(privacy as participation)의 모델로 전환되어야 한다. 이러한 관점에서 공공기관개인정보법이 신상정보 외에 개인에 관한 일체의 정보를 그 보호대상으로 설정한 것은 긍정적으로 평가되어야 할 것이다. 그러나 동일한 맥락에서, 자연인에 관한 정보만을 보호대상으로 하고, 동일한 사회적 활동단위인 법인이나 단체에 관한 정보를 제외하고 있는 것은 아직 참여로서의 사생활보호의 가치를 전면 수용하지 못하고 있는 아쉬운 부분이라고 하겠다. 그리고 수기화일에 의해 처리되는 개인정보를 제외하고 있는 것도 이 법의 결함이라고 하겠다.[48]

특히, 이 법은 행정기관이 다양한 방식으로 수집·처리하고 있는 모든 형태의 개인정보를 보호하는 것이 아니고, 일정한 개인식별자(personal identifier)에 의해 검색할 수 있도록 체계적으로 구성된 개인정보처리시스템, 즉 개인정보화일에 담긴 개인정보(이른바 "처리정보")만을 그 보호대상으로 하고 있음에 유의할 필요가 있다.

(2) 적용범위의 제한 : 기본법으로서의 성격 부존재

법 제3조 제1항은 "공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법이 정하는 바에 의한다."

46) 심지어 총무처, 「축조해설 개인정보보호법」, 1994, 32면은 개인사업자의 당해 사업에 관한 정보도 여기에 포함되는 것으로 해석하고 있다.
47) 강경근, 「행정정보의 공동이용에 따른 법적 과제」, 한국법제연구원, 2001, 53면, 각주 26.
48) 성낙인, 앞의 글(각주 31), 295면.

고 규정하고 있다. 그러나 일반법으로서의 성격을 나타내는 이 규정은, 필자가 보기에, 이 법이 명실상부한 개인정보보호법으로서 기능함에 있어 오히려 제약요인으로 작용할 수 있다.

이 법은 공공기관에 의한 개인정보의 수집·이용·제공으로부터 정보주체의 자기결정권을 보호하기 위하여 정보처리의 기본원칙들을 구체화한 것으로서, 그 수집·이용·제공의 과정에 일정한 절차적 및 실체적 제한을 가하고 있는 법률이다. 그리고 그 제한은 개인정보자기결정권을 보장하기 위한 기본적인 헌법적 요청이고, 뒤에서 살피는 바와 같이 현재 제도화된 제한의 정도는 아직 충분하지 못한 상태로서 최저한의 제한이라고 할 수 있다. 그리고 이 법은 종래 공공기관에 의한 개인정보처리의 근거가 되던 다른 법률에서는 규율하지 않던 새로운 제한과 절차를 설정하는 것이기 때문에 종래의 처리관행을 이 법의 규율에 따라 개선해야 할 필요가 있다. 그렇다면, 이 법은 오히려 "다른 법률의 규정에 불구하고 공공기관에 의한 개인정보의 수집·이용·제공에 관하여는 이 법이 정하는 바에 의한다."고 규정하였어야 했던 것이 아닌가 생각된다.

더 나아가, 법 제3조 제2항은 "통계법에 의하여 수집되는 개인정보와 국가안전보장과 관련된 정보분석을 목적으로 수집 또는 제공요청되는 개인정보의 보호에 관하여는 이 법을 적용하지 아니한다."고 규정하고 있다. 이러한 적용제외는 이 법의 치명적인 결함이다. 통계법 적용제외의 문제점은 아래에서 언급한다. 그리고 국가안보와 관련한 개인정보처리에 관해 전면적으로 이 법의 적용을 배제한 것은 심각한 문제이다. 법상 요구되는 절차적 및 실체적 제한 중 합리적인 범위 내에서 그 일부분의 적용을 배제하는 것은 타당성이 있을 수 있지만, 국가안보와 관련한 개인정보처리의 존재 자체가 정보주체의 인식으로부터 그리고 사회적 감시로부터 완전히 벗어날 수 있도록 하는 것은 민주적 참여의 가치를 담고 있는 개인정보자기결정권의 헌법정신과 양립하지 않는다고 하겠다.

다. 수집제한 원칙의 부분적 구체화

개인정보자기결정권의 보장의 출발점은 수집 단계에서부터 시작되어야 하고,[49] 그렇기 때문에 그 파생원칙의 하나로서 수집제한의 원칙이 요구된다. 동 원칙은 (i) 정당한 수집목적을 위하여(수집목적의 정당성) (ii) 필요한 범위 내에서(수집범위의 필요최소성) (iii) 공정하고 합리적인 방식으로(수집방식의 합리성) (iv) 정보주체의 분명한 인식 또는

49) 최영규, 앞의 글(각주 37), 49면.

동의 하에(정보주체의 인식명확성) 수집되어야 한다는 것을 의미한다.

그런데 공공기관개인정보법은 이러한 수집제한의 원칙을 부분적으로만 구체화하고 있다. 위에서 언급한 바와 같이, 동법은 공공기관이 다양한 방식으로 수집·처리하고 있는 모든 형태의 개인정보를 규율대상으로 하는 것이 아니고, 개인정보처리시스템 즉 개인정보화일에 기록된 처리정보만을 그 보호대상으로 한다. 그리하여 동법은 개인정보의 개별적인 수집에 대해 수집제한의 원칙을 밝히고 있는 것이 아니라, 공공기관이 개인정보화일을 보유하고자 하는 경우 그 범위 및 내부절차에 관해서만 한정적으로 규율하고 있다. 즉 법 제5조는 "공공기관은 소관업무를 수행하기 위하여 필요한 범위안에서 개인정보화일을 보유할 수 있다."고 규정하고 있고, 제6조는 개인정보화일을 보유하기 전에 보유목적 등 일정한 사항[50]을 행정자치부장관에게 사전통보하도록 요구하고 있을 뿐이다. 다만, 법 제4조는 "사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보"를 동의에 의하지 않고 수집하는 것을 금지하고 있다.

따라서 위 제4조 소정의 수집금지대상이 아니고 또 개인정보화일에 기록되지 않는 개인정보에 대한 수집은 아무런 제한 없이 행해질 수 있다.[51] 이것은 이 법의 중요한 흠결부분이다.

한편, 개인정보화일을 보유하고 그에 따라 개인정보를 수집하고자 하는 경우에, "소관업무 수행에 필요한 범위" 안에서의 보유 및 수집이라는 실체적 요건을 규정하고 있는 것은 수집제한의 원칙 중 수집범위의 필요최소성 요건을 채택한 것으로서 긍정적으로 평가해야 할 것이다. 따라서 개인정보화일의 보유 자체 및 수집되는 특정한 개인정보가 합법적인지의 여부는 "업무수행의 필요성" 요건의 판단에 좌우될 것이다.

그러나 이러한 수집과 관련해서 이 법의 취약점은 수집제한의 원칙의 또 다른 요건인 수집방식의 합리성 요건과 정보주체의 인식명확성 요건을 규정하고 있지 않다는 점이다. 우선 수집방식의 합리성 요건과 관련해서, 수집되는 개인정보에 기초해서 당해 정보주체에게 불이익한 행정결정이 내려질 수 있는 경우에는 가능한 한 당해 정보주체로부터 직접 수집되어져야 한다.[52] 또한 정보주체의 인식명확성 요건과 관련해서, 개별적인 정보수집시에, 설령 정보주체의 동의는 반드시 요구되지 않는다 하더라도, 적어도

---

50) "1. 개인정보화일의 명칭 2. 개인정보화일의 보유목적 3. 보유기관의 명칭 4. 개인정보화일에 기록되는 개인 및 항목의 범위 5. 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭 6. 개인정보화일의 열람예정시기 7. 열람이 제한되는 처리정보의 범위 및 그 사유 8. 기타 대통령령이 정하는 사항"(법 제6조 제1항).

51) 同旨 : 김연태, 앞의 글(각주 19), 206면.

52) 미국 연방프라이버시법(Privacy Act) 5 U.S.C. §552a(e)(2) 참조.

수집의 법적 근거, 정보제공이 강제적인 것인지 임의적인 것인지의 여부, 수집목적, 이용형태, 요청된 정보를 제공하지 않는 경우 당해 정보주체에 미칠 효과 등을 합리적인 방법으로 고지하여야 할 것이다.[53] 현행 공공기관개인정보법이 이렇게 개별적인 고지가 아니고 개인정보화일의 보유와 관련한 일반적 사항들을 행정자치부장관에게 통보하도록 하고(법 제6조 제1항), 이 사항들을 연 1회 이상 관보에 게재하여 공고하도록 규정하고 있는 것(법 제7조)만으로는 헌법적 요청인 정보주체의 인식명확성 요건을 충족시킬 수 없다고 할 것이다.

라. 목적구속 원칙의 형해화 가능성

(1) 목적구속 원칙의 선언과 예외사유의 광범위한 인정

개인정보자기결정권에 포함된 목적구속의 원칙이란 '개인정보를 수집하는 목적은 (i) 수집 당시에 명확히 특정되어 있어야 하고(목적의 특정성), (ii) 그 후의 이용은 이 특정된 수집목적과 일치되어야 한다(목적일치성)'는 요청이다. 이 원칙은 개인정보 수집기관 내부의 이용을 제한함과 동시에 특히 수집기관 이외의 제3자 제공을 통제하기 위한 것이다. 물론 이 원칙이 절대적일 수는 없고, 법률이 명시적으로 허용하는 예외가 있을 수 있다. 다만, 제3자 제공의 경우에도 위 수집제한의 원칙이 적용되기 때문에 제공목적의 정당성, 제공범위의 필요최소성, 제공방식의 합리성, 정보주체의 인식명확성이 요구된다.

공공기관개인정보법 제10조는 사전에 공시된 개인정보화일의 보유목적이 아닌 다른 목적으로 처리정보를 이용하거나 제공하는 것을 금지하는 이른바 목적구속의 원칙을 규정하고 있다.

그러나 여기에는 매우 광범위한 예외가 인정되고 있다. 첫째, 다른 법률이 보유목적 이외의 목적으로 보유기관의 내부에서 이용하는 것을 허용하거나 또는 제3자 제공을 허용하는 경우에는 그에 따른다(제10조 제1항 전단). 따라서 공공기관개인정보법이 선언하는 목적구속의 원칙은 다른 법률에 의하여 얼마든지 훼손될 수 있다. 즉 위 법상의 목적구속의 원칙은 다른 법률에서 보유목적 외의 이용 및 제공을 규정하고 있지 않는 한도 내에서만 적용되는 원칙일 뿐이다. 이러한 규범적 태도는 공공기관개인정보법이 기본법으로서의 성격을 가지는 것이 아니라 단순한 일반법으로서의 성격을 가질 뿐이

53) 미국 연방프라이버시법(Privacy Act) 5 U.S.C. §552a(e)(3) 참조. 우리의 민간부문 일반법이라고도 할 수 있는 「정보통신망이용촉진및정보보호등에관한법률」 제22조 제2항도 수집시에 정보주체에게 일정한 사항을 고지하도록 의무지우고 있다.

라는 것을 의미한다. 다시 말해서, 다른 법률의 규정에도 불구하고 동법상의 목적구속의 원칙이 적용되는 것이 아니라, 언제든지 다른 법률의 규정에 의하여 목적구속의 원칙이 배제될 수 있는 것이다. 이러한 규범적 성격은 이미 동법 제3조 제1항에서 선언되고 있다.

둘째, 이 법 자체에서도 8가지 광범위한 예외[54]를 인정하고 있다. 이러한 예외의 경우에는 사전에 공시된 보유목적에 구속되지 않고 얼마든지 다른 용도로 수집기관 내부에서 활용할 수 있으며, 또 정보주체의 동의를 받거나 통지함이 없이 임의로 제3자에게 제공할 수 있다(법 제10조 제2항 본문). 이에 따라 각 공공기관이 자신이 보유하는 개인정보화일과 다른 기관이 보유하는 개인정보화일을 상호 연결시키는 것(computer matching)이 법적으로 허용되어 있는 셈이다. 심지어, 2001년 7월 1일부터 시행된 전자정부법 제21조 제1항은 이들 예외의 경우에 보유하고 있는 처리정보를 공동이용하도록 각 행정기관에 의무지우고 있는 실정이다.

여기서 특히 제2호, 6호, 7호, 8호의 예외사유가 문제된다. 이처럼 광범위한 예외는 목적구속의 원칙을 무의미하게 만들 가능성을 지니고 있기 때문이다. 그 중에서도 특히 제2호의 사유는 행정기관 상호간에 거의 무제한적으로 개인정보를 공동이용할 수 있도록 하는 포괄적인 조항이다. 각 행정기관의 활동 중 "법률에서 정하는 소관업무의 수행"이 아닌 것이 없기 때문이다. 더 나아가, 제8호는 소관업무의 수행과 관련이 없는 보유목적 이외의 이용과 제3자 제공(예컨대, 상거래의 활성화를 위한 이용 및 민간기업에의 제공 등)을 포괄적이고 무제한적으로 대통령령에 위임하고 있다. 현행 시행령은 이러한 특별사유를 별도로 정하고 있지 않지만, 언제든지 대통령령에 의해 목적구속의 원칙이 파기될 수 있는 규범상태라고 하겠다.

다행히, 법은 이 같은 보유목적 이외의 이용 및 제3자 제공에 대해 몇 가지 실체적 및 절차적 제한을 두고 있다.

---

54) "1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우
2. 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우
3. 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우
4. 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우
6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우
7. 법원의 재판업무수행을 위하여 필요한 경우
8. 기타 대통령령이 정하는 특별한 사유가 있는 경우" (법 제10조 제2항 본문 각호)

(2) 제3자 제공에 대한 실체적 제한

우선, 이들 예외사유 전부에 적용되는 실체적 제한으로서, “정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는” 보유목적 이외의 이용 및 제3자 제공이 허용되지 않는다(법 제10조 제2항 단서). 그러나 “부당한 침해의 우려” 여부는 당해 보유기관의 장에게 판단여지가 있다고 보아야 하기 때문에 법원에 의한 엄밀한 사법적 평가를 기대하기 어려울 것으로 보이고, 그 만큼 이 제한요건은 개인정보의 남용을 통제하는 효과적인 장치로 보기 어렵다. 더구나 전자정부법이 공동이용을 강제하고 있는 규범상태에서는 더욱 그러하다.

다음으로, 각호의 예외사유에 고유한 실체적 제한으로서, 제2호의 경우 소관업무 수행을 위한 “상당한 이유”가 존재하여야 한다. “상당한 이유”의 존재 여부는 전적으로 법원이 판단할 사항이고, 따라서 이 사유에 의한 제3자 제공의 합법성 기준은 향후의 법원의 정책에 맡겨져 있는 문제이다. 그렇지만, 법원은 제2호가 목적구속의 원칙을 무의미하게 만들 수 있는 포괄적인 예외조항이라는 점을 고려하여 “상당성” 판단을 엄격하게 하여야 할 것이다. 예컨대, 수령기관에서의 용도가 원래의 보유목적과 상호관련성이 있어야 하고, 또 당해 개인정보의 이용이 수령기관의 소관업무에 필수불가결한 것이어야 하는 등의 요건이 충족되는 경우에 한하여 그 상당성을 인정하여야 할 것이다.

한편, 제6호의 경우 그 실체적 제한으로서, 범죄수사 및 공소유지를 위한 “필요성”이 인정되어야 한다. 이 필요성 판단에 있어서도 법원은 엄격해석을 해야 할 것이다. 그리고 제7호의 경우 법원의 재판업무수행의 “필요성”은 법원의 제출명령이 있는 경우로 한정되어야 할 것이다. 물론 여기의 법원에는 헌법재판소도 포함된다고 해석된다.

한편, 법은 이렇게 보유목적을 넘어서서 제3자 제공을 하는 경우, 보유기관의 장은 수령기관에게 그 “사용목적·사용방법 기타 필요사항에 대하여 제한을 하거나 제공정보의 안전성을 위해 필요한 조치를 강구하도록 요청하여야 한다.”고 규정하고 있고(법 제10조 제3항), 특히 정보제공이 “통신망을 이용하여” 이루어지는 것일 때 만약 수령기관이 위 제한이나 요청사항을 이행하지 않는 경우에는, 보유기관의 장은 “즉시 처리정보의 제공을 중지”하도록 하고 있다(시행령 제12조 제2항). 그 밖에 정보수령기관은 “제공기관의 동의 없이 당해 처리정보를 다른 기관에 제공하여서는 아니 된다.”(법 제10조 제5항).

(3) 제3자 제공에 대한 절차적 제한

법은 위 보유목적을 넘어선 제3자 제공에 대한 절차를 달리 규정하고 있지 않다. 다

만, 법시행령은 보유기관이 임의로 제공할 수는 없고, 수령기관이 그 이용목적 및 이용하고자 하는 처리정보의 범위를 명시하여 보유기관의 장에게 문서로 요청하도록 하고 있다. 그리고 이에 따라 제공하는 경우 보유기관의 장은 관련사항[55]을 처리정보제공대장에 기록하고 이를 관리하여야 한다(시행령 제11조). 특히 보유기관의 장은 "통신망을 이용하여" 정보제공을 하는 경우에는 제공정보의 항목을 한정하고, 수령기관이 그 범위를 넘어서 이용할 수 없도록 필요한 조치를 취해야 하며, 위 처리정보제공대장에 기록되는 사항을 행정자치부장관 또는 관계중앙행정기관의 장에게 통보하여야 한다(시행령 제12조 제1항).

(4) 제3자 제공절차에 있어서의 기본결함

그러나 이러한 절차적 제한만으로는 개인정보자기결정권의 헌법정신과 양립할 수 없다. 개인정보자기결정권에 포함된 정보주체의 인식명확성의 요건은 자신에 관한 정보가 어떤 법적 근거 하에서 어떤 목적을 위하여 어떤 기관에 의해 어떻게 이용될 것인지를 당해 정보주체가 명확하게 인식할 수 있을 것을 요구한다. 그러나 현행의 법은 정보주체 이외의 제3자에게 개인정보를 제공하는 경우 달리 정보주체의 동의를 받거나 그에게 통지하도록 요구하지 않고 있다.

더 나아가, 시행령이 규정하는 처리정보제공대장은 법상의 개인정보화일의 개념에 포함되지 않기 때문에, 개인정보화일에 적용되는 법 제7조에 의한 관보게재, 제8조에 의한 일반인의 열람, 그리고 제12조에 의해 정보주체에게 인정되는 열람청구권의 대상이 되지도 않는다. 다만, 처음에 개인정보화일을 보유하고자 할 때, 당해 보유기관의 장은 "처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭, 제공항목 및 법령상 근거(법령상 근거가 있는 경우에 한한다)"를 행정자치부장관 또는 관계중앙행정기관의 장에게 사전통보하고(법 제6조 제1항 제5호 및 시행령 제5조 제4호), 그 통보사항이 연 1회 이상 관보에 게재되며(법 제7조), 이 사항이 기재된 개인정보화일대장이 일반인에게 열람되도록 하고 있을 뿐이다(법 제8조).

요컨대, 현행법은 정보주체의 인식이 없는 상태에서 컴퓨터결합(computer matching)을 통한 보유정보의 공동이용을 거의 무제한적으로 허용하면서 정보주체에 대한 행정결정을 가능하게 하고 있는 바, 이는 목적구속의 원칙 및 수집제한의 원칙을 크게 약화

55) ① 개인정보화일의 명칭 ② 제공받는 기관의 명칭 ③ 이용목적 ④ 법령상 제공근거가 있는 경우에는 그 근거 ⑤ 제공하는 처리정보의 항목 ⑥ 제공의 주기 ⑦ 제공의 형태 ⑧ 이용기간이 정하여져 있는 경우에는 그 기간 ⑨ 법 제10조 제3항의 규정에 의하여 수령자에 대하여 사용목적등에 제한을 가하거나 필요한 조치를 취할 것을 요청한 경우에는 그 내용

시키는 규범상태라고 하지 않을 수 없다. 컴퓨터결합에 대한 보다 엄격한 실체적 및 절차적 요건을 설정하고, 동시에 효과적인 감독장치를 마련하여야 할 것이다.

마. 시스템공개 원칙의 위반

개인정보자기결정권의 파생원칙인 시스템공개의 원칙은 '개인정보처리시스템의 설치여부, 설치목적, 정보처리방식, 처리정보의 항목, 시스템운영책임자, 처리시스템에 의한 자동결정이 이루어지는지 여부 등이 일반에게 투명하게 공개되어야 한다'는 요청이다. 그러나 공공기관개인정보법은 이러한 시스템공개에 대해 애매하고 포괄적인 예외를 지나치게 넓게 인정하고 있는 것으로 판단된다.

이 법에 의하면, 개인정보화일을 보유하고자 하는 각 공공기관은 그 처리내역[56]을 관계중앙행정기관의 장에게 통보하고, 관계중앙행정기관은 이를 종합하여 행정자치부장관에게 제출하도록 하고(제6조 제1항), 관계중앙행정기관과 행정자치부장관은 이들 처리내역을 연 1회 이상 관보에 게재하여 공고하도록 규정하고 있다(법 제7조 본문). 또한 각 보유기관의 장은 그 처리내역을 개인정보파일별로 기재한 대장(개인정보화일대장)을 작성하여 일반인이 열람할 수 있도록 하여야 한다(법 제8조 본문).

그러나 이러한 시스템공개에 대한 예외가 지나치게 넓다. 즉 일정한 유형의 개인정보화일[57]은 관계중앙행정기관에의 통보 및 행정자치부장관에의 제출이 요구되지 않고(제6조 제2항), 따라서 관보게재에 의한 공고대상에서 처음부터 제외되며(제7조 본문), 일반인의 열람대상에서도 제외된다(제8조 본문).

이 같은 광범위한 예외는 시스템공개의 원칙과 부합할 수 없다. 위 법률조항의 통보, 공고 및 열람의 대상이 되는 정보는 구체적인 개인정보가 아니라 처리내역정보이다. 이

---

56) ① 개인정보화일의 명칭 ② 개인정보화일의 보유목적 ③ 보유기관의 명칭 ④ 개인정보화일에 기록되는 개인 및 항목의 범위 ⑤ 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭 ⑥ 개인정보화일의 열람예정시기 ⑦ 열람이 제한되는 처리정보의 범위 및 그 사유 ⑧ 기타 대통령령이 정하는 사항 (법 제6조 제1항)

57) "1. 국가의 안전 및 외교상의 비밀 기타 국가의 중대한 이익에 관한 사항을 기록한 개인정보화일
2. 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보화일
3. 조세범처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한 사항을 기록한 개인정보화일
4. 컴퓨터의 시험운영을 위하여 사용되는 개인정보화일
5. 1년 이내에 삭제되는 처리정보를 기록한 개인정보화일
6. 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보화일
7. 대통령령이 정하는 일정한 수 이내의 정보주체를 대상으로 하는 개인정보화일
8. 기타 이에 준하는 개인정보화일로서 대통령령이 정하는 개인정보화일" (법 제6조 제2항)

러한 처리내역정보가 공개된다고 해서 개인의 사적 정보가 공개되는 것이 아니다. 오히려 처리내역정보의 공개는 국가기관에 의한 은밀한 개인정보처리를 막음으로써 개인의 인격과 존엄을 보장하고 민주적 정부운영을 위한 기본적인 전제조건이다. 따라서 중대한 공익에 의해 불가피한 사정이 존재하지 않는 한, 모든 개인정보처리시스템의 운용 및 활용상황이 일반에게 공개되어야 한다. 위 법률조항의 예외는 정당화되기 어려운 사유라고 하겠다.

더 나아가, 법 제7조 단서는 제6조의 통보대상이 되는 처리내역정보라 하더라도 "공공기관의 적정한 업무수행을 현저하게 저해할 우려가 있다고 인정되는 때에는 대통령령이 정하는 바에 따라 당해 개인정보화일에 기록되어 있는 항목의 전부 또는 일부를 공고하지 아니할 수 있다."고 하여 이중의 예외를 설정하고 있고, 이 공고 제외 사항은 개인정보화일대장에도 기재하지 않을 수 있도록 하고 있다(법 제8조 단서). 또한 법 제12조에 의하면, 정보주체는 "개인정보화일대장에 기재된 범위안에서"만 본인에 관한 처리정보의 열람을 청구할 수 있도록 되어 있다.

이 같은 규정들은, 공공기관에 의한 개인정보의 처리에 대해 당해 정보주체 및 사회 일반에게 감시의 기회를 제공함으로써 개인정보자기결정권을 구체화하고자 하는 이 법의 입법취지를 무색하게 만드는 것으로서, 시민이 전혀 알지 못하는 상태에서 국가가 개인정보를 마음껏 처리할 수 있는 길을 열어 주고 있다. 요컨대, 이들 규정은 시스템 공개의 원칙을 위반하여 개인정보자기결정권을 위헌적으로 침해하고 있는 것이 아닌가 생각된다.

바. 개인정보분리 원칙의 무시

개인정보분리의 원칙은 특정 목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 통합되지 않고 분리된 상태로 유지되어야 한다는 요청이다.

그런데 공공기관개인정보법은 그 입법목적이 "컴퓨터에 의하여 처리되는 개인정보의 보호"에 있음에도 불구하고, 디지털화된 개인정보의 특성을 충분히 고려하지 못한 채 개인정보화일을 마치 종이 문서인 양 취급하고 있는 것이 아닌가 생각된다.[58] 컴퓨터 데이터베이스는 그 전부 또는 일부가 다른 데이터베이스의 일부 또는 전부와 매우 용이하게 결합되어 새로운 데이터베이스를 형성할 수 있다. 특히 우리나라의 경우 표준개인식별자인 주민등록번호를 중심으로 하여 모든 개인정보화일을 구축하고 있기 때문에,

58) 김주환, "디지털 時代의 個人情報保護와 私民權", 『인터넷법률』 제4호, 법무부, 2001년 1월, 54면 참조.

개인정보화일간의 정보통합은 매우 용이하다. 이는 포괄적인 개인정보통합관리시스템의 구축을 용이하게 하고, 그 결과 국가는 개인의 총체적인 인격상을 손쉽게 파악할 수 있는 위험성을 드러낸다. 이것은 개인정보자기결정권의 헌법정신과 양립하기 어렵다. 개인정보자기결정권은 타인의 수중에서 총체적인 인격상이 형성되는 것 자체를 거부하는 개인의 기본권이기 때문이다.

그럼에도 공공기관개인정보법에는 컴퓨터결합 등에 의한 정보통합을 효과적으로 규율하는 장치가 대단히 미흡하고, 심지어 전자정부법은 컴퓨터결합을 통한 공동이용을 오히려 의무화하고 있다.[59] 위에서 본 바와 같이, 보유목적 외의 이용 및 제공이 정보주체의 동의나 인식 없이 폭넓게 허용되고 있는 반면에, 이러한 이용 및 제공의 결과 컴퓨터결합 등에 의한 새로운 개인정보화일의 생성을 명시적으로 금지하는 규정을 두고 있지 않다.

다만, 법 제10조 제3항은 보유목적 외 제3자 제공의 경우 보유기관의 장이 그 수령기관에 대하여 "사용목적·사용방법 기타 필요한 사항에 대하여 제한을 하거나 처리정보의 안전성확보를 위하여 필요한 조치를 강구하도록 요청하여야 한다."고 규정하고 있고, 시행령은 그 정보제공이 "통신망을 이용하여" 이루어지는 것일 때 만약 수령기관이 위 제한이나 요청사항을 이행하지 않는 경우에는, 보유기관의 장은 "즉시 처리정보의 제공을 중지"하도록 하고 있을 뿐이다(시행령 제12조 제2항). 그러나 이들 규정만으로는 개인정보의 통합에 따르는 위험성을 차단하기에는 역부족이다.

참고로, 지난 2002년 9월 19일자 미국의 연방관보(Federal Register)에 고시된 교육부(Department of Education)와 연방이민국(Immigration and Naturalization Service) 사이에 운용되는 컴퓨터결합프로그램에 관한 내용을 소개한다.[60] 우리의 규범상태와 크게 비교된다.

---

59) 행정자치부가 2001년 7월 발간한『전자정부법의 이해와 해설』, 56면은 현재 Data 가공여부에 따른 행정정보공동이용의 방식에 네 가지가 있는 것으로 설명하고 있다.
- (ⅰ) Data Integration 방식 : 관련 DB의 요약본을 수집하여 하나의 DB로 통합 구축하고, 개별 수요자에게 제공하는 방식. 사실상 이중적 DB가 구축된다는 문제점 있음.
- (ⅱ) Data Pool 방식 : 관련 DB의 요약 DB를 수집하여 pool로 관리하고, 통합활용시스템에 요약 DB를 제공하는 방식. 주민, 부동산, 호적 등 DB의 요약 DB 등 시군구 공통 21개 업무 DB의 pool을 구축하고 이를 시군구 행정종합정보화시스템에 제공하여 일선 민원처리시 활용하고 있음.
- (ⅲ) Data Profiling 방식 : 일관된 정보를 집적하는 DB complex에 변동되는 DB 구성요소를 전송, 업데이트하는 Super DB를 제공하는 방식. 자동차등록기록 등 자동차 관련 사항을 발생시점별로 입력하여 일관된 관리를 도모함.
- (ⅳ) Data matching 방식 : DB를 보유기관에 그대로 두고, 대조할 DB를 대조될 DB와 대조하여 목적을 달성하는 시스템 방식. 여권전산망에서 여권신청자의 신청항목을 주민 DB에 보내어 그 항목의 진위여부를 yes/no로 회신 받는데 활용하고 있음.

60) Notice of Computer Matching Program, 67 Fed. Reg. 59056, 59056 (Sept. 19, 2002)

두 기관 사이에 운용되는 컴퓨터결합프로그램은 "연방이민국과 교육부간의 자격확인용 외국인조회시스템"(Systematic Alien Verification for Entitlement INS/ED)이라는 타이틀을 가진다. 이 프로그램은 교육부가 연방학생보조금을 받고 있거나 또는 신청을 한 외국인학생의 입국자격(immigration status)을 조회할 수 있도록 허용할 것이다.

입국자격정보는 1986년의 입국개혁및통제법(Immigration Reform and Control Act of 1986)에 근거하여 연방이민국이 외국인자격조회색인(Alien Status Verification Index)이라는 개인정보DB를 통해 보유하고 있다. 한편, 교육부는 1965년의 고등교육법(Higher Education Act of 1965)에 근거하여 위 외국인자격조회색인에 접근할 수 있는 권한을 부여받고 있고, 또 연방이민국은 입국및국적법(Immigration and Nationality Act) 제103조의 일반적 권한에 따라 입국자격을 다른 기관에게 확인해 줄 수 있다. 연방학생보조금을 받고 있거나 신청을 한 외국인학생이 그러한 자격이 있는지를 검증하기 위한 목적에서 교육부가 연방이민국의 외국인자격조회색인 데이터베이스에 접속하는 것을 허용하는 두 기관 사이의 컴퓨터결합협정(matching agreement)이 최초로 승인된 것은 1990년이었다.[61]

위 컴퓨터결합프로그램의 운용을 통해, 교육부는 자신이 보유하는 "연방학생보조금신청화일"(Federal Student Aid Application File)에 담겨 있는 외국인학생의 데이터(외국인등록번호와 생년월일을 포함해서)를 연방이민국에 전송할 것이다. 이 데이터를 이용해서, 외국인자격조회색인 데이터베이스에서 검색이 이루어질 것이고, 서로 일치하는 개인기록들이 있으면, 그 데이터베이스는 교육부에게 당해 외국인학생의 입국자격정보를 제공하게 될 것이다.

그러나 교육부는 무자격자를 발견했더라도 곧 바로 보조금지급과 관련한 불이익결정을 내릴 수 없다. 즉, (i) 교육부가 무자격이라는 정보의 정확성을 독자적으로 확인하거나, 아니면 (ii) 교육부 소속의 자료보전위원회(Data Integrity Board)가 그 정보가 정확하다는 점 및 당해 외국인학생이 교육부로부터 그 요지와 그에 대해 다툴 수 있는 기회가 있음을 통지받았다는 점을 상당한 확신을 가지고 판단을 내리기 전에는 달리 불이익결정을 할 수 없다. 또한 교육부는 당해 외국인학생이 위 컴퓨터결합프로그램에 의한 무자격 인정사실을 통지받은 후 최소 30일 이내에는 그 불이익결정을 집행할 수 없다.

위 컴퓨터결합프로그램은 양 기관의 자료보전위원회가 승인한 컴퓨터결합협정(matching agreement)의 사본이 연방의회에 제출되어 관리예산국(Office of Management and Budget)의 승인을 받은 후 40일이 지나 발효한다.

---

61) 55 Fed. Reg. 5904 (1990).

사. 소결

요컨대, 우리의 현행 전자정부 모델에서는 개인정보자기결정권의 기본권적 이익이 효율성의 가치에 밀려 상당부분 무시되고 있으며, 공공부문의 개인정보보호법제는 아직 참여로서의 사생활보호 모델을 완전하게 구현하지 못하고 있는 것으로 평가된다.

3. 주민등록법상 주민등록번호 강제부여의 위험성

1996년 정부가 국가통합전자신분증 내지 전국민신원확인카드(National Identification Card)의 개념으로 추진하려고 했던 전자주민카드사업은 시민사회단체와 학계 등 여론의 강력한 반대에 부딪혀 일단 유보되었다.[62] 사실 전국민신원확인카드의 개념에는 전국민을 추적할 수 있는 통합된 데이터베이스(centralized database)의 구축이 전제되어 있다.

비록 현재는 정부가 이 같은 전자주민카드사업을 유보한 상태지만, 표준개인식별번호(universal identification number)와 전국민신원확인카드 및 이에 기초한 개인정보통합관리시스템을 구축하고자 하는 시도는 그 무시할 수 없는 효용성 때문에 어느 정부도 쉽게 포기할 수 없는 유혹이다. 최근 미국과 유럽에서는 불법이민의 고용통제, 범죄방지 등의 효율적인 법집행, 복지사기의 방지, 조세포탈자의 추적, 국민보건의 증진 등의 강력한 논거에 입각하여 개인정보통합관리시스템의 구축을 주장하는 목소리가 점차 높아지고 있다. 이에 더하여 시장의 압력도 가중되고 있다. 전자상거래의 성공 여부는 전자거래를 하고자 하는 자의 신원을 확인할 수 메커니즘의 존재에 달려 있기 때문이다.[63]

---

62) 정부가 애초 계획했던 전자주민카드는 중앙처리장치(CPU)를 내장한 스마트카드에 주민등록등·초본 수록정보, 운전면허증 수록정보, 의료보험증 수록정보, 국민연금증 수록정보 등 7개 분야 42개 정보를 수록하도록 되어 있었다. 그러나 여론의 반대에 부딪히자 정부는 1997년 11월 주민등록자료와 인감만을 스마트카드에 수록하는 주민등록법개정안을 정기국회에 제출하였고, 개정안은 야당의 반대 속에 통과되었다(1997. 12. 17. 법률 제5459호). 이 동안의 경과에 대해서는, 김기중, "전자주민카드 반대운동의 성과와 정보지배사회에서 시민사회의 역할",『인권보고서』제12집 (대한변호사협회, 1998), 420-422면 참조. 그러나 이 제한된 형태로 제도화된 전자주민카드는 사실상 시행되지 못한 상태에서, 결국 1999년의 개정법률에 의하여 전자주민카드사업은 유보되고, 다만 그 동안 투자된 설비를 활용하여 종이와 비닐재질로 된 주민등록증을 플라스틱재질의 주민등록증으로 일제히 경신하였다(1999. 5. 24. 법률 제5987호).

63) 이러한 신원확인도구로서 현재 개발된 대표적인 것이 여러 형태의 전자서명(digital signature)이다. 이 전자서명방식은 전자상거래를 가능하게 하지만, 동시에 심각한 개인정보자기결정권의 침해문제를 야기한다. 전자서명에 개인정보 보호장치가 내장되지 않는다면, 전자서명은 완벽한 전자추적기능을 수행할 것이기 때문이다. 현재까지의 전자서명 자체에는 개인정보 보호장치가 없는 것으로 알려지고 있다. Graham Greenleaf & Roger Clarke, "Privacy Implications of Digital Signatures (Mar. 10, 1997)

북유럽과는 달리 표준개인식별번호를 부여하지 않는 미국에서도 이미 1960년대 중반에 전국민을 대상으로 하는 통합데이터뱅크(comprehensive national databank)의 구축이 주장된 적이 있었다. 그러나 연방의회에서의 격렬한 논쟁 속에서 그 주장은 크게 후퇴하였고, 그 결과 연방의 각 정부기관이 분리된 개인정보처리시스템을 구축하는 것으로 일단락되었다.[64] 그러나 이후의 정보기술의 발전은 물리적 정보분리를 무의미하게 만들고 있다. 즉 표준개인식별자(universal identifier)를 이용한 무제한적인 컴퓨터결합(computer matching)은 사실상의 전국민통합데이터뱅크를 가능하게 하는 것이다.

우리들은 거래연관에 따라 여러 개인식별자(personal identifier)를 가지고 있다. 예금계좌번호, 신용카드번호, 운전면허번호, 의료보험번호, 여권번호 등이 그것이다. 이들은 원래는 각자 다른 목적을 위해 분리되어 사용되는 것으로 예정되었다. 그리고 이들이 분리되어 존재한다는 사실 자체가 개인정보통합관리시스템의 형성에 있어 자동적인 방화벽이 될 수 있는 것이다.

그러나 전 국민이 표준개인식별자로서의 주민등록번호를 강제로 부여받고 있고, 또한 정부와의 거래 또는 민간에서의 거의 모든 거래에 있어 주민등록번호의 제출을 요구하고 있는 우리의 상황[65]은 개인정보통합관리시스템의 형성을 막을 수 있는 자동적인 방화벽이 이미 존재하지 않는다는 것을 의미한다.

주민등록법 제7조는 개인별 및 세대별 주민등록표를 작성하도록 하고(제1항), 개인별 주민등록표는 "개인에 관한 기록을 종합적으로 기록·관리"하며 세대별 주민등록표는 "그 세대에 관한 기록을 통합하여 기록·관리"하도록 하고 있다(제2항). 그리고 같은 조 제3항은 주민에 대하여 개인별로 고유한 등록번호(주민등록번호)를 부여하도록 하고 있다.[66] 나아가 제9조는 개인별 주민등록표를 주민등록번호순으로 정리하도록 하고 있

<http://www.anu.edu.au/people /Roger.Clarke/DV/DigSig.html>

64) John Shattuck, "In the Shadow of *1984:* National Identification Systems, Computer-Matching, and Privacy in the United States", *35 Hastings L.J. 991, 996 (1984).* 최근에 미국 재무부 산하 비밀보호국(Secret Service)은 운전면허증상의 사진과 이름을 연결시키는 사기방지용 전국민데이터뱅크(comprehensive national anti-fraud database)를 구축하려고 시도하였으나, 여론의 반대에 부딪혀 갑작스레 취소하였는데, 취소하기 전에 이미 비밀보호국은 많은 주로부터 2200만명 이상의 미국민의 사진과 이름을 구입한 상태였다고 한다. "The Surveillance Society", The Economist(U.S. Edition), May 1, 1999, at 22.

65) 「주민등록법 개정을 위한 행동연대」가 2001년 4월에 조사한 바에 따르면, 회원가입제 인터넷 웹사이트의 경우 무작위로 선정된 총 547개 사이트 중 주민등록번호를 요구하는 곳은 500개 사이트(91.41%)였고, 주민등록번호를 기재하지 않는 사이트는 31개 사이트(5.67%)였으며 주민등록번호의 기재가 선택사항인 곳은 모두 16개 사이트(2.92%)였다고 한다. 윤현식, "주민등록관련 피해사례 실태 및 주민등록번호문제의 환기", <http://www.privacy.or.kr/>에서 인용.

66) 이 조항은 2001. 1. 26. 공포된 법률 제6385호에 의하여 신설되었다.

다. 또한 이렇게 정리된 주민등록표의 기재사항은 전산정보처리조직에 의하여 처리하도록 하고, 이 전산화된 주민등록표화일은 주민등록표와 같은 것으로 간주된다(제7조의2 제1항).

개인별 주민등록표에 수록되는 개인정보는 법 제10조에서 명시적으로 신고사항으로 정하고 있는 성명, 성별, 생년월일, 세대주와의 관계, 본적, 주소, 주소이동사항 외에도 시행령이 정하는 항목으로서 세대번호, 혈액형, 혼인여부, 본적변경사유, 호주와의 관계, 인력동원사항(동원대상여부, 기술·기능·예능사항, 동원훈련사항, 자격면허, 직업훈련사항 등), 학력, 직업 등으로 이루어져 있다(시행령 제6조 별지 제1호 서식).[67] 물론 이들 개인정보는 강제부여되는 주민등록번호를 표준개인식별자로 하여 전산 처리된다. 이들 정보 중 특히 "혈액형, 혼인여부, 학력, 직업"은 비록 그 자체 개인의 비밀에 속하는 정보는 아니라 하더라도, 주민등록표라고 하는 국가운영의 전산화된 개인기록관리시스템에 통합관리된다는 측면에서 볼 때 이들 정보에 대해서는 정보주체의 사생활보호의 이익이 존재한다고 보아야 할 것이고, 따라서 이들 정보를 수집해서 통합관리하고자 하는 경우에는 기본권 제한에 있어 요구되는 법률유보의 원칙에 따라 법률에 그 명시적 근거가 있어야 할 것이다. 나아가 혈액형이나 학력의 수집과 주민등록표의 작성·관리 목적 사이에 합리적인 비례관계를 입증하지 못하는 한 그 수집은 개인정보자기결정권을 침해하는 것이 될 것이다.[68]

한편 정부는 이 외에도 디지털화된 수많은 개인정보파일을 보유하고 있다. 2000. 8. 30. 현재 중앙행정기관, 지방자치단체, 정부투자기관 등 전체 4,373개의 공공기관이 모두 452종, 8,421개의 개인정보화일을 보유하고 있다. 그리고 이들 개인정보화일은 예외없이 주민등록번호를 중심으로 구축되어 있다.[69] 이처럼 디지털화된 수많은 개인정보파일이 강제부여된 표준개인식별자로서의 주민등록번호에 의해 전산처리되고 있다고

---

67) 현행 시행령은 1999. 5. 24. 법률 제5987호로 개정된 주민등록법에 따라 1999. 7. 23. 대통령령 제16477호로 전문개정된 것으로서, 이전의 전자주민카드 시행계획을 담고 있었던 1997. 12. 17. 법률 제5459호의 개정법률에서보다 개인정보항목의 수를 줄이고 있다.

68) 정영화, "현행 주민등록번호의 헌법문제와 행정개선방안",『민주사회를 위한 변론』2001년 3/4월호는 개인별 주민등록표에 수록되는 데이터는 "법적 보호이익을 요청하는 민감한 개인정보(sensitive personal information)로서 그 수집과 처리에서 본인의 명시적인 동의를 필요로 한다"고 전제하고, "현행 주민등록법은 본인에게 의사에 반하여 개인 데이터의 신고의무를 지우고 있다는 점에서 명백한 개인의 프라이버시를 침해하는 결과를 초래한다."고 주장하나, 다소 의문이다. 국가에 의한 개인정보수집이 모두 정보주체의 명시적인 동의를 필요로 한다면, 국가의 기능은 정지될 가능성이 높다. 개인정보자기결정권은 정보주체의 동의에 의해서만 정보수집이 이루어질 것을 요구하는 것은 아니라고 보아야 한다.

69) 박홍윤,『한국의 통합정보관리체계에서 개인정보 프라이버시 보호에 관한 연구』(서울대 행정학박사학위논문, 1994), 178면.

하는 사실은 곧 정부가 의도하기만 한다면 포괄적인 개인정보통합관리시스템을 언제라도 구축할 수 있다는 것을 의미하는 것이다.

요컨대, 국가가 전 국민에게 아무런 사용목적의 제한 없이 표준개인식별자로서의 주민등록번호를 강제부여하고 있고, 이러한 주민등록번호를 전면적이고 무분별하게 요구하고 이용하는 현재의 관행은 개인정보통합관리시스템의 구축을 사실상 가능하게 함으로써 헌법상의 개인정보자기결정권을 심각하게 위협할 수 있는 가능성을 안고 있다.

한편, 주민등록번호의 구성상의 문제점을 지적할 수 있다. 주민등록번호의 구성은 생년월일, 주민등록발행지, 성별, 검색숫자로 되어 있는데, 개인의 특성을 식별할 수 있는 생년월일(연령)과 성별은 개인에 따라서 공개하고 싶지 않은 정보일 수 있다. 국가가 이러한 개인정보를 주민등록번호의 강제부여를 통해 공개하는 것은 개인정보자기결정권을 합리적 이유 없이 제한하는 것이라고 생각된다. 물론 주민등록번호의 공개는 직접적으로는 정보주체에 의해 이루어지는 것이지만, 현실 생활에서 주민등록번호의 무분별한 요구 관행은 정보주체가 원하든 원치 안하든 공개하고 싶지 않은 개인정보를 드러내도록 사실상 강요하고 있다. 주민등록번호의 구성은 개인의 특성을 식별할 수 없는 임의의 번호로 이루어져야 할 것이다.

4. 통계법의 문제점

통계목적의 개인정보 수집과 이용을 규율하는 통계법이 있다. 이 법은 통계청장이 지정·고시하는 이른바 지정통계의 경우 통계작성을 위한 정보수집에 응해야 할 의무를 부과하고 있고(법 제10조 및 제12조), 달리 익명권 보호를 위한 장치를 마련하고 있지 않다. 다만, 통계작성을 위하여 수집된 개인 또는 법인이나 단체의 "비밀에 속하는 사항"을 통계작성의 목적 외에 사용하는 것을 금하고 있고(법 제13조 제2항 및 제14조), 통계작성기관에서 통계작성을 위하여 수집·보유·관리하고 있는 기초자료를 변경 또는 말소하거나 통계결과를 변경하는 행위를 금하고 있다(법 제23조). 그러나 이 법 제16조는 통계작성기관의 장에게 법 제13조의 규정에 위배되지 아니하는 범위 안에서 통계자료를 널리 활용하도록 의무지우고 있다. 이 법의 취지에 따른다면, 통계목적으로 수집한 기초자료가 신원확인이 가능한 형태로 보유·관리하는 것이 허용되고 있고, 그것이 "비밀"에 속하지 않는 개인정보인 경우에는 이용 및 제3자 제공에 있어 목적구속의 원칙도 받지 않도록 되어 있다.

더 나아가, 통계목적으로 수집된 개인정보의 이용 및 제3자 제공에 대해서는 그 규율의 일반법인 공공기관개인정보법의 적용도 받지 아니한다(공공기관개인정보법 제3조 제2항). 따라서 수집제한의 원칙, 목적구속의 원칙, 시스템공개의 원칙, 정보주체의 열람 및 갱신청구권의 보장 등 개인정보자기결정권의 헌법적 요청이 거의 무시되고 있다. 판단컨대, 통계목적으로 수집되는 개인정보는 가능한 한 익명으로 수집되어야 하고, 설령 신원확인이 가능한 형태로 수집되었다 하더라도 통계작성의 목적이 완수된 경우에는 그 기초자료는 지체 없이 폐기되어야 할 것이다.[70]

VI. 체계정비를 위한 몇 가지 제언

1. 「개인정보보호기본법」과 「부문별 개별입법」의 체계

현행 법제는 개인정보처리의 위험성이 높고 그만큼 보호필요성이 큰 분야에 보다 엄격한 보호체계가 마련되어야 함에도 그러한 체계성이 부족한 것이 아닌가 생각된다. 즉, 아직 생성 중에 있고 기술발전이 어떤 방향으로 작용하게 될지 명확한 비전이 확립되어 있지 않은 인터넷의 초기 발전단계에서, 그리고 민간의 온라인 개인정보에 대한 상충하는 이익들의 조정에 대해 충분한 사회적 합의가 없는 상태에서, 민간부문 온라인 개인정보에 대해서는 보다 엄격한 보호체계를 마련하고 있는 반면, 보다 큰 위험성이 있는 공공기관이 처리하는 개인정보 및 신용정보에 대해서는 그 보다 약한 보호체계를 갖추고 있는 것으로 평가된다.

또한 여전히 법적 공백상태로 남아 있는 영역들이 많이 있다. 특히 근로자의 개인정보, 유전자정보, 의료기록 등 민감한 영역들에 있어서 개인정보자기결정권을 구체화하

70) 정부가 5년마다 실시하는 인구주택총조사는 매우 광범위한 개인정보를 수집하면서도 그 법률적 근거가 매우 취약하다. 지난 2000년 11월 1일 오전 0시를 기준으로 실시한 인구주택총조사의 직접적인 법적 근거는 2000년 7월 1일 재정경제부령 제143호로 제정된 인구주택총조사규칙이다. 물론 동규칙 제1조는 그 법률적 근거로 통계법 제4조를 들고 있으나, 통계법 제4조 제1항은 "통계청장은 해당 기관의 신청에 의하여 지정기관 또는 지정통계를 지정한다. 이 경우 지정기관 또는 지정통계의 지정요건은 대통령령으로 정한다."고만 규정하고 있을 뿐 인구주택조사에 관한 직접적인 근거규정이라고 보기 어렵다. 가사 이 조항이 법률적 근거가 될 수 있다 하더라도, 재정경제부장관에게 인구주택조사에 관한 권한을 위임하고 있지도 않다. 그렇다면 조사규칙은 일종의 집행명령이라고 할 수 있을 것이나, 이러한 집행명령만으로 국민의 개인정보자기결정권을 심각하게 제한하는 국가행위의 법적 근거로 삼기에는 매우 부족하다. 현행 인구주택조사제도를 본질성이론에 입각하여 그 위헌성을 논하고 있는 것으로, 정태호, 앞의 글(각주 15), 218-225면 참조.

는 입법의 필요성이 높아지고 있다. 물론 이들 영역의 개별 입법에서 대부분 개인의 "비밀"을 강력한 형사처벌의 수단을 통해 보호하고 있다. 다시 말해서, 개인정보처리기관의 내부자가 권한 없이, 또는 권한 없는 제3자에 의해 개인정보가 불법적으로 유출되는 것을 규율하는 정도에 그치고 있다.

그러나 단순한 비밀보호만으로는 오늘날의 놀라운 정보처리기술로부터 개인의 인격적 이익과 인간존엄을 보호하기에는 역부족이다. 수집단계에서부터 그 이용 및 제3자 제공에 이르는 전 과정에 걸쳐 정보처리의 투명성을 확보할 수 있어야만 한다. 그리고 그 처리과정에서 혹시 있을 수 있는 왜곡된 가상인격을 손쉽게 바로 잡을 수 있는 법적 가능성을 확보하여야 한다.

21세기 인간존엄이 보장되는 고도정보사회로의 기반을 조성하기 위해서는 국가사회의 모든 개인정보처리에 대해 정보주체의 개인정보자기결정권이 구현되어야 한다. 이를 구체화하기 위한 입법체계로서는, 「개인정보보호기본법」과 「부문별 입법」의 체계로 나아가는 것이 바람직한 것으로 판단된다.

「개인정보보호기본법」에서는 공공부문과 민간부문을 포괄하여 개인정보의 개념과 보호범위, 수집할 수 없는 개인정보의 종류, 개인정보처리의 기본개념들, 개인정보처리의 기본원칙(수집제한의 원칙, 목적구속의 원칙, 시스템공개의 원칙, 정보분리의 원칙), 정보주체의 권리(열람·정정·삭제청구권, 처리된 개인정보에 근거하여 자동결정이 이루어지는 경우 그에 대한 고지를 받을 권리 및 효율적인 불복청구권 등), 그리고 이를 집행하기 위한 독립된 감독기구(가칭 "개인정보보호위원회")의 조직과 권한을 규정하여야 할 것이다. 이 기본법에서는 개인정보보호를 위한 최저한의 기준을 설정하고, 부문별 입법이 마련되어 보다 강력한 기준이 채택되기 전이라도 기본법상의 최저기준이 집행되어야 할 것이다. 그리고 「부문별 입법」에서는 예컨대 정부부문, 신용정보부문, 의료정보부문, 전자상거래부문(또는 온라인부문) 등 각 부문별로 개인정보처리의 필요성과 위험성의 정도에 따라 보호수준과 기준을 보다 구체적으로 설정하여야 할 것이다.

2. 독립된 지도감독·권리구제 총괄기구의 설치필요성

훌륭한 법제가 아무리 잘 정비되어 있다 하더라도 그 법제운용이 미숙하거나 결함이 있는 경우 개인정보보호의 이념은 충분히 실현될 수 없다. 자기정보에 대한 열람청구권과 갱신청구권 등 개인정보자기결정권을 법률에서 구체화하고 있다고 하더라도 그 실

현을 위한 이니셔티브는 각 정보주체에게 있기 때문에 언제나 일정한 한계를 지닐 수 밖에 없다. 여기에서 개인정보보호를 위한 총괄적이고 독립된 감독기구를 설치할 당위성이 인정된다.

공공기관개인정보법상의 '개인정보보호심의위원회'는 국무총리 소속 하의 단순한 심의기구로서의 성격밖에 가지고 있지 않다.[71] 또한 정보통신망이용촉진및정보보호에관한법률에 의하여 조직된 '개인정보분쟁조정위원회'도 조정기구로서의 성격만을 가지고 있다. 결국 정부부문의 개인정보처리가 법에 따라 이루어지는지를 감독하고 집행할 기구는 전혀 존재하지 않으며, 민간부문의 경우에는 정보통신부 등 관련 부처가 집행책임을 지고 있으나 이들 부처는 민간의 정보처리기관과 깊은 연관을 맺고 있고 한편에서는 관련 산업을 활성화하는 책무도 동시에 지고 있기 때문에 개인정보보호법을 엄격히 집행할 수 있는 전제조건이 갖추어져 있다고 보기 어렵다.

따라서 공공부문과 민간부문에서 개인정보보호원칙의 준수 여부를 실효성 있고 일관되게 감독할 독립적인 개인정보보호감독기관의 설치가 필수적이고 시급하다.[72] 감독기관은 또한 개인정보보호법, 기술규약, 그리고 자율규제의 3요소가 개인정보를 효과적으로 보호하는 공통된 방향으로 결합될 수 있도록 정책을 개발하고 수립하여야 할 것이다. 아울러, 개인정보보호는 이제 국내법제의 영역을 벗어나 범세계적 성격을 띠게 되었다. 이것은 국내법제만으로는 국경이 없는 온라인상에서 개인정보보호를 효과적으로 달성할 수 없다는 것을 의미한다. 감독기관은 개인정보보호를 위한 범세계적 차원의 원칙과 집행기준을 마련하는데 국제협력을 모색하여야 할 것이다.

3. 개인정보보호의 가치와 자유로운 정보유통의 가치 사이의 적정한 균형점 모색

개인정보보호의 가치가 절대적일 수는 없다. 그와 필연적으로 상충하는 또 다른 가치, 즉 자유로운 정보유통의 가치와 조화될 수 있는 적정한 균형점을 찾아내어야 한다. 이러한 균형의 모색에 있어 우선 유의하여야 할 점은, "개인정보보호의 가치"를 "사생활비밀보호의 가치"와 동일시해서는 안 된다는 것이다.

사생활비밀은 그것이 공개되었을 경우 직접적인 인격적 파괴의 위험성이 있기 때문

71) 활동 마저도 거의 전무한 상태이다. 개인정보보호심의위가 1998년부터 2002년까지 정식회의를 개최한 것은 단 한차례에 불과했다고 한다. 또 참여연대의 지적에 따르면, 행정정보 통합 등 전자정부사업을 추진하던 2001년 1월부터 2003년 1월까지 개인정보보호심의위가 교육행정정보시스템(NEIS) 등 전자정부사업의 프라이버시 침해 가능성에 대해서도 전혀 논의하지 않았다고 한다. 한겨레 2003. 8. 5자.

72) 구체적인 방안에 관해서는 성낙인, 『언론정보법』(나남출판, 1998), 540-542면 참조.

에 그 수집에서부터 엄격한 보호가 요구된다. 압수·수색에 있어서의 영장주의, 사생활비밀, 통신비밀의 헌법적 보장은 이러한 요구의 반영이다. 반면에, 이러한 사생활비밀에 속하지 않는 개인정보의 유통은 많은 경우 사회의 형성에 불가결한 조건이 되기도 한다. 우리는 타인의 개인정보의 유통을 통해 그를 평가하면서 다양한 사회관계를 형성시켜 나간다. 오히려 헌법 제21조가 보장하는 언론·출판의 자유는 사생활비밀에 속하지 않는 개인정보의 자유로운 유통을 보장하고 있다고 하겠다.

그럼에도 불구하고 오늘날 개인정보에 대한 보호의 요구가 생겨나는 것은 디지털화된 개인정보의 효과적인 통합가능성에 따르는 위험성을 사전에 봉쇄하기 위한 데에 기본취지가 있다. 따라서 디지털시대의 개인정보보호는 '은둔으로서의 사생활비밀보호'에 초점이 있는 것이 아니라, 정보처리에 대한 참여권 내지 역감시권으로서의 기능에 중점이 놓여져 있는 것이다.

개인정보보호법제를 형성하고 적용함에 있어 혹시라도 '은둔으로서의 사생활비밀보호'의 관점에서 접근한다면 그것은 상충하는 가치 사이의 균형을 잃게 될 것이다. 개인정보자기결정권의 가치와 자유로운 정보유통의 가치를 함께 조화시키는 방향으로 법제가 마련되어야 할 것이다.

이 점과 관련해서 균형을 상실했다고 볼 수 있는 몇 가지 사례를 예시하면 다음과 같다.

첫째, 공공기관의정보공개에관한법률 제7조 제1항 제6호는 비공개대상정보의 하나로서 "개인정보"를 제시하고 있다. 이 조항은 개인정보, 즉 "당해 정보에 포함되어 있는 이름·주민등록번호등에 의하여 특정인을 식별할 수 있는 개인에 관한 정보"에 해당하기만 하면 곧 공개하지 않을 수 있도록 하고 있는 것이다. 이는 공공기관이 보유하고 있는 일체의 개인정보를 사생활비밀보호의 관점에서 접근한 결과라고 생각된다.

둘째, 공개되는 판결문에 당사자의 이름을 정확하게 표시하지 않는 법원과 헌법재판소의 관행은 헌법상 공개가 요구되는 공적 기록(헌법 제109조)에 담긴 이름을 마치 사생활비밀성이 인정되는 개인정보로 잘못 이해한 결과라고 하겠다. 이 같은 문제점은 언론사의 범죄보도와 관련한 명예훼손소송에서 익명보도의 원칙을 법적 기준으로 채택한 대법원의 판결에서도 유사하게 발견된다.[73]

셋째, 스팸메일 규제방식 중 Opt-in 방식은 온라인상의 이메일계정을 사생활비밀의 보호영역으로 간주한 결과 광고표현의 자유를 경시하는 정책결정이라고 평가될 수 있

73) 이 대법원 판결에 대한 비판은 이인호, "범죄보도와 면책사유의 적용", 『언론중재』 제19권 제3호 (언론중재위원회, 1999. 9) 참조.

다. 또한 우리 정보통신보호법 제50조 제6항이 전자우편주소의 자동생성프로그램을 이용한 광고성 정보전송을 금지하고 위반에 대해 1천만원 이하의 벌금에 처하고 있는 것은 전자우편주소 및 이메일계정을 사생활비밀로 이해한 결과가 아닌가 생각된다. 마찬가지로, 동법 제50조의2는 수집거부의사가 명시된 홈페이지에서 이메일추출기를 이용하여 전자우편주소를 수집하는 행위를 처벌(1천만원 이하 벌금)하고 있는데, 만약 이메일추출기가 수집거부의사를 인식하여 정확히 해당 홈페이지를 제외시키는 것이 기술적으로 불가능하다면, 이 규정은 사실상 이메일추출기의 사용 자체를 금지하는 것이 된다. 이러한 입법정책의 배경에는 공개된 전자우편주소까지도 사생활비밀의 관점에서 지나치게 보호하고자 하는 사고가 작용하고 있는 것이 아닌가 생각된다.

VII. 맺는 말

20세기 후반부에 펼쳐진 "위험사회"(Risikogesellschaft)는 근대적 인간이 그 동안 자연과 역사에 관한 예측가능성에 대한 믿음을 바탕으로 사회적 삶의 조건과 자연에 개입한 결과 이른바 가공된 위험(manufactured risk)이 항존하고 그에 따른 불확실성이 증대하는 사회이다. 독일의 사회학자인 울리히 벡(Ulrich Beck)은 그의 저서 『위험사회』[74]에서 산업혁명 이래 근대적 합리화과정 전반에 대한 비판적인 재평가 및 향후의 발전방향에 대한 새로운 모색을 추구하고 있다. 위험이 평상적인 지각범위를 벗어나고 산업적 논리 속에서 체계적으로 재생산되면서 현대사회는 위험사회로 이행된다고 전망하는 그는, 경제적 부를 희생할지라도 위험을 사전에 철저히 봉쇄하는 것이 위험사회에서 인류가 취할 수 있는 유일한 발전경로라는 점을 지적한다.

디지털 정보혁명의 결과 정부와 시장은 개인정보의 수집・처리・이용・공개의 매력적인 유혹을 쉽게 뿌리칠 수 없게 되었다. 그것은 엄청난 효율성과 생활의 편익을 제공한다. 그러나 그 효율성과 편익의 배면에는 동시에 엄청난 파괴력을 지닌 위험이 도사리고 있다. 그 위험은 인간존엄과 자유민주체제의 근간을 흔들 정도로 위협적이다. 그 위험이 가시화되었을 때는 이미 돌이킬 수 없는 상태로 드러날 것이다. 따라서 그 위험이 더 이상 진행되기 전에 방어벽을 구축해야 한다. 그리고 새로운 성격의 위험은 새로운 내용의 방어벽으로 차단해야 할 것이다.

---

74) 울리히 벡/홍성태(역), 『위험사회 - 새로운 근대(성)를 향하여』(새물결, 1997).

공공기관 보유 개인전자정보의 학술적 이용에 대한 고찰

김 옥 주
(고려대학교 의과대학 : 의사학 및 의료윤리 전공)

순 서

1. 들어가는 말 ……47
2. 개인정보보호와 학술활동을 위한 정보유통 ……48
3. 국내 공공기관 보유 개인전자정보의 학술적 이용의 현황과 문제점 : 의료 정보의 예 ……50
4. 외국의 사례 : 미국과 영국 ……52
5. 체계 정비를 위한 제언 ……55
6. 맺는 말 ……56

공공기관 보유 개인전자정보의 학술적 이용에 대한 고찰

김 옥 주
(고려대학교 의과대학 : 의사학 및 의료윤리 전공)

1. 들어가는 말

1990년대 후반에 이르러 정보가 전산화되어 다량의 정보가 누적되고 옮겨지는 것이 용이해진 이래, 정보 관리의 효율성과 개인의 정보 보호의 중요성이 대두되기 시작했다. 집적된 다량의 정보는 원래의 행정적 목적 이외에도 공익성을 갖는 지식 창출을 위한 다양한 학술 연구의 자료로 사용되어 왔다. 선진국에서는 수십년간 집적된 정보를 통해 사회적으로 유용한 연구들이 많이 수행되어 이루어 왔으나, 최근 들어 전자정보 기술의 발달로 인해 정보 구축이 보다 용이해지면서 개인정보의 보호에 대한 필요성이 민감한 주제로 떠오르게 되었다. 특히 의료 정보와 같이 개인의 사생활과 비밀과 관련된 정보가 당사자가 알지도 못하는 사이에 제3자에 의해 학술연구의 목적으로 이용될 때, 이는 인간의 기본 권리인 사생활에 대한 권리를 침해할 수 있다는 점이다. 개인의 사생활 보호와 공공의 이익을 위한 연구라는 양극의 가치를 어떻게 하면 균형을 맞출 수 있을 것인가? 선진 각국에서는 자국의 역사, 제도, 문화, 법률 등에 따라 양 쪽의 비중이 차지하는 정도가 다르나, 각 사회에 맞는 균형점에서 정책을 수립하고 있다. 즉, 개인 정보의 학술적 이용에 대한 안전장치, 한계, 공정한 절차 등을 제시하고 이를 실행에 옮길 수 있는 지침과 법률을 마련하고 있다.

'공공기관 보유 개인전자정보의 학술적 이용'이라고 할 때 상당히 다양한 범주의 공공기관과 이들이 보유한 개인정보가 포함될 것이다. '공공기관'이라는 범주를 어디까지 정할 것인가? 정부 행정 각 부처, 통계청, 보험공단 뿐 아니라 학교, 병원, 은행 등 사설 기관이나 공공성을 띄는 다양한 기관들도 이에 포함될 수 있을 것이다. 또한 이들이 보유하고 있는 '개인전자정보'의 종류와 성격도 각 기관의 목적에 따라 다양하다고 볼 수 있다. 다양한 종류의 학술 연구 가운데, 국제적으로 연구대상자의 비밀과 정보보호

를 포함하여 연구대상자의 안녕과 복지를 보호하도록 연구윤리가 발달된 분야가 의학연구이므로 이 글에서는 의료 정보와 보건의료 및 의학연구의 예를 들어 이 문제에 접근하고자 한다.

2. 개인정보보호와 학술활동을 위한 정보유통

개인의 사생활에 대한 보장은 기본적인 인권이다. 자신이 원하는 사람에게만 자신과 관련된 정보에 대해 언급할 수 있어야 한다. 자신과 관련된 사실과 정보를 통제할 수 있는 것은 한 인간이 안전, 자유, 존엄성을 유지하는 데에 기본적인 전제가 된다. 또한 이것은 자신을 부당한 차별과 편견으로부터 보호하게 해 준다. 의료에서 의사가 환자로부터 환자진료를 위해 취득한 정보에 대한 비밀을 유지하는 것은 의사-환자관계의 토대를 이루며, 사회가 의료계 전반에 대한 신뢰를 가능케 하는 전제를 이룬다. 이 전제가 없이는 진료가 불가능할 것이다. 따라서 환자의 사생활과 비밀을 지키는 것은 B.C. 460년 경의 히포크라테스 시대의 고대로부터 지금까지 가장 중요한 의사윤리이자 법적인 의무이기도 하다. 업무상 환자로부터 취득한 기밀을 누설하지 않는 의료인의 법적 윤리적 의무는 정상적 진료와 보건의료 활동을 위해 필수적인 환자-의사관계의 확립을 위해 필수적인 것이다. 의료정보는 환자 자신이 본인의 진료를 위해, 즉 본인의 이익을 위해서 의료인에게 제공되며, 진료환경 밖으로 누출되지 않는다는 점을 전제로 한다. 또한 한 개인으로서 환자는 자신의 사생활과 의료정보에 관한 정보를 통제할 권리가 있다.

이렇듯 진료 목적으로 수집하고 축적된 의료정보가 환자 자신이나 공공의 이익을 위해서 사용하여야 할 경우가 많다. 특히 중요한 의학연구에서는 의료정보가 필수적인 경우가 많다. 급성전염병 관리 및 감독을 위해서나 신약 부작용을 전국적인 규모로 감시하고 관리하기 위해서, 또한 국민 보건의료와 직접 관련되는 대규모 역학 연구 등을 위해서는 축적된 개인건강정보를 이용하여야 한다. 예들 들어 핵 시설 근처에서 발생하는 백혈병에 관한 환경 역학연구와 같이 핵시설과 백혈병발생과의 인과관계를 밝히기 위한 목적으로 수행하는 연구는 동일한 목적을 위해 처음부터 피험자를 모집하여 연구를 수행하는 것이 비윤리적이며 불가능한 경우도 많다. 또한 1950년대 말에 대규모로 유럽에 판매되었던 진정제인 탈리도마이도가 유럽 전역에 걸쳐서 판매되었을 때, 유럽의 소

아과 여러 곳에서는 팔다리가 절단되어 출생되는 기형인 사지절단증(포코맬리아)이라는 희귀한 기형이 많이 발생되었으나, 그 인과관계를 파악하는 데에 아무런 장치가 없었기 때문에 약은 계속 팔렸고 피해자는 계속 증가하였다. 의약사(醫藥史)에 잊지 못할 뼈아픈 교훈으로 기억된 탈리도마이드 약화사고 이후, 의약품 허가조건이 까다로워진 것 뿐 아니라 시장에 약이 판매된 이후에도 이상부작용 정보를 수집하는 체계 및 연구분야(약물역학, 약물안전성감시체계론)가 생기게 되었다. 이러한 분야는 상당한 규모로 다년간 축적된 의무기록을 바탕으로 이루어져야 하고, 정확성을 위해 개인식별자가 필요한 경우도 많다. 약물안전성감시 및 약물역학이 발달된 미국의 경우, 20여년 전부터 환자 처방 및 의약품 제조 기록이 누적된 정보나 큰 보험회사들의 데이터베이스들이 이러한 연구에 사용되었다.(J.S. Gardner, B.J. Park, and A. Stergachis, 2000) 이 외에도 많은 종류의 보건의료 및 의학연구는 진료 목적으로 수집 및 축적된 자료를 사용하여야 하는 경우가 많다. 기존의 의료정보를 사용하는 것을 피하기 위해, 동일한 연구 목적으로 연구를 새로 설계여 피험자를 모집하고 임상연구를 할 경우 효율성과 비용 면에서 비교되지 않을 정도로 차이가 나는 경우도 있다. 이는 어느 사회나 항상 부족하기 마련인 의료자원을 낭비하며, 불필요하게 피험자들을 새로운 위험에 노출시키며, 동시에 국가나 사회의 비용과 자원을 중복되게 사용하여 사회 구성원의 부담을 증가시키는 결과를 낳게 된다.

개인의료정보를 이용한 의학 및 보건학 연구들이 사회의 공익을 위해 반드시 필요하다고 하여도, 환자의 사생활권리를 침해할 수 있으며 의료인의 비밀보장의 의무를 위반할 수 있기 때문에 중요한 윤리적 문제를 제기한다. 이에 관해서 다양한 의학연구 마다 각자의 분야에서 제기되는 의학연구 윤리의 문제를 해결하고, 연구의 공공성과 개인의 권리보호 사이에 균형을 맞추어 양자를 최대한 보장할 수 있는 장치를 개발하고, 이에 대한 사회적 합의를 도출하는 것이 과제가 된 것이다.(Arthur Caplan et al.2000; D.A. Boswell & E.B. Andrews. 2002)

개인건강정보를 사용하는 연구에서 가장 중요하게 발생하는 문제는 사생활 침해(privacy)와 비밀보장(confidentiality)의 문제이다(B. A. Brody. 1998). 사실상 환자들은 자신의 정보가 어느 범위까지 누구에게 어떤 방법으로 공유되고 전파되는지 알고 있지 못한 경우가 많다. 또한 의료정보는 개인의 안녕과 복지에 큰 영향을 줄 수 있는 "민감한 정보(sensitive information)을 포함한다. 예를 들어 유전성 질환, 정신질환, 전염성 질환, 선천성 기형 등에 관한 진료정보는 본인의 결혼, 취업 뿐 아니라 가족들의 문제

에도 영향을 줄 수 있는 민감한 정보이다. 또한 개인의 유전정보는 정보가 포함하는 범주가 개인에 그치지 않고, 가족과 친척에게까지 이르게 된다. 이렇게 안녕과 복지에 영향을 주는 의료정보를 이요하는 연구들은 마땅히 필요한 정당한 절차와 안전장치를 거쳐서 수행되어야 한다. 이 절차의 핵심은 정보보유자의 ”동의(informed consent)"나 “승인(authorization)"을 받는 것과 연구자로부터 독립된 연구윤리심의위원회(research ethics review board, institutional review board, ethics committees 등)로부터 연구로 인해 피험자에게 초래하는 위험이 크지 않으며, 전체적으로 연구의 위험보다 이로부터 얻는 이익이 상회할 때 승인을 받고 지속적인 관리 감독을 받으며 최대한의 안전장치를 가동시킨 가운데 연구를 수행하는 것이다.

21세기의 의학 및 보건학 연구는 점점 더 국제화 · 세계화되는 추세여서 연구에 필요한 의학정보가 한 나라에 국한되지 않으므로 윤리규정 및 지침 또한 세계적으로 통일되는 추세이다. 예를 들어 전 세계의 100개 센터에서 시험이 되는 신약 임상연구의 경우, 한 곳에서 부작용이 발생하여도 24시간 이내에 곧 다른 100여 센터에서 누구에게 무슨 문제가 발생했는지 보고받으며, 이 보고서에는 개인 정보도 포함되어 있다. 세계의사회, 세계보건기구 등을 중심으로 선진국이나 개발도상국, 후진국 모두에서 동일하게 표준화된 의학연구윤리지침에 근거하여 연구를 수행하도록 권고하고 독려하여, 연구에서 발생할 수 있는 취약한 피험자들이 받을 수 있는 피해를 최소화하고, 신진국 연구자들에 의하여 후진국 피험자들이 피해보는 것을 방지하도록 지속적인 노력을 하고 있다.(B.A. Brody. 1998)

3. 국내 공공기관 보유 개인전자정보의 학술적 이용의 현황과 문제점 : 의료 정보의 예

우리나라에서는 공공기관에서 보유하고 있는 개인의료정보의 학술이용에 대한 지침이나 법률이 마련되어 있지 않다. 예를 들어 연구자가 국민건강보험공단의 자료를 이용하여 특정 암에 관련된 연구를 하려고 할 때, 이를 뒷받침해 줄 수 있는 법이나 지침이 없는 실정이다. 공단 자료 뿐 아니라 각급 병원 및 의료기관에서 환자를 진료하면서 생성되는 진료 및 진료비 지불과 관련된 모든 전자 정보는 개인건강정보(personal health information)로 보호받는다. 우리나라 의료법 19조와 형법 317조에 의해 환자 정보의 비밀 누설을 금지하게 되어있다.

현재 국내에서 공공기관이 보유한 개인건강정보의 학술적 이용에 대한 지침이나 법률이 없지만, 이 두 가지 문제를 최소화하는 연구 수행을 위해서 다음의 방법을 취할 수 있다. (1) 각 개인에게 연구목적으로 정보사용에 대한 동의(informed consent)나 허가(authorization)를 얻는다. (2) 정보를 소지한 기관에서 연구자에게 연구목적으로 정보를 제공할 경우, 통계전문가에 의해 이름, 주민등록번호, 주소 등과 같은 개인 식별자(identifier)를 없애고 익명화된 자료를 제공한다. (3) 연구수행 이전 연구계획에 대한 소속 기관의 연구윤리위원회(Institutional Review Board, 이하 IRB)의 승인을 받는다.

그러나 국내의 연구 현장을 보면, 위의 세 가지 요건이 현실적으로 실천 가능하지 못하다. 첫째, 개인별 동의취득은 현실적으로 불가능한 경우가 대부분이다. 둘째, 자료를 가지고 있는 공공기관에서 연구의 중요성에 대한 인식이 부족한 경우가 많다. 또한 연구목적으로 자료를 제공할 경우, 각 공공기관이 어떠한 원칙과 표준운영지침(standardized operating procedure, SOP)에 따라 연구자에게 자료를 제공할 것인가에 대한 제도적 장치가 없다. 셋째, 국내 보건복지부에 의해 임상시험센터로 지정된 70여 개의 병원에서 기관 연구윤리위원회(Institutional Review Board)가 존재하는데, 5년 정도의 짧은 역사를 지닌 국내 IRB들은 연구 심사 및 감독의 범위과 질이 매우 다양하다. 2002년 설문조사에 의하면 국내 IRB는 주로 법률에 의해 구속을 받는 임상시험(clinical trial)만을 심사하고 의료정보에 기초한 연구 등 학술연구는 심의하지 않는 곳이 많다. 즉, 개인이 식별되는 개인의료정보를 이용한 연구는 피험자 보호를 위해 IRB 심의를 받아야 하지만, 국내 IRB 중 잘 운영되고 있는 곳은 몇군데에 불과한 것으로 나타났다.(김옥주 2002, 2003)

무엇보다 가장 큰 문제는 우리 사회 전반적으로 개인 정보보호에 대한 인식이 취약하다는 점이다. 즉, 개인은 개인의료정보에 대한 권리의식이 취약하며, 연구자들은 의료정보로 연구할 때에 윤리적 민감성을 가지고 다루어야 한다는 의식이 보편적으로 형성되어 있지 못하다. 현재 이러한 정보를 가지고 연구를 수행하는 학자들은 필요할 때 통계학자의 도움을 받거나 본인 스스로 자료를 익명화(anonymise)하거나, 연구자 자신의 양식에 근거하여 연구를 수행하고 있다. 그리고 연구윤리심의위원회(IRB) 운영이 잘되고 있는 연구기관에서는 연구계획서를 사전 심사하여 연구를 관리·감독하고 있다. 지금까지는 관련 분야 연구자들이 선의의 연구(bona fide)를 수행하고 연구자로서의 성실성(integrity)의 문제가 있었던 경우가 없었기 때문에, 다행스럽게도 제도의 미비함에도 불구하고 외국에서와 같은 불명예스러운 일들(scandal)이 발생하지 않았다고 볼 수 있다.

또한 의료 정보보호를 의료인의 진료상 취득한 개인정보보호에 한정되어 있다는 것이 문제이다. 이것은 소극적 의무로 비밀을 누설하지 않는 의무이며, 공익을 위해 정보사용이 필요한 경우, 의료인이 책임의 주체가 되어 할 수 있는 일이 없다. 공익을 위해 안전하게 정보를 유통할 수 있게 하려면, 기관이 주체가 되어 대규모 의료정보에 관한 수집, 저장, 가공, 전달, 사용 등에 관한 책임을 지는 체계가 필요하다. 또한 법적으로 포괄하는 의료정보의 범위가 보험공단 등의 공공기관 자료 뿐 아니라 병원 및 연구소에 있는 의료정보에 대한 통일적 접근을 하여야만, 정보를 이용한 학술연구에서의 실제적이고 효율적인 의료정보보호가 이루어질 것이다.

4. 외국의 사례

의료가 사회주의화된 유럽에서는 개인건강정보를 가지고 있는 기관이나 연구기관 공히 국가 공공기관이므로, 개인정보보호가 엄격하다고 평가받는다. (A. Caplan; 2000: 417-431) 반면, 미국은 사보험(private insurance)이 주를 이루기 때문에, 개인건강정보에 대하여 비교적 실용주의적인 정책을 취하고 있으며, 영국은 유럽대륙과 미국의 중간적 입장을 취하고 있다.

(1) 미국

의학연구와 관련해서 사회적으로 문제를 야기시키는 일이 많았던 미국에서는 1970년대 이후 의학연구윤리와 관련된 법률과 지침을 강화하였다. 정보전산처리 기술의 발전으로 보건의료체계의 효율성을 높이고자 의료관련 행정적, 재정적 자료의 전자 교환을 표준화하는 것을 의무화하는 법률이 1996년 8월 21일 Health Insurance Portability and Accountability Act of 1996 ("HIPAA", Public Law 104-191)이란 이름으로 통과되었다. HIPAA의 Sections 261 - 264는 전자정보교환, 건강정보의 사생활보호(Privacy)와 안전에 관한 조항을 규정하고 있다. 이 법에 근거하여 1999년 11월 3일 미국연방정부의 Department of Health and Human Services (DHHS)에서 '사생활보호법(Privacy Rule)' 초안을 공고하고 의견수렴에 들어가, 수차례의 의견수렴과정을 거쳤다. 2002년 8월 14일 최종적으로 The *Standards for Privacy of Individually Identifiable Health Information*

(줄여서 "Privacy Rule")이라는 이름으로 법률이 확정되어 (45 CFR Part 160 and Part 164, Subparts A and E), 2003년 4월 14일까지 대부분의 의료정보보유기관들이 이 법률에 따라야 하고, 2004년 4월 14일까지는 소규모의 의료보험기관들도 모두 이 법률에 따르도록 되어있다. (http://www.hhs.gov/ocr/hipaa)

이 법안은 처음으로 건강정보의 보호에 관하여 미국 전역에 적용되는 최소한의 법률로서 각 주마다 더 엄격한 법률이 있는 경우에는 그것도 준수되어야 한다. Privacy Rule의 핵심을 즉, 개인의료정보의 자기결정권을 명확히 부여하였다는 점이다. 즉, 건강정보를 보유하는 기관("covered entities")들이 지켜야 할 보호되는 개인건강정보("protected health information")의 사용과 제3자 제공의 기준을 정하였고, 개인이 자신의 건강정보에 관한 사생활보호권리(privacy right)를 이해하고 자신의 건강정보 사용에 대해 통제할 수 있는 방법에 관한 기준을 마련하였다. 이 법률을 집행하고 감독하기 위해 DHHS내에 Office for Civil Rights ("OCR")를 두어 각 기관이 Privacy Rule을 반드시 준수하도록 하였다. Privacy Rule의 주요 목표는 개인 건강정보가 적절하게 보호되는 것을 보장하는 동시에 공중보건과 질높은 보건의료제공을 위해 건강정보의 흐름을 허용하는 것이다. 따라서 이 법률은 중요한 정보사용 사업들과 개인의 의료정보보호 사이에 정확한 균형을 잡고자 하는 것이라고 볼 수 있다. 미국의 의료시장이 워낙 방대하고 다양하여서, 이 법률은 유연하고 다양한 요구들을 포괄하도록 고안되어있다.

이 법률에 의해서 연구 목적으로 보호되는 개인건강정보("protected health information")의 사용이 적법한 절차를 거치면 허용되었다. 연구자들은 기존의 피험자 보호 법률은 다 지키면서도 “사생활보호법”이라는 새로운 법률을 지켜야한다. 기본적으로 의료정보의 당사자가 정보사용을 허가(authorization)하여야 정보를 사용할 수 있다. 허가를 받지 못하는 경우에 세부사항에 대해서도 자세한 규정이 있다. 의료정보에 기초한 학술연구 지침은 연방정부와 주정부 지침이 공히 적용되는데, 연방정부지침은 최소한의 지침이며 각 주마다 법적 요구가 더 엄격할 수 있다. 즉, Common Rule이라는 Title 45CFR Part 46과 FDA의 Title 21 CFR Part 450과 56에 Privacy Rule은 Title 45 CFR Part 164로 포함되게 된 것이다. 피험자 보호를 위하여 IRB 심의를 거쳐야 하고, 정보보호를 위한 심사는 IRB에서 같이 검토할 수도 있으며, 위원의 구성조건이 조금 더 약한 Privacy Board Review에서 심의할 수 있다.

(2) 영국

영국의 경우 국가 의학연구비를 지급, 관리하고 연구 관련 정책을 수립하는 의학연구위원회(Medical Research Council)에서 1972년부터 임상연구, 임상시험, 역학 및 기타 공중보건 연구에 개인정보를 수집 · 사용할 수 있는 제도를 정비하였다.(Medical Research Council. Personal Information in Medical Research. October 2000) 이후, 이러한 의무기록에 근거한 연구들을 통하여 영국에서는 중요한 의학적 지식의 진보가 있었다. 즉, 신종 전염성 질환의 역학 연구에 중요한 발전이 있었으며, 암환자 치료에 진보가 있었고, 걸프전쟁과 연관된 질병이나 핵시설 근처의 백혈병 발병 등 불명확했던 병인들이 밝혀졌고, 아스피린 등 심장병의 새로운 예방 및 치료에 대한 평가가 이루어졌으며, 유아사망률이 저하되었다. 의학연구에서 개인정보의 사용이 불가피하고, 정보주체로부터 동의를 받는 것이 불가능하고, 정보주체에 대한 피해가 미미하며, 연구의 결과가 사회에 주는 유용성이 클 때, 영국은 의학연구에 개인정보의 사용을 허락하고 있다. Medical Research Council의 기본 입장은 의학연구에 개인정보를 사용하는 것이 법적으로 정당한가에 대한 판단은 개별 연구를 직접 판단해야 한다는 공식입장을 표명하였으며, 다음과 같은 판단기준을 제시하였다. (1) 동의구득의 불가능과 익명화된 자료사용이 불가능한 상황인 불가피성(necessity) (2) 자료의 민감성 (sensitivity) (3) 연구의 중요성 (importance) (4) 자료처리 및 사용과정의 안전성 (safeguards) (5) 연구윤리위원회의 독립적인 심사 (independent review) (6) 명시적 동의가 불가능한 상황이라면 만일 동의가능한 상황에서는 정보주체가 동의를 하였겠는가에 대한 예측(expectation)

2003년 1월에는 국무총리가 2001년 Health and Social Care Act의 “section 60"을 부과해서 정보주체의 동의 없이도 연구를 수행할 수 있는 제도를 만들어 공포했다. 이에 의하면, 동의르 ᆯ 구한다든지, 익명화된 자료 사용이 불가능한 상황에서, 즉 다른 실제적인 대안이 불가능한 상황에서만 허용되며, 연구가 중요한 주제인 경우, 법률에 의해 만들어진 환자정보자문위원회(Patient Information Advisory Group, PIAG)에서 심사하여 연구를 허용하도록 하였다.(Health and Social Care Act 2001: "Section 60" New guidance added - January 2003)

영국과 미국의 경우를 요약하면, 개인정보보호의 중요성을 보장하는 가운데, 안전장치와 적법한 절차를 거쳐 필요한 연구를 수행하도록 정보의 사용을 허용하고 있다고

볼 수 있다. 이는 국제적으로 의학연구윤리의 경향이 과거의 소극적인 피험자 보호라는 측면에서 적극적으로 피험자보호와 연구의 발전을 통일적으로 접근하는 쪽으로 방향전환 한 것과도 일맥상통한다고 볼 수 있다. (김옥주, 뉘른베르그강령과 인체실험의 윤리. 2002)

5. 체계 정비를 위한 제언

첫째, 정보보호와 공공연구의 촉진을 이루기 위해서는 국가 차원에서 의료정보 전반에 대한 법률, 규정 또는 관리 지침이 있어야 한다. 먼저 개인의 의료정보통제권을 부여하여야 한다. 즉, 개인이 자신의 의료정보를 열람하고, 자신의 의료정보가 누가, 언제, 어떻게, 왜 저장하고 사용하는지 알 수 있어야 한다. 또한 의료서비스를 제공하는 공사립 의료기관의 의료정보, 각종 연구기관이 보유한 의료정보, 보험공단 등의 의료정보의 수집, 저장, 가공, 이용, 전달에 관하여 일관성 있고 포괄적인 법률 및 지침이 있어야 할 것이다. 현실적으로 대규모 인구를 대상으로 하는 연구들이 진행 중이며, 생명의료공학이 첨단과학기술분야로 국가적으로 지원을 받고 있는 지금, 각종 사업단, 각종 정보은행 및 조직은행, 연구소 등에서 연구목적으로 의료정보를 축적 및 사용하고 있는데, 어떠한 기준으로 정보를 수집하고, 누가 어떠한 절차를 거쳐, 왜 정보를 사용하고 관리하는 지에 대한 기준이 마련되어 있지 않은 것이다. 이러한 상황에서 개인의료정보보호의 책임 주체를 환자 진료를 하는 의료인 개인에만 둔다면, 연구에 사용되는 정보에 대한 공정하고 책임 있는 절차의 확립이 가능하지 않을 것이다. 진료기관, 연구기관, 진료비처리기관 등 정보를 다루는 기관이 책임의 주체가 되어 의료정보의 수집, 저장, 가공, 이용, 전달에 관한 표준화된 지침을 따르도록 해야 할 것이다.

둘째, 이러한 규정들이 원칙성과 현실성을 동시에 지니기 위해서는 이 문제에 관해 실질적인 문제의 담지자들의 의견을 수렴하여야 한다. 정보보호의 중요성에 대한 공감과 더불어 길고 복잡한 과정을 거쳐 이루어지는 보건의료 연구의 중요성과 필요성에 대해서도 사회적인 공감이 이루어져야 하며, 투명하고 공정한 정보처리과정에 대한 사회적 합의도 이루어져야 할 것이다. 일반 시민들의 의견, 환자들의 의견, 연구자들의 의견, 학회의 의견, 관련 정부부처의 의견 등, 사회 각 부문의 의견이 수렴되어야 할 것이다. 미국의 Privacy Rule에 대해서도 이것을 확정하고 공포하기 전까지 오랜 기간을 거

쳐 다양한 분야의 사람들로부터 의견을 종합하고 수렴하는 과정을 거치었다.

셋째, 연구자가 개인의 권리와 존엄성을 보장하는 연구를 수행하도록 심의과 감독의 책임이 있는 연구윤리심의위원회(IRB)를 국내에서 더욱 활성화시켜야 할 것이다. 현재 식픔의약픔안전청의 규정 하에 신약임상시험에만 국한되어있는 활동을 더욱 확대하여, 역학연구 등 정보와 기록에 근거한 학술연구의 안전성과 윤리성에 대한 심사 및 감독도 수행하여야 할 것이다. 우리나라처럼 국가규모로 의학연구윤리를 진작시키는 위원회나 조직이 없는 상황에서, IRB에 많은 것을 의존할 수밖에 없는 상태이지만, 각 기관별로 IRB 운영이 차이가 많이 나므로, IRB위원 교육을 더욱 확대하고 행정적, 재정적 지원을 더욱 많이 하도록 하여야 한다. 중장기적으로는 생명의료위원회나 정보보호를 위한 위원회의 산하에 의료정보보호를 위한 소위원회를 두어 개인정보보호와 효율적인 정보유통을 가능하도록 하여야 한다.

마지막으로, 정보보호의 중요성에 대하여, 사회구성원 전반, 연구자, 의료인, 의료정보 소유기관, 이용기관, 연구윤리심의위원회 등에서 활발한 논의와 교육이 이루어져야 한다. 미국의 경우 의료정보에서의 사생활규칙(Privacy Rule)을 2004년 4월까지 적은 보험회사까지 포함하여 모든 의료정보처리기관이 준수하도록 되어있다. 이의 집행을 위해 DHHS 산하에 시민권리국(Office for Civil Rights)에서 2-3년의 기간을 두고 일반인에 대한 홍보와 교육, 병원 및 보험회사들에 대한 교육, 연구자들에 대한 교육 등 해당 사항에 관한 지식, 법률, 지침, 절차상 지켜야할 점 등에 대하여 널리 홍보 및 교육을 하고 있다. 특히 연구 부문과 관련해서는 CDC, NIH, OHRP 등, 해당 관련 기관과 협력하여 홍보와 교육사업을 진행하고 있다.

6. 맺는 말

정보화가 빠르게 진행되는 우리 사회에서는 정보와 관련된 시민의 권리, 인권의 문제는 더 이상 미룰 수 없는 중요한 문제가 되었다. 그러나 아직 이 문제에 대해 사회 전체적으로 문제를 인식하고 정책에 대한 합의를 도출하지 못한 상태이다. 학술연구와 관련된 정책 뿐 아니라 의료정보 및 개인정보 전반에 대한 정책이 수립되어야 한다. 또한 개인전자정보를 사용하는 학술연구와 관련한 제도적 정비와 인프라를 구축하는 것이 필요하다. 이러한 구조적인 정비가 되지 않았기 때문에, 개인정보에 대한 권리를 행사

해야 할 개인 뿐 아니라, 정보를 보관 및 관리하고 있는 기관의 역할과 정보를 활용하여 연구를 해야 할 연구자들이 모두 보호받지 못하고 불투명한 가운데 되어가는 대로 일을 하고 있는 것이다.

어떻게 개인정보 보호와 공익성을 갖는 학술연구 진흥을 동시에 이루어낼 것인가? 이제 이 문제에 직접 관련된 사회 구성원들이 모두 나서서 지혜를 모아야 할 때이다.

▌참고자료 목록

논문 및 저서

T.L. Beauchamp & J. F. Childress. Principles of Biomedical Ethics. Fifth edition. 2001. Oxford University Press.

B.A. Brody. The ethics of biomedical research: An international perspective. 1998. New Yok; Oxford University Press.

D.A. Boswell & E.B. Andrews. Ethical Oversight, Consent, and Confidentiality. Pharmacovigilance. Edited by R.D. Mann & E.B. Andrews. 2002. John Wiley & Sons, Ltd.

J.S. Gardner, B.J. Park, and A. Stergachis. Automated Databases in Pharmacoepidemiologic Studies. Pharmacoepidemiology: An Introduction.2000. 368-38.

Arthur Caplan et al. Bioethical Issues in Pharmacoepidemiology Research. Pharmacoepidemiology. Third Edition. Edited bu B. L. Strom. 2000. John Wiley & Sons, Ltd.

R. F. Weir. Edited. Stored Tissue Samples: Ethical, Legal, and Public Policy Implication. 1998. University of Iowa Press.

Kim OJ, Park BJ, Sohn DR, Lee SM, Shin SG. Current status of the institutional review boards in Korea: constitution, operation, and policy for protection of human research participants. J Korean Med Sci 2003 Feb;18(1):3-10

김옥주, 뉘른베르그강령과 인체실험의 윤리. 의료・윤리・교육 2002; 5(1): 69-96.

김옥주, 우리나라 임상연구심의위원회의 현황. 대한임상약리학회지 2002: 10(1): 67-69.

영국 자료

Health and Social Care Act 2001: "Section 60" New guidance added - January 2003

Medical Research Council. Personal Information in Medical Research. October 2000. www.mrc.ac.uk

Responsibility in the use of Personal Medical Information for Research - Principles and Guide to Practice, Prepared for Council's standing Committee on the Use of Medical Information for research, 1985. Reprinted with minor revisions as footnotes, September 1994. To be revised 2001.

Human Tissue and Biological Samples for use in Research. Medical Research Council Ethics Series. Medical Research Council. April 2001.

미국 자료

USA. Department of Health & Human Services. Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule. NIH Publication Number 03-5388

USA. Department of Health & Human Services. HIPAA Privacy Rule. http://www.hhs.gov/ocr/hipaa.

담당 미연방 정부 기관

- Office for Civil Rights (OCR), Department of Health and Human Services (HHS)
  http://www.hhs.gov/ocr/hipaa
- Agency for Healthcare Research and Quality (AHRQ)
  http://www.ahrq.gov/
- Centers for Disease Control and Prevention (CDC)
  http://www.cdc.gov/nip/registry/hipaa7.htm
- Food and Drug Administration (FDA)
  http://www.fda.gov/
- Indian Health Services (IHS)
  http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm

◦ National Institutes of Health (NIH)
http://privacyruleandresearch.nih.gov/

◦ Office for Human Research Protections (OHRP), HHS
http://ohrp.osophs.dhhs.gov/

◦ Substance Abuse and Mental Health Services Administration (SAMHSA)
http://www.hipaa.samhsa.gov/

미연방정부 자료

◦ DHHS Office for Civil Rights - HIPAA guidelines
http://www.hhs.gov/ocr/hipaa

◦ CDC - Privacy Rule guidelines
http://www.cdc.gov/privacyrule

◦ Centers for Medicare and Medicaid Services
http://www.cms.gov/hipaa/
http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

◦ Health resources and Services Administration - HIPAA
http://www.hrsa.gov/website.htm

◦ National Center for Health Statistics
http://www.cdc.gov/nchs/otheract/phdsc/phdsc.htm

◦ National Committee on Vital and Health Statistics
http://www.ncvhs.hhs.gov/

◦ National Health Information Infrastructure
http://www.health.gov/ncvhs-nhii/
http://www.oft.state.ny.us/hipaa/index.htm

◦ Indian Health Service - HIPAA
http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm

◦ National Institutes of Health
http://privacyruleandresearch.nih.gov

◦ Substance Abuse and Mental Health Services Administration- HIPAA
http://www.smhsa.gov/hipaa/

미국 주정부 자료

California

http://www.dhs.ca.gov/hipaa/

http://www.ohi.ca.gov/state/calohi/ohiHome.jsp

http://www.dmh.ca.gov/hipaa/

Colorado

http://www.cdphe.state.co.us/HIPAA/

Florida

http://www.myflorida.com/myflorida/sto/hipaa/

Illinois

http://www.state.il.us/dpa/hipaa.html

Kentucky

http://chs.state.ky.us/dms/HIPAA/default.htm

http://dmhmrs.chr.state.ky.us/hipaa.asp

Maryland

http://www.mhcc.state.md.us/edi/hipaa/_hipaa.htm

http://dhmh.state.md.us/HIPAA/

Minnesota

http://www.dhs.state.mn.us/hipaa/

Missouri

http://www.health.state.mo.us/HIPAA/

New York

http://www.oft.state.ny.us/hipaa/index.htm

North Carolina

http://dirm.state.nc.us/hipaa/

Ohio

http://www.state.oh.us/hipaa/

Pennsylvania

http://www.dpw.state.pa.us/omap/hipaa/omaphipaa.asp

http://www.insurance.state.pa.us/html/hipaa.html

South Carolina

http://www.hipaa.state.sc.us/

Texas

http://www.hhsc.state.tx.us/NDIS/NDISTaskForce.html

Virginia

http://www.dmas.state.va.us/hpa-home.htm

Wisconsin

http://www.dhfs.state.wi.us/HIPAA/

수사와 범죄 예방 활동에서의 감시기술의 활용과 그에 대한 통제

이 은 우
(민주사회를 위한 변호사모임)

순 서

1. 서론 ……65
2. 범죄의 수사 및 예방 활동에 대한 법적 통제 ……65
3. 정보통신망에서의 감시활동과 그에 대한 통제 ……71
4. 수사 또는 범죄 예방 활동의 수단으로 CCTV의 활용 ……84
5. 결론 ……88

수사와 범죄 예방 활동에서의 감시기술의 활용과 그에 대한 통제

이 은 우
(민주사회를 위한 변호사모임)

1. 서론

CCTV 감시, 위치정보의 파악, 유전자 검사, 컴퓨터 이용현황에 대한 로그기록의 분석 등 최근 감시기술은 눈부시게 발전하고 있다. 이러한 감시기술이 발전하게 된 요인으로는 정보의 가치가 높아지면서 정보수집의 요구가 높아지고, 정보처리기술이 발전하게 되었기 때문이다. 수사기관은 끊임없이 새로운 감시기술을 수사 및 범죄 예방 활동에 활용하고자 한다. 이하에서는 최근 감시기술의 발달과 더불어 문제가 되는 분야에 대한 감시기술의 활용과 그에 대한 통제방안을 검토하고자 한다.

2. 범죄의 수사 및 예방 활동에 대한 법적 통제

가. 강제수사 법정주의와 영장주의

수사란 범죄의 혐의 유무를 명백히 하여 공소의 제기와 유지 여부를 결정하기 위하여 범인을 발견, 확보하고 증거를 수집, 보전하는 수사기관의 활동을 말한다.[1] 수사는 인권과 밀접한 관계를 가지고 있는 절차이기 때문에, 수사기관의 재량에 의하여 수사를 하도록 방치해서는 안된다[2]. 수사는 구체적 사실에 근거한 범죄의 혐의가 있는 있는 경우[3]에만 허용되며, 그 목적을 달성하기 위한 필요 최소한에 그쳐야 한다[4].

1) 이재상. 형사소송법 169 페이지.
2) 위 책 175 페이지
3) 위 책 175 페이지
4) 위 책 177 페이지

그래서 우리 형사소송법은 강제수사의 경우에는 형사소송법에 특별한 규정이 있는 경우에만, 필요한 최소한도의 범위 내에서 법에서 정하고 있는 절차에 의하여만 할 수 있다는 규정을 두고 있다(형사소송법 제199조 제1항[5]). 우리 형사소송법은 강제수사의 방법으로 압수, 수색, 검증, 체포, 구속, 감정유치 등을 규정하고 있다. 압수란 물건의 점유를 취득하는 강제처분이며,[6] 수색은 압수할 물건이나 체포할 사람을 발견할 목적으로 주거나 물건 또는 사람의 신체 또는 기타 장소에 대하여 행하는 강제처분을 말하며,[7] 검증이란 사람, 장소, 물건의 성질·형상을 오관의 작용에 의하여 인식하는 강제처분을 말한다[8]. 그리고 체포란 사람을 단시간 동안 일정한 장소에 인치하는 것을 말하며,[9] 구속이란 사람의 신체의 자유를 장기간에 걸쳐 제한하는 강제처분을 말하고[10], 감정유치란 정신 또는 신체의 감정을 위하여 일정한 기간 동안 병원 또는 기타 적당한 장소에 피고인 또는 피의자를 유치하는 강제처분을 말한다[11]. 따라서 이러한 유형의 강제처분이 아닌 강제수사는 허용될 수 없다. 그러나 현재 통신비밀보호법은 통신의 검열과 감청을 통신제한조치라고 하여 인정하고 있다.

그리고 이러한 강제수사는 원칙적으로 법원 또는 법관이 발부한 적법한 사전 영장에 의하여야 한다(형사소송법 제215조, 제221조의 4). 또한 영장은 범죄의 혐의가 충분히 인정되는 경우로서, 필요성이 인정되는 경우에만 발부될 수 있다(형사소송법 제201조, 제215조). 이를 영장주의라고 한다.

한편 긴급한 상황에서 부득이한 경우에는 사전 영장주의에 대한 예외가 인정되기도 한다. 그러나 이 경우에도 적법한 체포·구속영장을 발부 받았거나, 즉시 사후 영장을 발부 받아야 한다. 즉, 현행범인의 체포(형사소송법 제211조, 제212조)나 긴급체포시에는 체포영장 없는 체포가 허용되나(형사소송법 제200조의 3), 즉시 사후 영장을 발부 받지 않으면 석방하여야 하며, 체포·구속시에 체포·구속을 목적으로 한 피의자 수색시에는 수색영장 없는 수색이 허용되나 이 경우에는 체포나 구속 영장을 발부 받았어야 한다. 구속·체포 현장에서의 압수·수색·검증, 피고인 구속현장에서의 압수·수

---

5) 형사소송법 제199조
① 수사에 관하여는 그 목적을 달성하기 위하여 필요한 조사를 할 수 있다. 다만, 강제처분은 이 법률에 특별한 규정이 있는 경우에 한하며, 필요한 최소한도의 범위 안에서만 하여야 한다.
6) 이재상 273 페이지
7) 위의 책 273 페이지
8) 위의 책 285 페이지
9) 위의 책 215 페이지
10) 위의 책 225 페이지
11) 위의 책 287 페이지

색・검증(형사소송법 제216조), 긴급체포시의 압수・수색・검증(형사소송법 제217조 제1항)의 경우도 마찬가지이다. 범죄장소에서의 압수・수색・검증(형사소송법 제216조)시에는 즉시 사후 영장을 발부 받아야 한다.

한편 형사소송법은 수사에 관하여는 공무소 기타 공사단체에 조회하여 필요한 사항의 보고를 요구할 수 있다(제199조 제2항)는 규정을 두고 있다. 이에 의하면 수사기관은 공무소나 공사단체에 수사에 필요한 사항을 특별한 절차나 허가없이도 보고하도록 요구할 수 있는 것으로 해석될 소지도 있다. 그러나 이 규정은 같은 조 제1항에서 강제처분 법정주의를 채택하고 있는 취지에 비추어 당해 보고가 특정인의 프라이버시나 기타 기본권을 침해하지 않는 경우(예를 들어 특정일의 일몰시간, 특정시점의 환율 등)로 국한하여 해석해야 할 것이다.

나. 경찰관의 범죄예방 및 공공질서 유지활동과 법적 통제

한편 경찰은 범죄의 예방과 공공의 질서유지 등의 업무를 수행하게 되는데, 이러한 경찰의 범죄 예방 활동과 공공질서 유지활동도 법률의 규정에 의하여 정해진 요건과 절차를 준수해야 한다.

현재 경찰관의 범죄 예방 활동과 공공질서 유지활동의 근거법으로 경찰관직무집행법이 제정되어 시행되고 있다. 이 법에 의하면 경찰관의 범죄 예방 활동과 공공질서 유지활동은 수상한 거동 기타 주위의 사정을 합리적으로 판단하여 어떠한 죄를 범하였거나 범하려 하고 있다고 의심할 만한 상당한 이유가 있는 자 또는 이미 행하여진 범죄나 행하여지려고 하는 범죄행위에 관하여 그 사실을 안다고 인정되는 자에 대하여 질문을 하거나 흉기의 소지여부를 조사할 수 있다. 이 때에는 경찰관은 상대방의 의사에 반하여 답변을 강요할 수 없다.[12)]

---

12) 제3조 (불심검문)
① 경찰관은 수상한 거동 기타 주위의 사정을 합리적으로 판단하여 어떠한 죄를 범하였거나 범하려 하고 있다고 의심할 만한 상당한 이유가 있는 자또는 이미 행하여진 범죄나 행하여지려고 하는 범죄행위에 관하여 그 사실을 안다고 인정되는 자를 정지시켜 질문할 수 있다.
② 그 장소에서 제1항의 질문을 하는 것이 당해인에게 불리하거나 교통의 방해가 된다고 인정되는 때에는 질문하기 위하여 부근의 경찰서 · 지서 · 파출소 또는 출장소(이하 "경찰관서"라 하되, 지방해양경찰관서를 포함한다)에 동행할 것을 요구할 수 있다.이 경우 당해인은 경찰관의 동행요구를 거절할 수 있다. <개정 88.12.31, 96.8.8>
③ 경찰관은 제1항에 규정된 자에 대하여 질문을 할 때에 흉기의 소지여부를 조사할 수 있다.
④ 제1항 또는 제2항의 규정에 의하여 질문하거나 동행을 요구할 경우 경찰관은 당해인에게 자신의 신분을 표시하는 증표를 제시하면서 소속과 성명을 밝히고 그 목적과 이유를 설명하여야 하며, 동행의 경우에는

다. 새로운 감시기술의 수사활동에서의 활용과 그에 대한 통제

감시기술의 발달로 인하여 수사기법은 나날이 새로워지고 있다. 이처럼 발전하는 수사기법을 범죄수사나 범죄예방 활동에 활용한다면, 과학수사가 이루어져 범죄 검거율을 높이거나, 피고인의 자백에 의존하는 전근대적인 수사관행에서 탈피하여 수사과정에서 고문이나 가혹행위가 자행되는 것을 줄일 수도 있을 것이다. 그러나 이러한 감시기술의 활용은 다른 한편으로는 지나친 인권침해로 이어질 가능성이 높으며, 수사권이 남용될 가능성도 배제할 수 없다. 새로운 감시기술에 대해서는 적절한 범위 내에서의 활용과 그에 대한 법적인 통제가 따라야 할 것이다.

또한 새로운 기술이 수사에 활용될 경우에는 법적인 통제 뿐만 아니라 기술에 대하여 입법부나 법원이 완전한 이해를 하고, 통제를 하고 있어야 한다. 알려지지 않은 성능이 있을 경우, 강제처분의 일환으로 이루어지는 감시행위에 대한 통제가 불가능하기 때문이다.

(1) 강제수사 법정주의와 영장주의의 관철

이를 위하여 무엇보다도 먼저 새로운 감시기술은 강제수사 법정주의와 영장주의라는

동행장소를 밝혀야 한다. <개정 91.3.8>

⑤ 제2항의 규정에 의하여 동행을 한 경우 경찰관은 당해인의 가족 또는 친지등에게 동행한 경찰관의 신분, 동행장소, 동행목적과 이유를 고지하거나 본인으로 하여금 즉시 연락할 수 있는 기회를 부여하여야 하며, 변호인의 조력을 받을 권리가 있음을 고지하여야 한다. <신설 88.12.31>

⑥ 제2항의 규정에 의하여 동행을 한 경우 경찰관은 당해인을 6시간을 초과하여 경찰관서에 머물게 할 수 없다. <신설 88.12.31, 91.3.8>

⑦ 제1항 내지 제3항의 경우에 당해인은 형사소송에 관한 법률에 의하지 아니하고는 신체를 구속당하지 아니하며, 그 의사에 반하여 답변을 강요당하지 아니한다. <신설 88.12.31>

제6조 (범죄의 예방과 제지)

① 경찰관은 범죄행위가 목전에 행하여지려고 하고 있다고 인정될 때에는 이를 예방하기 위하여 관계인에게 필요한 경고를 발하고, 그 행위로 인하여 인명 · 신체에 위해를 미치거나 재산에 중대한 손해를 끼칠 우려가 있어 긴급을 요하는 경우에는 그 행위를 제지할 수 있다.

② 삭제 <88.12.31>

제10조 (경찰장비의 사용등)

① 경찰관은 직무수행중 경찰장비를 사용할 수 있다. 다만, 인명 또는 신체에 위해를 가할 수 있는 경찰장비에 대하여는 필요한 안전교육과 안전검사를 실시하여야 한다.

② 제1항의 "경찰장비"라 함은 무기, 경찰장구, 최루제 및 그 발사장치, 감지기구, 해안감시기구, 통신기기, 차량 · 선박 · 항공기등 경찰의 직무수행을 위하여 필요한 장치와 기구를 말한다.

③ 경찰장비를 임의로 개조하거나 임의의 장비를 부착하여 통상의 용법과 달리 사용함으로써 타인의 생명 · 신체에 위해를 주어서는 아니된다.

④ 제1항 단서의 경찰장비의 종류 및 그 사용기준, 안전교육 · 안전검사의 기준등에 대하여는 대통령령으로 정한다. [본조신설 99.5.24]

대원칙에 입각하여 통제되어야 한다. 즉, 새로운 감시기술의 활용이 형사소송법이 예정하고 있지 않은 것이라면, 허용되어서는 안될 것이며, 형사소송법이 예정하고 있는 범위 내의 것이라면 사전 영장주의에 의하여 통제되어야 할 것이다.

따라서 형사소송법에 규정이 없는 강제수사나 영장없는 강제수사는 위법하며, 위법한 수사에 의하여 확보한 증거물은 증거능력이 부정되어야 한다. 예컨대 CCTV의 촬영이나, 비디오 촬영, 투시장치를 통한 투시촬영, 위성에 의한 사진촬영, 위치추적 장치를 통한 위치추적, 홍채인식이나 정맥인식 등은 일종의 검증으로 볼 수 있을 것이므로 영장주의가 적용되어야 할 것인데, 그 인정여부, 인정시의 허용범위 등은 아래와 같은 점을 고려하여야 할 것이다.

⑵ 기술에 대한 완전한 통제

새로운 기술이 수사에 활용될 경우에는 기술에 대하여 입법부나 법원이 완전한 이해를 하고, 통제를 하고 있어야 한다. 따라서 해당 감시기술의 모든 성능과 기술의 확장가능성, 오용가능성 등까지 그 일체의 내용이 알려지고, 평가되어 있어야 한다. 이러한 평가가 불충분한 경우로서 위험성이 내포되어 있는 때에는 해당 감시기술은 활용하지 말아야 한다.

⑶ 기본권 침해의 정도

해당 감시를 허용할 경우의 기본권 침해의 정도가 고려되어야 한다. 그래서 기본권 침해의 정도가 큰 경우에는 해당 기술의 활용이 허용되어서는 안될 것이다. 예컨대 고도의 수준의 위치정보 - 부가서비스로서의 위치정보 -의 경우에는 사생활의 비밀의 침해의 정도가 너무나도 크기 때문에 이를 수사에 활용하는 것보다는 활용되지 못하도록 막는 것이 좋을 것이다. 그리고 지나치게 정밀한 감시장치의 경우에도 활용을 못하도록 하는 것이 좋을 경우가 많을 것이다. 따라서 특히 새로운 감시기술은 그것이 수사기관에 의하여 수사의 기법으로 활용될 경우 그로 인한 기본권의 침해의 정도가 어떤지가 미리 충분히 조사, 평가되어 있어야 한다.

⑷ 대체할 방법이 없는지

감시로 인한 기본권 침해의 효과가 큰 감시방법의 경우에는 해당 감시방법의 활용이

해당 범죄에 대한 수사를 할 때 반드시 필요하며, 다른 대체할 방법이 없으며, 다른 범죄수사 방법을 시도했으나 실패한 경우에만 허용될 수 있을 것이다.

⑸ 필요 최소한의 허용

그리고 필요성이 인정되어 만약 허용한다고 하더라도 형사소송법은 강제수사는 필요한 최소한의 범위 내에서만 인정되어야 한다고 하여 강제수사를 허용할 경우에 발생할 수 있는 인권침해의 위험을 최소화하려고 하고 있는바, 최소한의 범위 내에서만 허용되어야 할 것이다.

라. 우리 대법원의 태도

그런데 우리 대법원은 법원의 영장을 발부받지 않은 CCTV의 촬영 행위나 비디오 촬영 행위에 대하여 현재 범죄가 행해지고 있고(현행성), 긴급하게 증거보전을 할 필요가 있으며(긴급성), 일반적으로 허용되는 한도를 넘지 않는 상당한 방법에 의한 것(상당성)이라면 위법하다고 볼 수 없다고 판시하여, CCTV의 촬영이나, 비디오 촬영에 영장주의가 적용되지 않는다고 보고 있다.

즉, 우리 대법원은 경찰이 무인장비(폐쇄회로 텔레비전, CCTV)를 설치해 놓고, 제한속도를 위반하는 차량의 사진을 촬영한 경우에 그 하는 행위에 대하여, 범죄가 현재 행해지고 있고, 긴급하게 증거보전을 할 필요가 있으며, 일반적으로 허용되는 한도를 넘지 않는 상당한 방법에 의한 것이므로 (인용자 첨가 : 법적인 근거가 없고, 법원에 의한 영장을 발부받지 않았지만) 적법하다고 보았으며[13], 영장없이 몰래 비디오로 범죄현장을 촬영한 행위를 위법하다고 단정할 수가 없다고 보았다[14].

---

13) 대법원 1999. 12. 7. 선고 98도3329 판결.
수사, 즉 범죄혐의의 유무를 명백히 하여 공소를 제기·유지할 것인가의 여부를 결정하기 위하여 범인을 발견·확보하고 증거를 수집·보전하는 수사기관의 활동은 수사 목적을 달성함에 필요한 경우에 한하여 사회통념상 상당하다고 인정되는 방법 등에 의하여 수행되어야 하는 것인바, 무인장비에 의한 제한속도 위반차량 단속은 이러한 수사활동의 일환으로서 도로에서의 위험을 방지하고 교통의 안전과 원활한 소통을 확보하기 위하여 도로교통법령에 따라 정해진 제한속도를 위반하여 차량을 주행하는 범죄가 현재 행하여지고 있고, 그 범죄의 성질·태양으로 보아 긴급하게 증거보전을 할 필요가 있는 상태에서 일반적으로 허용되는 한도를 넘지 않는 상당한 방법에 의한 것이라고 판단되므로, 이를 통하여 운전 차량의 차량번호 등을 촬영한 사진을 두고 위법하게 수집된 증거로서 증거능력이 없다고 말할 수 없다.

14) 대법원 1999. 9. 3. 선고 99도2317 판결
누구든지 자기의 얼굴 기타 모습을 함부로 촬영당하지 않을 자유를 가지나 이러한 자유도 국가권력의 행사로부터 무제한으로 보호되는 것은 아니고 국가의 안전보장·질서유지·공공복리를 위하여 필요한 경우

이러한 대법원의 태도는 비록 (i) 범죄가 벌어지고 있는 경우로서 (ii) 증거수집을 위한 긴급한 필요가 있고, (iii) 상당한 방법에 의한 경우라는 제한을 두고 있기는 하지만, 이러한 경우에는 비록 강제수사라 할지라도 사전은 물론 사후라도 영장을 발부받지 않아도 된다는 것이어서 형사소송법의 규정에 정면으로 반하는 문제점이 있다. 교통관련 단속을 위한 CCTV의 촬영의 경우에는 일반적인 영장주의를 적용하게 되면 지나치게 번거로와지는 문제가 있고, CCTV의 촬영으로 인한 기본권 침해의 정도도 크지 않으므로 이 경우는 별도의 법률 규정을 두는 것이 좋을 것이지만, 비디오 촬영의 경우는 사실상 대화를 녹음하는 것과 동일한 기본권 침해의 효과가 있는데, 통신비밀보호법에서 대화의 녹음시에는 영장을 발부받아야 한다고 규정하고 있는 취지에 비추어, 영장주의를 엄격하게 적용해야 한다. 그 외에도 감시기술을 활용한 수사에 대해서는 엄격하게 영장주의가 적용되어야 한다.

3. 정보통신망에서의 감시활동과 그에 대한 통제

가. 정보통신망의 발달

최근 인터넷을 비롯한 정보통신망의 발달로 인하여, 과거의 우편이나 전화를 이용하여 통신이 이루어지던 시대에 비하여 통신의 양과 질이 비약적으로 확장되게 되었다. 인터넷을 통한 전자우편, 채팅, 메신저를 이용한 통신은 물론, 전자게시판은 물론 홈페이지를 통한 통신, 무선인터넷, 이동전화를 통한 통신, 이동전화의 문자메시지 등 그 수단이 다양해지고, 양도 대폭 늘어났으며, 통신의 방법도 문자, 소리, 영상 등 다양해지고 있다.

에는 상당한 제한이 따르는 것이고, 수사기관이 범죄를 수사함에 있어 현재 범행이 행하여지고 있거나 행하여진 직후이고, 증거보전의 필요성 및 긴급성이 있으며, 일반적으로 허용되는 상당한 방법에 의하여 촬영을 한 경우라면 위 촬영이 영장 없이 이루어졌다 하여 이를 위법하다고 단정할 수 없다. 이 사건 비디오촬영은 피고인들에 대한 범죄의 혐의가 상당히 포착된 상태에서 그 회합의 증거를 보전하기 위한 필요에서 이루어진 것이고 박경순의 주거지 외부에서 담장 밖 및 2층 계단을 통하여 OOO의 집에 출입하는 피고인들의 모습을 촬영한 것으로 그 촬영방법 또한 반드시 상당성이 결여된 것이라고는 할 수 없다 할 것인바, 위와 같은 사정 아래서 원심이 이 사건 비디오 촬영행위가 위법하지 않다고 판단하고 그로 인하여 취득한 비디오테이프의 증거능력을 인정한 것은 정당하고 거기에 영장 없이 촬영한 비디오테이프의 증거능력에 관한 해석을 그르친 잘못이 있다고 할 수 없다

기술의 발달과 정보통신망의 특징으로 인하여 통신의 즉시성이 사라지고, 저장성이 증대하고 있다. 전화의 경우에도 과거에는 요금의 산정을 위한 발신번호, 수신번호, 통화시간 정도가 저장되는 기록이었으나, 최근에는 통화위치[15]까지 저장되고 있다. 그리고 문자메시지의 경우는 메시지의 수신자 뿐만 아니라 내용까지도 저장될 수 있다. 인터넷을 통한 통신의 경우는 수신자와 발신자에 대한 기록은 물론, 접속위치, 통신의 모든 내용이 저장되어진다. 특히 문자메시지나 인터넷의 통신의 경우 수신자나 발신자가 자신의 컴퓨터에서 통신의 내용을 삭제하더라도 서버에는 그 내용이 남아있게 되며, 로그기록은 당사자가 그것이 저장되는지를 모르는 경우가 많다.

이렇게 저장된 정보는 매우 쉽게 검색될 수 있다. 심지어는 마음만 먹으면 인터넷을 통하여 유통되는 모든 통신을 실시간으로 검색할 수도 있다. 그리고 검색을 하더라도 당사자에게 알리지 않는 이상 당사자는 검색을 했는지 여부를 알 수 없다.

특히 인터넷을 통한 통신의 경우에는 그것이 공개적인 것인지, 비공개적인 것인지를 구별하는 것이 쉽지 않다. 전자우편이나 메신저 등을 통한 통신의 경우에는 비공개적인 것임이 분명하지만, 채팅방에서의 통신이나, 전자게시판을 통한 통신, 커뮤니티에서의 통신 등은 그것이 공개적인 것인지, 비공개적인 것인지를 판단하기가 쉽지 않다. 그러나 인터넷에서의 통신이 특정인을 전제로 하는 것이거나, 익명성을 전제로 한 것일 경우에는 특정인의 범위를 벗어나는 자에 대하여는 비공개성을 띤 것이고, 익명성을 침해하는 경우에는 통신의 비밀을 침해하는 것으로 보아야 할 것이다.

나. 정보통신망 또는 통신망에서의 감시기술과 감시활동

(1) 전자우편의 검열

1:1 또는 1:다, 또는 다:1, 다:다의 통신수단인 전자우편의 검열은 기존의 우편물의 검열과 달리 다양한 방법으로 손쉽게, 그러나 상대방은 전혀 모르는 상태에서 이루어질 수 있다. 수신자의 컴퓨터에 다운로드를 받아 놓은 전자우편을 검열할 수도 있고, 전자우편 서버를 제공하는 자를 통하여 검열할 수도 있고, 그 보다도 상위 단계에서도 전자우편의 검열이 가능하다. 검열의 수준도 발신자의 주소만을 검열할 수도 있고, 제목만을 검열할 수도 있고, 내용까지도 검열할 수도 있다.

15) 통화위치를 통신회사가 고객의 동의없이 저장기록하고 있는 것이 고객에게 서비스 제공을 위하여 불가피한 것으로 보기는 어렵다고 생각한다. 따라서 이는 위법한 것으로 판단된다.

전자우편과 유사한 것으로 메신저를 통한 통신의 내용이나, 채팅방에서의 채팅내용 등이 있을 수 있다.

⑵ 게시판의 글

게시판이나 동호회의 자료실 등에 남긴 글을 검열할 수도 있다. 이러한 게시판, 채팅룸, 동호회에서 남긴 글은 수신자나 참여자의 범위가 제한이 없는 것인지, 아니면 제한되어 있는 것인지, 누구에게나 볼 수 있도록 남긴 것인지 아니면 특정인만 볼 수 있도록 남긴 것인지에 따라 구분될 수 있으며, 자신의 실명을 밝힌 것인지 익명을 사용한 것인지에 따라 구분될 수도 있다.

⑶ 인터넷 이용현황

인터넷 이용현황도 검열할 수 있다. 스파이웨어 프로그램을 통하여 검열할 수도 있고, 당사자가 남기도록 업체에 승낙을 하여 업체가 축적해 놓은 현황자료를 제공받는 방식으로 검열할 수도 있다.

⑷ 통화기록 등의 검열

가입자의 전기통신일시, 전기통신개시, 종료시간, 발, 착신 통신번호, 상대방의 가입자번호, 사용도수 등의 통화기록도 검열이 가능하다.

⑸ 위치정보의 파악

컴퓨터의 접속위치 정보, 핸드폰의 접속지 정보 등의 과거의 정보와 실시간으로 파악되는 현재의 위치정보가 있을 수 있다.

다. 정보통신망에서의 감시활동에 대한 통제

⑴ 영장주의의 엄격한 적용의 필요성

정보통신망에서의 수사나 범죄 예방 활동 중에서 통신의 당사자의 통신의 비밀과 자유를 침해하는 것에 대해서는 엄격한 영장주의가 적용되어야 할 것이다. 특히 통신제한

조치는 비록 법원의 영장에 의하여 제한적으로 허용되다 하더라도, 당사자가 감청이나 검열당하고 있다는 사실 그 자체를 전혀 모르고 있는 상태에서 이루어지는 것이기 때문에 개인의 사생활이 침해될 우려가 매우 높다. 그리고 헌법상 영장주의가 의미하는 특정성, 공개성, 영장제시와는 달리 감청이나 검열은 일반성, 비밀처분성, 영장제시의 결여라는 특성으로 인하여 사실상 헌법상 영장주의에 대한 예외적인 절차이기 때문에 그 적용이나 실행은 매우 한정적, 특정적이어야 한다. 나아가서 사회공공의 안녕질서 유지라는 공익적 목적을 달성하기 위하여 희생되어야 하는 개인의 사생활 침해가 최소한에 그치도록 운영되어야 한다[16].

⑵ 영장주의의 적용범위

강제처분 법정주의와 강제처분에 대한 영장주의를 취하고 있는 현행 헌법과 형사소송법의 규정의 취지에 비추어 본다면, 기본권을 침해할 소지가 있는 모든 것에 영장주의가 적용되어야 한다. 따라서 전자우편, 게시판의 글, 인터넷 이용기록, 통신사실, 위치정보 등에 모두 영장주의가 적용되어야 한다.

다만, 예컨대 공개게시판에 올린 글이나, 공개 채팅룸에 공개한 대화처럼 당사자가 공개를 전제로 한 통신의 경우에는 이를 검열하여도 통신의 비밀이나 자유가 침해되지 않을 것이므로 이 경우에는 영장주의를 적용할 필요는 없을 것이다. 그러나 특정한 그룹 내에서의 통신의 경우(예를 들어 인터넷상에서의 메일링리스트 서비스나 이동전화의 문자메시지나 전화의 그룹전송 서비스의 경우)에도 해당 그룹의 수신자 이외의 자에 의한 통신비밀의 침해는 엄격히 금지되어야 하며, 그에 대한 감청은 법원의 영장에 의해서만 허용될 수 있다. 우리 법은 당사자의 동의를 받지 않은 감청을 금지하고 있는데, 당사자란 통신의 수신자와 발신자를 모두 포함하기 때문이다. 한편 불특정다수인에게 공개된 곳에 올린 글이라 하더라도 당사자가 익명을 사용한 경우에는 글쓴이의 본명을 추적하는 행위는 법원의 통신제한조치에 대한 영장에 의해서만 허용되어야 할 것이다.

통신의 비밀에는 통신의 내용 뿐만 아니라 통신의 상대방, 통신의 시간, 장소 등도 포함된다. 따라서 통신의 상대방, 통신의 시간, 장소 등에 대한 자료를 공개할 경우에도 원칙적으로 영장주의가 적용되어야 할 것이다. 물론 통신의 내용에 대한 정보에 비하여 영장주의가 적용되는 정도는 완화될 수 있을 것이다.

---

16) 통신비밀보호법상 감청제도의 문제점, 성낙인, 시민과 변호사 1999. 7. 96p.

⑶ 통신사실확인자료에 대한 영장주의 배제규정의 문제점

그런데 현행법은 검사 또는 사법경찰관은 검사장의 승인을 얻거나 긴급한 경우에는 사후승인을 얻어서 가입자의 전기통신일시, 전기통신개시, 종료시간, 발, 착신 통신번호 등 상대방의 가입자번호, 사용도수, 그 밖에 대통령령으로 정하는 전기통신사실에 관한 자료(한편 시행령 제3조의 2는 1. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, 2. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치 추적자료, 3. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료를 추가하고 있다)를 통신사실확인자료라고 하여 수사 또는 형의 집행을 위하여 필요한 경우 열람이나 제출을 요청할 수 있다고 규정하고 있다. 심지어는 서면으로 통신사실확인자료제공을 요청할 수 없는 긴급한 사유가 있는 경우에는 사후에 통신사실확인자료 요청서를 제출해도 된다고 하고 있다.

앞서도 보았듯이 통신의 비밀에는 통신의 내용 뿐만 아니라 통신의 상대방, 통신의 시간, 장소 등도 포함된다. 따라서 통신의 상대방, 통신의 시간, 장소 등에 대한 자료를 공개할 경우에도 원칙적으로 영장주의가 적용되어야 할 것이다. 물론 통신의 상대방에 대한 정보에 비하여 영장주의가 적용되는 정도는 완화될 수 있을 것이다. 그러나 대통령령에 규정된 통신사실확인자료(컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치 추적자료, 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료)의 경우는 인터넷에 익명으로 올린 글의 발신자를 확인할 수 있는 자료로서 통신의 내용의 비밀을 직접 침해하는 것으로서 상위법률의 위임범위를 넘는 것이기도 하고, 엄격하게 영장주의가 적용되어야 할 것들이다. 그러나 현행법은 이러한 것들을 모두 법원의 관여없이 검사장의 승인만을 얻어서 열람하거나 제출을 요청할 수 있게 하고 있어서 통신의 비밀을 침해하고 있다.

현행법은 통신사실확인자료 요청의 요건을 수사 또는 형의 집행을 위하여 필요한 경우 열람이나 제출을 요청할 수 있도록 하고 있다. 그리고 이 경우 요청사유, 해당가입자와의 연관성, 필요한 자료의 범위를 기재한 서면이나 긴급한 경우에는 사후에 서면을 제출함으로써 가능하도록 하고 있다(법 제13조 제4항). 통신사실확인자료의 경우에도 엄격하게 범죄혐의를 기재하고 소명하도록 하여야 할 것이다.

전화, 인터넷 통신을 포함한 모든 통신서비스에 적용되는 유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 1997. 12. 15. 지침(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)에서는 통신서비스 가입자나 통신서비스 이용자의 통신서비스 이용정보(traffic data)는 통신이 통신이 끝나면 삭제되거나 익명화되어야 한다고 규정하고 있다. 단, 가입자에 대하여 요금청구를 하거나 상호접속 요금의 지급을 위하여 가입자의 전화국의 번호나 식별정보, 가입자의 주소, 해당 요금부과 기간동안의 요금부과 대상 총 통화수, 걸려온 가입자의 전화번호, 유형과 시작시간과 지속시간 또는 전송된 데이터의 양, 전화나 서비스의 일자를 요금이 수금될 때까지 보관할 수 있다고 한다. 그리고 이용정보나 요금청구에 관련한 정보는 해당 업무를 처리하는 사람이나 고객의 질의에 답하는 사람, 사기행위를 감시하거나 분쟁해결을 위하여 법적으로 허용되는 경우에만 접근 가능하도록 하고 있다[17].

⑷ 통신제한조치의 허용 요건의 강화

현행법은 통신제한조치의 대상범죄를 광범위하게 규정하고 있는데, 통신제한조치는 최소화해야 할 수사방법이라는 점에서 대상범죄를 대폭축소할 필요가 있다. 예컨대 뉴질랜드의 경우는 마약범죄와 조직범죄와 중대한 폭력범죄로 국한하고 있으며[18], 오스트리아는 전화도청의 경우에는 1년 이상의 징역에 처해질 범죄에 대해서만, 전자통신의 도청에 대해서는 조직범죄나 10년 이상의 징역에 처해질 범죄에 대해서만 허용하고 있으며[19], 이탈리아의 경우에는 5년 이상의 징역에 처해질 범죄에 대해서만 도청을 허용하며[20], 룩셈부르크의 경우에는 2년 이상의 징역에 처해질 범죄에 대해서만 도청을 허용하며[21], 일본의 경우에는 총기, 약물, 밀입국, 조직적인 살인과 관련된 조직범죄의 수사를 위해 도청이 허용된다고 한다[22].

---

17) 유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 1997. 12. 15. 지침 (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector) Aricle 6.

18) 뉴질랜드 Law Commission Study Paper 12, Electronic Technology and Police Investigations Some Issues, 1페이지. the Misuse of Frugs Amendment Act 1978, the Crime Amendment Act (No 2) 1987, 1997.

19) Privacy and Humanrights 2002, 117 페이지. §149a - 149p Strafprozessordnung - StPO.

20) Privacy and Humanrights 2002, 232 페이지, Penal Procedure Code article 266-271.

21) Privacy and Humanrights 2002, 262 페이지, Criminal Code Art 88-1 - 88-4.

현행법은 도청의 허용기간을 2개월로 하고 있는데, 오늘날 통신의 빈도나 통신에의 의존도 등을 고려할 때, 2개월 동안의 통신제한조치 기간동안 당사자는 수사와 관련이 없는 통신의 비밀을 당사자가 알지도 못하는 상태에서 침해당할 것인바, 2개월 동안 비밀성을 갖는 일반영장을 부여하는 것은 지나치게 길다고 보지 않을 수 없다. 30일로 줄이거나 그보다 더 짧은 기간으로 줄여야 할 것이다.

⑸ 국가안보를 위한 통신제한조치

현행법은 정보수사기관의 장은 국가안전보장에 대한 상당한 위험이 예상되는 경우에 한하여 그 위해를 방지하기 위하여 이에 관한 정보수집이 특히 필요한 때에는 통신의 일방 또는 쌍방당사자가 내국인인 경우에는 고등법원 수석부장판사의 허가를 받아서, 외국인인 경우에는 대통령의 승인을 얻어 통신제한조치를 할 수 있다고 규정하고 있다.

이 규정은 '국가안전보장', '상당한 위험', '위해방지', '정보수집' 등 매우 추상적인 표현으로 이루어져 있어서 남용될 가능성이 높다. 대상범죄나, 적용되는 경우를 쉽게 예측할 수 있도록 표현을 보다 구체화해야 할 것이다.

그리고 외국인인 경우에는 법원의 영장을 발부받지 않고 대통령의 승인을 얻도록 하고 있는 것도 남용의 소지가 있다. 법원의 관여가 인정되어야 한다.

⑹ 긴급통신제한조치를 폐지해야 한다.

현행법은 법원에 대하여 통신제한조치의 허가를 신청할 수 없는 긴급한 사유가 있는 때에는 법원의 허가없이 통신제한조치를 할 수 있다고 규정하고 있다(법 제8조). 앞서 보았듯이 통신제한조치는 개인의 사생활 침해가 매우 큰 수사방법으로 최후의 수단으로 인정되는 것이다. 통신제한조치는 사실상 영장주의에 대한 예외인 셈이다. 이처럼 영장주의의 예외에 해당하는 통신제한조치를 법원의 사전허가 없는 긴급통신제한조치로까지 확장하는 것은 예외에 대한 예외로서 인권침해의 소지가 지나치게 커지므로 허용되어서는 안된다. 긴급통신제한조치는 폐지되어야 한다. 아니면 차선책으로는 야간당직영장제도를 도입하여 긴급한 상황에서 야간에 영장을 발부받도록 할 수도 있을 것이다[23].

---

22) Privacy and Humanright 2002, 237 페이지. 통신도청법에 반대하는 웹사이트(http://www.geocities.co.jp/Milkyway/8332/what.html)

23) 현재 미국의 경우 야간당직 영장제도를 활용하고 있다.

(7) 통신제한조치의 절차상의 요건과 집행결과의 봉인

법원에서 영장을 발부 받기 위하여는 전자감시의 목적이 되는 통신수단 등이 특정하고 심각한 범죄에 사용되고 있다는 것을 보여주는 다음과 같은 요건이 갖추어져야 한다. (i) 다른 수사기법을 시도하였거나 실패하였고, 또는 실패할 가능성이 높거나 너무 위험한 경우라야 한다. (ii) 전자감시에 필요한 기간이 명시되어야 한다. (iii) 동일 인물에 대하여 이전에 행하였던 전자감시를 명시하여야 한다. (iv) 전자감시를 연장하기 위한 영장청구서에는 이전에 행한 전자감시로 인하여 얻은 결과물이 있어야 한다.

영장발부는 판사 중 전자감시에 관하여 특수한 교육을 받은 사람만이 전자감시를 허가하는 영장발부를 할 수 있도록 하여야 할 것이다. 이때 영장이 발부되기 위해서는 다음과 같은 요건이 충족되어야 한다. (i) 전자감시의 대상이 되는 자가 범죄를 행하고 있거나, 급박하게 행할 상당한 이유가 있어야 한다. (ii) 전자감시를 통하여 범죄와 관련이 있는 특정 정보를 취득할 수 있는 상당한 이유가 있어야 한다. (iii) 일반적인 수사기법이 이미 시도되어 실패하였거나 혹은 성공할 가능성이 없거나 너무 위험한 경우라야 한다. (iv) 전자감시의 대상이 되는 특정 통신수단이 범죄에 사용되었거나 막 사용되려고 하거나, 그 범죄와 관련하여 감시대상자에 의하여 보통 사용되고 있는 상당한 이유가 있어야 한다.

영장집행의 단계에서는 수사기관은 감청도구를 작동시키지 않았다가 수분 간격으로 이를 작동시키는 등 범죄와 관련이 없는 대화, 특히 가족생활 등 사생활에 관한 이야기를 감청 대상에서 제외시킴으로써 사생활침해를 최소화하여야 할 것이다. 이렇게 최소화 되지 않은 전자감시결과는 그 증거능력이 부정되어야 할 것이다.

한편 전자감시의 결과는 검찰이 그 원본을 보관하되, 복사본은 범죄의 확정적 증거가 되는 것만으로 편집된 것이어야 할 것이다.

목적한 증거를 수집하였거나 영장의 유효기간이 경과하였다면, 영장의 집행은 중지되어야 하며, 새로운 영장을 발부받아야만 전자감시를 계속하는 것이 가능하다.

감시의 결과물(원본)은 법원의 판단에 증거로 사용될 수 있고, 법원의 감시아래 봉인되고 정해진 기간동안 봉인된 채 보관되어야 한다. 현행 법 시행령은 통신제한조치의 집행으로 취득한 결과의 요지를 조서로 작성하고, 그 결과를 봉인하여 열람제한하여 보존하도록 하고 있는데(시행령 제16조 제1항), 수사기관의 통신제한조치의 집행의 적법성과 결과물에 대한 조작가능성을 막기 위하여는 통신제한조치 집행결과물을 법원의 감시아래 봉인하고 법원으로 제출하도록 하는 절차를 마련하는 것이 바람직하다.

전자감시가 종료된 후 또는 영장청구가 기각된 후, 판사와 검사는 전자감시에 관한 사항을 법무부 장관과 국회에 보고하도록 하는 것이 좋을 것이다. 이러한 보고결과에는 영장발부여부, 기간, 감시대상 기구나 장소, 범죄의 종류, 하나의 감시기구에 포착된 평균 감시·감시자·범죄수, 감시비용, 감시의 종류, 수사 또는 재판의 진행정도가 포함되어야 한다. 이러한 자료는 감시영장 발부에 대한 기준을 정하는데 도움을 주며, 입법과정에서도 도움을 주게 될 것이다.[24]

⑻ 컴퓨터 시스템의 압수, 수색에 관한 문제

컴퓨터 시스템을 압수, 수색영장을 발부받아 압수, 수색하는 경우가 있는데, 이때에도 당사자의 통신의 비밀이 침해되지 않도록 유의해야 할 것이다. 특히 컴퓨터 시스템에 다른 사람으로부터 받은 통신이 있거나, 자신이 다른 사람에게 보낸 통신이 포함되어 있는 경우에는 이를 분리하여 압수수색을 하여야 할 것이다.

다. 위치정보의 보호

최근 무선인터넷과 모바일 컴퓨팅 기술의 급속한 발전으로 다양한 위치기반서비스(Location Based Service)가 개발, 제공되고 있다. 오늘날 위치기반서비스가 주목받는 이유는 크게 3가지 측면이 있다고 한다. 첫째, 위치기반서비스는 소위 엠커머스(mobile commerce)를 현실적으로 가능하게 하기 때문이라고 한다. 즉, 위치기반서비스를 기반으로 다양한 사용자 위치 기반의 엠커머스가 가능하며, 위치기반서비스가 없다면 엠커머스는 가능하지 않다. 둘째, 위치기반서비스의 도입으로 다양한 응용서비스가 가능하게 됨으로서 이동통신사의 수익을 극대화할 수 있기 때문이라고 한다. 셋째, 위치기반서비스는 향후 급성장할 차량 인터넷 서비스(automotive telematics : 움직이는 차량을 대상으로 제공되는 무선인터넷 서비스)의 핵심기술이기 때문이라고 한다. 이것은 2010년에 시장규모 50조원으로 성장할 것으로 전망된다고 한다.

위치기반서비스에는 비상구조지원 서비스, 각종 위치정보 서비스, 트래픽과 네비게이션 정보서비스(교통량 및 교통정보 등), 위치밀착형 빌링 서비스, 지능형 교통정보 서비

24) 'wiretap laws and procedures what happens when the U. S. government taps a line' Donald P. Delaney, Dorothy E. Denning, John Kaye, Alan R. McDonald, September 23, 1993의 미국법 소개를 참조하였음.

스 등이 있는데, 앞으로 다양한 신규분야가 생겨날 것으로 보인다.

위치를 측정하는 기술로는 삼각형의 네트워크 망을 이용하는 방법, GPS(Global Positioning System)를 이용하는 방법 과 양자를 결합하는 방식 등이 있다. 삼각형의 네트워크를 이용하는 방식은 이용자로부터 가장 가까운 곳에 있는 세 개의 네트워크 전송탑으로부터 무선 전파신호를 수집하여 이용자의 위치를 계산하여 위치를 측정하는 방식이며, GPS 방식은 항상 같은 위치에 있는 24개의 위성을 이용하는 방식이다. 이 경우 GPS 처리 장치가 단말기에 부착되어 위성으로부터 수신한 GPS 정보를 이용하여 위치를 측정하는 방식이며, 혼합형은 이 두가지를 결합한 방식이다[25].

우리나라의 경우 현재 다양한 위치기반 서비스가 제공되고 있고, 새롭게 연구개발되고 있다. 위치추적을 통한 비상구조지원 서비스도 활성화되었으며, 각종 위치정보 서비스(지도찾기, 친구찾기, 물류정보서비스 등), 트래픽과 네비게이션 정보서비스(교통정보서비스, 자동항법서비스), 이동전화를 통한 각종 콘텐츠 제공서비스 등이 서비스되고 있다[26].

개인의 위치를 파악할 경우 이를 통해서 그 개인의 활동영역과 활동내용을 파악하거나 추측할 수 있다. 특히 이동전화나 PDA 등을 이용하여 위치정보를 파악하는 경우에는 개인들이 일상생활에서 대부분을 이런 장치들을 가지고 있기 때문에 축적되는 개인의 위치정보의 양은 그 개인의 거의 모든 생활영역을 포괄하므로 과도한 사생활 침해의 결과를 낳는다. 일반적으로 개인들은 자신의 위치를 알리려고 하지 않을 경우가 많으며, 때에 따라 개인의 위치는 개인의 매우 민감한 사생활을 침해할 수도 있다. 결국

---

25) 미국 연방공정거래위원회 공개 워크샵 (2002. 2.) The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues. 8페이지

26) 정보통신부 입법안 해설자료

○ 이동통신업체와 같은 통신사업자가 위치정보(기지국 정보, GPS 정보)를 수집할 수 있는 특정장치를 단말기와 통신망에 설치하여 자사의 통신서비스 가입자를 상대로 LBS를 제공

※ 이동통신사업자의 '내친구 찾기 서비스', '주변식당 찾기 서비스' 등

○ 보험회사, 물류업체, 경호회사 등은 해당 위치기반서비스를 제공하기 위하여 고객의 동의를 얻어 고객의 차량, 단말기 등의 위치정보 수집장치를 부착하고, 통신사 통신망을 통해 전달받은 위치정보를 가공·처리하여 자사 고객에게 긴급구난, 최적배차 관리, 긴급출동 등의 LBS를 제공

※ 삼성화재(찾아가는 서비스)는 고객차량에 GPS를 부착한 후 차량사고 발생시 차량위치를 KTF 통신망을 통해 삼성화재센터에서 접수 후, 긴급출동 서비스 제공

※ SK(주)(entrac)은 GPS 기기와 특정휴대폰을 물류차량 등에 제공한 후, 차량위치를 SKT 통신망을 통해 엔트랙 센터로 전송받아, 주문연계, 최적배차 서비스를 제공

○ 부가통신업체 등이 허가 없이 사용할 수 있는 무선망이나 CCTV 등을 활용하여 파악한 위치정보를 통신망을 통해 수집·가공한 후, LBS를 제공

※ 교통정보 전문회사인 로티스는 계약차량에 위치확인 모뎀을 부착한 후 200MHz대역 무선망을 통해 차량위치를 수집하여, 시간대별, 구간별 정체상황, 최적경로 등을 제공

위치정보는 개인의 행동의 자유와 양심의 자유를 심각하게 침해할 수 있으며, 내밀한 사생활의 자유가 침해될 수도 있기 때문에 위치정보에 대해서는 특별한 보호가 필요하다.

이것은 가장 민감한 정보로서 이를 수집하는 경우에는 당해 위치정보 주체의 서면에 의한 사전동의가 있어야 할 것이다. 이때 위치정보 주체에게 수집하고자 하는 위치정보의 내용에 대하여 상세히 설명하고 수집의 목적이 충분히 알려져야 할 것이다. 이 경우 수집된 정보는 해당 서비스만을 위하여 이용되어야 할 것이다.

유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 2002. 7. 12. 지침(Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector)에 의하면 위치정보는 익명으로 처리되어야 하나, 단 가입자나 이용자가 부가서비스를 신청한 경우 그 부가서비스를 제공하기 위하여 필요한 한도와 기간동안만 처리될 수 있다고 한다. 서비스 제공자는 가입자에게 동의를 얻기 전에 위치정보의 유형과 목적과 정보처리 기간과 그 위치정보가 부가서비스를 위하여 제3자에게 제공되는지 여부를 알려야 한다고 규정하고 있다. 이 경우에도 가입자가 언제든지 간편하게 별도의 비용부담 없이 자신의 위치정보 처리의 중단을 요청할 수 있는 절차를 마련해 놓아야 한다고 한다[27].

라. 인터넷 침해사고에 대한 대응과 관련한 정보통신망이용촉진 및 정보보호에 관한 법률 개정안에 대하여

(1) 개요

정보통신부는 인터넷 대란을 계기로 인터넷 침해사고에 효과적으로 대응하고, 인터넷의 안전성을 확보한다는 명목으로 최근 정보통신망이용촉진 및 정보보호에 관한 법률 개정안을 발표하였다. 그런데 이 개정안은 인터넷의 안전성 확보라는 명목아래 국민들의 사생활 침해나 표현의 자유를 침해할 소지가 있으며, 정부에 의한 정보통신망의 통제의 소지가 있는 광범위한 조사권 등을 정보통신부와 한국정보보호진흥원에 부여하고 있어서 문제이다.

27) Aritcle 9.

⑵ 인터넷침해사고대응지원센터

개정안은 정보통신망 침해사고 정보의 수집·전파, 침해사고의 예·경보 및 신속한 대응을 위하여 한국정보보호진흥원에 인터넷침해사고대응지원센터(이하 "지원센터"라 한다)를 둔다고 규정하고 있다. 그런데 개정안에 의하면 지원센터는 각종 정보를 제공받게 되어 있고, 강제협약에 의하여 정보통신망을 실질적으로 관장하게 되어 있다. 현재의 개정안의 내용대로 정보통신망접속서비스제공자에게 지원센터로 침해사고를 신고해야 하는 의무가 부과되고[28], 의무적으로 협약을 맺도록 의무가 부과된다면, 지원센터는 정보통신시설에 대한 국가감독기구나, 수사기관으로 기능할 가능성이 크다[29]. 이러한 지원센터는 불필요하며, 위험하다. 따라서 지원센터는 설치하지 않는 것이 좋다. 만약 설치한다면 지원센터라는 이름 그대로 인터넷침해사고에 대응할 수 있도록 각종 정보의 제공이나 서비스의 제공을 하는 지원연구기관이 적당하다.

한편 국가의 주요 정보통신망에 대한 보호는 기존의 법률인 정보통신기반보호법에 의하여도 충분하다. 그 외의 정보통신망의 안전성의 확보는 국가가 개입하는 것보다는 민간의 자율에 맡기는 것이 좋다. 다만 충분한 안전조치를 취하지 않음으로 인하여 소비자에게 손해가 발생할 경우 소비자가 쉽게 손해의 배상을 받을 수 있도록 하고, 정보통신망사업자들에게는 적절한 수준으로 안전성 확보를 위한 기술적, 관리적 보호조치를 취하도록 하면 될 것이다.

---

28) 아래 각주 참조

29) 제48조의2(인터넷침해사고대응지원센터의 설치 등)
①정보통신망 침해사고 정보의 수집·전파, 침해사고의 예·경보 및 신속한 대응을 위하여 보호진흥원에 인터넷침해사고대응지원센터(이하 "지원센터"라 한다)를 둔다.
②주요정보통신망접속서비스제공자, 집적정보통신시설 사업자 등 정보통신부령이 정하는 사업자는 보호진흥원과 협약을 체결하여 제1항의 규정에 의한 지원센터에 침해사고 대응지원에 필요한 공격유형별 통계 등 정보통신부령이 정하는 정보를 제공하여야 하며, 보호진흥원장은 관계사업자에게 소속직원의 지원을 요청할 수 있다.
③제2항의 규정에 의해 체결한 협약은 정보통신부장관의 인가를 받아야 하며, 정보통신부장관은 상당한 기간을 정하여 협약체결 당사자에게 보완을 명할 수 있다.
④주요정보통신망접속서비스제공자는 정당한 이유 없이 제2항의 규정에 의한 협약체결을 거부하거나 그 이행을 지체 또는 불이행하여서는 아니된다. 협약의 변경을 요청 받은 경우에도 또한 같다.
⑤지원센터는 제2항의 규정에 의한 통계정보를 정보통신망침해사고의 대응을 위하여 필요한 범위에 한하여 사용하여야 하며, 다른 용도에 부당하게 사용하여서는 아니된다.

제48조의 3(침해사고의 신고 등) ①정보통신서비스제공자, 집적정보통신시설사업자, 정보통신시스템 관리자 등은 침해사고의 발생이나 침해사고가 발생할 징후를 발견한 때에는 지체 없이 그 사실을 제48조의 2의 규정에 의한 지원센터에 신고하여야 한다.
②제1항의 규정에 의하여 침해사고를 신고받은 지원센터는 침해사고 예·경보 등 필요한 조치를 하여야 한다.

(2) 정보통신부장관의 침해사고의 원인분석[30]

개정안은 침해사고에 대한 원인분석을 위해 정보통신부장관이 정보통신망접속서비스제공자에게 자료보전을 강제하며 관련자료 제출을 요구할 수 있도록 하고 있다. 이것은 통신의 비밀과 자유를 침해할 소지가 있는 조항이다. 침해사고에 대한 조사는 법원으로부터 영장을 발부받아 수사기관이 수행해야 한다. 다만 침해사고의 수사가 아닌 재발방지를 위한 차원에서의 원인분석이라면 수평적 지위에서 한국정보보호진흥원 등이 민간으로부터 의뢰를 받아서 진행할 수도 있을 것이다. 그러나 이때에도 고객의 개인정보의 유출이 되지 않도록 개인정보를 제거한 후 진행하는 것이 좋을 것이다. 그러나 정보통신부장관이 직권으로 자료보전과 제출을 명하고 조사까지 가능하도록 한 것은 매우 부적절하다.

30) 제48조의4(침해사고 원인분석 등)
①정보통신망을 보유한 자는 침해사고가 발생한 때에는 침해사고의 원인을 분석하고 피해확산을 방지하여야 한다.
②정보통신부장관은 정보통신망에 중대한 침해사고가 발생한 때에는 사고대응 및 복구와 재발방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 당해사고의 원인분석을 할 수 있다.
③주요정보통신망접속서비스제공자는 정보통신망에 접속된 주요장비로의 접속정보, 제공서비스 및 보안에 관련된 오류발생기록(이하 "통신망 접속기록등"이라 한다)을 정기적으로 수집·분석하는 시스템을 구축·운영하여야 한다.
④정보통신부장관은 제1항의 규정에 의한 원인분석을 위하여 필요하다고 인정하는 때에는 정보통신서비스제공자에게 통신망 접속기록등 침해사고 관련자료의 보전을 명할 수 있다.
⑤정보통신부장관은 침해사고 원인분석을 위하여 필요한 때에는 정보통신서비스제공자에게 침해사고 관련자료의 제출을 요구할 수 있으며, 제2항의 규정에 의한 민·관합동조사단으로 하여금 관계인의 사업장에 출입하여 침해사고 원인을 조사하게 할 수 있다. 다만, 통신비밀보호법 제2조의 규정에 의한 통신사실확인자료에 해당되는 사항에 대하여는 통신비밀보호법의 규정에 따른다.
⑥제5항의 규정에 의해 제출받은 자료 및 조사를 통하여 알게된 정보는 침해사고의 원인분석 및 대책마련 외에는 이를 사용하지 못하며 원인분석이 종료된 후에는 이를 파기하여야 한다.
⑦제2항의 규정에 의한 침해사고 관련자료의 보전대상, 보전기간 및 제출자료를 보호하기 위한 관리대책, 제3항의 규정에 의한 조사를 수행하는 자의 자격, 지정절차, 조사절차 등에 필요한 사항은 대통령령으로 정한다.

(3) 정보통신부장관의 기술적 관리적 조치 요구권[31]

개정안은 정보통신망접속서비스제공자는 정보통신부장관이 고시하는 바에 따라 안전성 확보에 필요한 기술적·관리적 조치를 하여야 한다고 하여 정보통신부장관에게 안전성 확보에 필요한 기술적·관리적 조치권을 부여하고 있다. 그런데 안전성 확보를 위한 기술적·관리적 조치에는 표현의 자유나 사생활의 비밀을 침해하는 내용이 들어갈 수도 있기 때문에, 조치의 내용을 포괄적으로 고시에 위임하는 것보다는 법률로서 그 대강을 규정하는 것이 바람직할 것이다.

4. 수사 또는 범죄 예방 활동의 수단으로 CCTV의 활용

가. 실태와 문제점

최근 CCTV를 통한 감시기술이 비약적으로 발전하고, CCTV 감시비용이 낮아지면서 세계 각국에서 CCTV를 수사 또는 범죄예방활동의 수단으로 활용하는 사례가 늘고 있다. 우리나라의 경우도 주로 과속이나 신호위반과 같은 교통단속용이나 지하철과 같은 위험시설에서 활용되었는데, 최근에는 주택가의 쓰레기 불법투기 단속, 경범죄 단속, 노점 단속용이나 강력범죄 단속용으로 도입이 추진되고 있는 실정이다. 그런데 CCTV는

---

31) 제45조
②정보통신부장관은 전기통신사업법 제2조제1항제1호의 규정에 의한 전기통신사업자로서 전국적으로 정보통신망접속서비스를 제공하는 자(이하 "주요정보통신망접속서비스제공자"라 한다) 및 정보통신부령으로 정하는 일정규모 이상의 정보통신서비스제공자가 정보통신망의 안정성확보를 위하여 준수하여야 할 다음 각호의 1에 해당하는 사항의 세부기준을 정하여 고시할 수 있다.
1. 정보통신망에 대한 부정한 접근을 방지하고, 침입에 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보시스템의 가용성을 확보하기 위한 기술적·물리적 보호조치
4. 정보보호 인력, 조직, 예산 확보 및 정보보호 계획 수립 등 정보시스템의 안전·신뢰성확보를 위한 관리적 보호조치
5. 기타 정보통신부장관이 정보통신망의 안정성확보를 위하여 필요하다고 인정하는 사항
③정보통신부장관은 제2항의 규정을 적용받지 아니하는 정보통신서비스제공자에 대하여 제2항 각호의 1의 규정의 준수를 권고할 수 있다.
④정보통신부장관은 정보보호 취약부문에 대해 정보보호기준을 권고하고 침해사고 예방 및 확산방지를 위하여 필요한 기술지원 등을 할 수 있다.

다음과 같은 문제를 야기한다.

첫째, 사생활 침해이다. 기술이 발달할수록 사생활 침해의 정도는 더 커질 것이다. 그리고 은밀한 CCTV 촬영의 경우는 사생활 침해의 정도가 훨씬 크다. 둘째, 거리나 공공시설에 시위방지용으로 CCTV를 설치할 경우에는 표현의 자유를 침해할 것이다. 이를 통한 위축효과(chilling effects)는 측정하기 곤란하나 분명하고 중대한 위협임에 틀림없다. 셋째, 촬영된 자료의 오용으로 인한 문제이다. 이와 관련해서 외국의 경우 많은 사례들이 보고되고 있다. 넷째, 설치된 CCTV의 규제는 어려운 반면, 기술은 촬영의 정확도나, 검색이나 인식의 정확도 등의 측면에서 점점 발전하고 있다. 한번 설치된 CCTV는 철거하기 어렵고, 늘어나는 추세인데다 설치된 CCTV의 기능도 검색기능, 회전기능, 정밀촬영 기능, 원격촬영 기능, 야간촬영 기능 등으로 늘어나고 있어서 문제가 더 심각해지는 것이다.

나. 범죄예방 효과에 대한 논란

한편 CCTV의 범죄 예방과 범죄 단속의 효과에 대하여도 논란이 있다. 예컨대 스코틀랜드의 글래스고우의 경우를 보면, 1994년에 32대의 카메라를 설치하였는데, The Scottish Office Central Research Unit의 조사 결과를 보면, 범죄발생율이 올라가고, 검거율이 떨어졌다고 한다[32]. 물론 범죄 예방과 단속에 효과가 있었다는 조사 결과도 있는데, 이 경우에도 단순히 범죄지만 이동시키는 효과만 가져온다는 반론도 만만치 않다. 어쨌든 CCTV의 범죄예방이나 단속 효과에 대하여는 확실한 결론을 내리기가 어렵다.

다. CCTV 감시의 법적 문제점

범죄예방이나 수사를 위한 CCTV 촬영이 당사자에게 미치는 효과를 본다면 침해의 정도는 불심검문에 비견될 수 있을 것으로 보인다. 즉, 불심검문의 경우 평온한 상태가 깨지고, 위축효과가 있는데, CCTV 촬영의 경우에도 마찬가지로 평온한 상태가 깨지고, 위축효과가 있게 된다. 물론 당사자는 의식하지 못하여 이런 효과가 크지 않을 수 있으나, 이것은 당사자가 그 효과를 잘 알지 못하기 때문일 수 있다. 오히려 그 효과의 측면에서는 1회적인 불심검문보다도 기록물이 남게 되고, 검색이 되며, 기록된 정보도 많

32) http://www.scotcrim.u-net.com/researchc2.htm

으므로(당시의 거동, 장소, 동행자, 소지물, 기타 행동의 정황 등) 인권침해의 정도가 클 수도 있다. 한편 특정인에 대한 CCTV 카메라의 조작에 의한 촬영은 통신이나 우편에 대한 감청이나 검열과 같은 수준의 침해로 볼 수 있을 것이다.

따라서 CCTV의 감시는 불심검문이나 통신에 대한 감청과 동일한 수준에서 법률적인 근거를 가지고 이루어져야 할 것이다.

그런데 경찰관직무집행법에 의하면 경찰권의 발동으로 불심검문을 하기 위한 요건은 다음과 같다(경찰관직무집행법 제3조).

(l) 요건 : 경찰관은 수상한 거동 기타 주위의 사정을 합리적으로 판단하여 어떠한 죄를 범하였거나 범하려 하고 있다고 의심할 만한 상당한 이유가 있는 자 또는 이미 행하여진 범죄나 행하여지려고 하는 범죄행위에 관하여 그 사실을 안다고 인정되는 자에 대하여(제1항)

(2) 내용 : 정지시켜 질문할 수 있고(제1항), 부득이한 경우는 경찰서 등으로 동행할 것을 요구할 수 있다(제2항).

(3) 절차 : 질문하거나 동행을 요구할 경우 경찰관은 당해인에게 자신의 신분을 표시하는 증표를 제시하면서 소속과 성명을 밝히고 그 목적과 이유를 설명하여야 하며, 동행의 경우에는 동행장소를 밝혀야 한다.

(4) 권리 : 불심검문을 당한 자는 질문이나 동행요구를 거절할 수 있다. 동행시에는 가족에게 알리고 본인에게 연락할 기회를 주고, 변호인의 조력을 받을 권리가 있음을 고지하여야 한다.

한편 경찰관직무집행법에 의하면 경찰관은 범죄행위가 목전에 행하여지려고 하고 있다고 인정될 때에는 이를 예방하기 위하여 관계인에게 필요한 경고를 발하고, 그 행위로 인하여 인명·신체에 위해를 미치거나 재산에 중대한 손해를 끼칠 우려가 있어 긴급을 요하는 경우에는 그 행위를 제지할 수 있다(경찰관직무집행법 제6조).

이상으로 검토한 바와 같이 개별적인 불심검문이나 범죄예방활동이 아닌 일반적인 검문이나 범죄예방활동의 일환으로 CCTV를 통하여 감시를 하는 것은 법적 근거가 희박하고, 사생활 침해와 표현의 자유 등의 위축효과가 크므로 위법의 소지가 크다고 보여진다. 불심검문의 경우는 권리의 고지나 거부의 자유가 있으나, CCTV에 의한 촬영은 반드시 그 장소를 가야 하는 경우에는 거부의 자유도 없다. 이와 같이 어떤 면에서는 권리의 침해정도가 더 큰 CCTV 촬영은 불심검문보다 더욱 더 엄격한 요건과 절차규정을 마련해야 할 것이다.

그리고 특정인에 대한 CCTV의 촬영은 통신제한조치에 준하여 영장에 의하여야 할 것이다. 비록 현행 통신비밀보호법은 통신비밀보호법과 형사소송법과 군사법원법의 규정에 의하지 아니하고는 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못하도록 하고 있어서, 대화를 녹음없이 녹화나 촬영만 하는 경우에 대해서는 보호가 미치지 않지만, 대화를 녹음하거나 청취하지 않더라도 공개되지 아니한 타인간의 대화를 녹화하거나 촬영하는 경우에는 대화의 내용상의 비밀 뿐만 아니라 대화의 상대방, 시간, 장소 등이 침해되므로, 공개되지 아니한 타인간의 대화를 청취하거나, 녹음, 녹화, 촬영 기타의 방법으로 기록하거나 저장하는 행위도 엄격히 영장주의에 의해야 할 것이다.

한편 특히 표현의 자유와 밀접한 관련을 가질 수 있는 장소에 설치 운영하는 CCTV는 표현의 자유를 위축시키게 되므로 명백하고 현존하는 위험이 존재하는 경우에만 제한적으로 허용되어야 할 것이다. 그리고 부득이 허용되는 경우라도 표현의 자유를 위축시킬 수 있는 용도로의 사용은 제한해야 할 것이다.

라. CCTV 촬영에 대한 입법안

이상의 논의를 기초로 CCTV 촬영에 대한 입법안을 정리해 본다면 다음과 같이 그 요건과 절차를 마련할 수 있을 것이다.

(1) 범죄예방 목적의 CCTV의 사용

범죄예방 목적으로 CCTV를 활용하는 것은 경찰관직무집행법 상의 불심검문에 준하여 범죄발생 가능성이 현저히 큰 경우 즉, 특정한 범죄가 발생할 고도의 개연성이 있는 경우로서 해당 범죄의 예방을 위해 다른 수단이 효과가 없을 경우로 한정하는 것이 좋을 것이다. 그리고 과속의 단속과 같은 교통안전을 목적으로 하는 경우는 요건, 절차, 기타 안전장치(설치장소, 표시, 촬영범위, 자료의 이용, 비밀유지, 피촬영자의 권리 - 접근권 등)를 법제화하여 허용하는 것이 좋을 것이다. 그리고 특히 프라이버시의 침해의 소지가 큰 주거지나 상업시설의 경우에는 CCTV의 설치는 특별한 긴박한 사유가 없으면 허용되어서는 안될 것이다.

그리고 CCTV 촬영을 하는 경우에는 CCTV에 대한 모든 정보를 공개하고(웹사이트 등에 설치장소, 성능, 녹화된 자료의 취급 절차, 자료취급자… 등), 미리 CCTV 설치에 대하여 의견을 수렴하는 것이 좋다. 그리고 CCTV 촬영에 관하여 분명하게 알아 볼 수

있도록 CCTV 촬영사실에 대하여 알려야 한다. 그리고 촬영방법은 가장 침해가 적은 방법으로 촬영이 이루어져야 한다. 그리고 이 경우 음성녹음을 허용해서는 안될 것이다.

그리고 촬영된 사람들의 정보접근권을 인정해 주며, 촬영된 화면은 목적 외 사용이 금지되며, 알게 된 사실을 누설하지 못하도록 비밀유지의무를 져야 한다. 그리고 촬영된 자료는 프라이버시 보호를 위하여 오랜 시간 보존해서는 안되며, 약 15일 정도 지나면 폐기하도록 하는 것이 좋다.

(2) 범죄수사 목적의 CCTV 사용

범죄수사 목적으로 CCTV를 사용하는 것은 통신제한조치에 준하여 이루어져야 할 것이다. 따라서 특정한 범죄에 대하여, 범죄혐의가 인정되고, 다른 방법으로 수사를 하는 것이 곤란한 경우에만 인정되어야 할 것이다.

5. 결론

이 외에도 새로운 감시기술의 활용사례는 매우 많다. 각각의 경우 무엇보다도 중요한 것은 해당 감시기술에 대하여 법원이나 입법부 등이 충분한 기술적 통제를 할 수 있어야 한다는 것이다. 그리고 감시기술의 수사에서의 활용은 강제처분 법정주의와 영장주의의 기초아래 엄격하게 이루어져야 한다.

인터넷과 인권

백 욱 인
(서울산업대학교 사회학교수)

순 서

I. 인터넷과 관련된 인권의 영역 ·····91
II. 네트와 법적 규제 ·····94
III. 네트와 인권 침해 ·····96
VI. 사이버스페이스에 대한 규제의 위상과 대응 ·····102

인터넷과 인권

백 욱 인
(서울산업대학교 사회학교수)

I. 인터넷과 관련된 인권의 영역

20세기 후반 들어 정보통신기술은 아주 빠른 속도로 발전하였다. 컴퓨터와 네트워크의 발전은 일상적인 생활 환경에 커다란 변화를 몰고왔다. 정보통신기술은 개개인의 사생활과 사회생활을 모두 변화시키고 있다. 인터넷을 포함한 새로운 정보통신기술이 일상화되면서, 정보통신기술의 기술적 차원뿐 아니라 그 사용과 관련된 사회적 차원의 문제들이 발생하게 된다. 사용자의 참여를 바탕으로 이루어지는 정보통신 네트워크는 새로운 사회영역을 만들어내기 때문에 그것에 이해와 관심을 가진 사람들의 참여도가 크고 그만큼 복잡한 문제가 벌어진다.

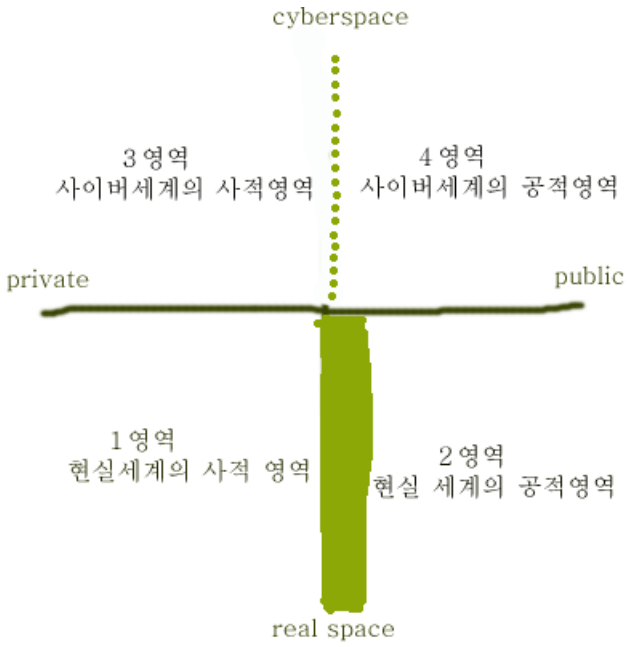
NEIS, 등급제, 몰래카메라, 실명제, 음란물, 스팸메일 등은 인터넷의 사용이 일반화됨에 따라 새롭게 등장한 말들이다. 실명제는 익명성을 토대로 전개되던 초기 인터넷이 누렸던 사상과 표현의 자유를 위협한다. 음란물을 빌미로 한 등급제는 사상과 표현의 자유를 심각하게 위협할 뿐만 아니라 새로운 검열과 통제를 합리화한다. 스팸메일과 몰래카메라는 개인의 프라이버시를 여지없이 짓밟아 놓는다. 이런 사태는 대한민국헌법 2장 국민의 권리와 의무 가운데 많은 부분이 위험에 처하게 됨을 보여준다.

정보기술과 관련하여 나타나는 인권문제를 사적 영역과 공적 영역으로 나누어 살펴볼 수 있다. 현실사회의 공적 영역과 사적 영역은 윤리적인 차원에서는 가정, 공간적으로는 집이라는 울타리에 의해 보호된다. 집과 가정은 가족과 개인의 사생활을 보호하는 울타리인 것이다. 그리고 집과 가정에서 이루어지는 일은 사적인 영역으로 보호되고 있다(헌법 16조/헌법 17조). 한마디로 현실세계의 집은 프라이버시 보호의 성채라 할 수 있다. 사적 영역과 공적 영역을 엄격하게 분리하는 방식은 근대자본주의 사회의 기본적인 틀을 이룬다. 현실세계의 집은 사적인 휴식과 재생산이 이루어지는 공간으로서 사회와 타자로부터 보호되고 격리되어 있다.

그러나 사이버스페이스의 집(홈페이지)은 공개성으로 나가는 길목이다. 현실세계의 집은 외부의 공적인 장소와 차단하는 공간이지만, 사이버스페이스의 홈페이지는 개인을 다른 개인들과 이어주는 매개체가 된다. 공적 영역과 사적 영역을 이어주는 통로인 것이다. 그래서 사이버스페이스의 사적 영역과 공적 영역은 현실세계의 그것처럼 엄격하게 구분되지 않는다. 사적인 것과 공적인 것 사이의 구분이 흐려지고 경계가 불투명해지며 상호 이동과 소통이 쉽게 이루어진다.

이처럼 현실세계의 사적 영역과 공적 영역에 대비되는 사이버세계의 사적 영역과 공적 영역을 표시하면 <그림 1>과 같다. <그림 1>의 '1영역'(현실세계의 사적 영역)에서는 개인의 자유와 권리가 프라이버시 보호를 중심으로 이루어진다. 주거의 자유(16조)와 신체의 자유(12조) 및 사생활의 비밀(17조)이 영역에서 이루어지는 주요한 인권들이다. 1영역과 2영역 사이에는 비교적 분명한 구분이 형성되고 있으며, 이에 따라 공적인 일과 사적인 일이 비교적 명확하게 분리되고 법률의 틀에서도 민사와 형사로 구분되어 있다. '2영역'에서 이루어지는 인권은 교육권(31조), 사회보장(34조), 환경권(35조) 등의 사회적 권리로 이루어진다. 최근에는 정보기술 발전과 더불어 정보접근권이나 정보공개권 등의 새로운 권리들도 주요한 인권으로 부각되고 있다.

한편 사이버세계의 권리는 개인 정보발신자의 권리로부터 출발한다. 자신의 집을 짓고 남들과 소통할 수 있는 권리는 사이버세계를 만드는 가장 기초적인 요소이다. 그래서 사상과 표현의 자유는 사이버세계에 존재하는 집의 대들보이다. 그리고 사상과 표현의 자유는 집회와 결사의 자유에 의해 확보되므로, 국가권력이나 특정 집단이 사상과 표현의 자유를 위해(危害)할 경우에 대비하여 사이버세계에서의 집회와 결사의 자유가 보장되어야 할 것이다. 정보화와 관련하여 사상과 표현의 자유가 제일 먼저 이슈로 떠오르는 이유는 컴퓨터 네트워크가 새로운 미디어이자 영토(territory)이기 때문이다. 사상과 표현의 자유 및 집회와 결사의 자유라는 기본적인 권리는 사이버세계의 사적 영역(3영역)과 공적 영역(4영역)을 이어주는 매개이자 통로 역할을 한다.



〈그림 1〉 사이버세계의 인권영역

정보통신기술이 일상생활에 폭넓게 활용되고 컴퓨터 네트워크의 이용이 늘어나면 인간의 기본적인 권리를 침해하는 새로운 문제들이 발생하게 되는데, 프라이버시 침해와 지적 재산권을 통한 정보와 지식의 제한이 그것이다. 컴퓨터 네트워크를 통해 이동하는 자료와 정보는 개인의 활동으로부터 빠져나간 것이기 때문에 이에 대한 의도하지 않은 통제와 활용이 이루어질 경우 프라이버시와 관련된 문제가 발생할 수 있다. 국가와 자본과 다른 개인에 의한 사적 정보의 도용과 오용이 이루어질 때 개인의 프라이버시는 심각한 위험에 처하게 되는 것이다. 자본과 국가는 데이터베이스를 활용한 감시와 통제를 강화할 수 있다. 이런 데이터베이스를 통한 감시와 통제는 개인의 프라이버시와 관련된 정보를 이용하여 개인을 통제하기 때문에 개인은 이중적으로 인권을 침해당한다.

한편 자본은 사적 정보의 공적 활용과 공적 정보의 사적 활용을 통해 정보와 지식을 상업화하고 상품화하며, 이런 정보와 지식의 독점과 상품화는 곧바로 공적 영역에서 정보불평등 문제를 불러일으킨다. 이것이 지적 재산권을 둘러싼 문제영역이다. 정보 접근권 및 사용권이 사이버스페이스의 기본 권리로 등장하는 이유가 여기에 있다.

II. 네트와 법적 규제

문제는 헌법에 보장하고 있는 기본적인 인권이 서로 상충되는 경우이다. 지적재산권과 사상과 표현의 자유가 부딪히거나 언론의 자유가 사생활의 비밀과 모순되는 경우가 흔히 일어난다. 재산권이 사상과 표현의 자유를 억압하는 경우도 있고 재산권의 행사가 공공복리와 위배되어 국민의 인권을 침해하는 사례도 많이 있다. 또한 국가와 시민사회 간의 대립뿐만 아니라 시민사회 내부에서 서로간의 긴장과 대립이 심화되고 그것이 인권을 침해하는 경우도 점차 늘어나고 있다.

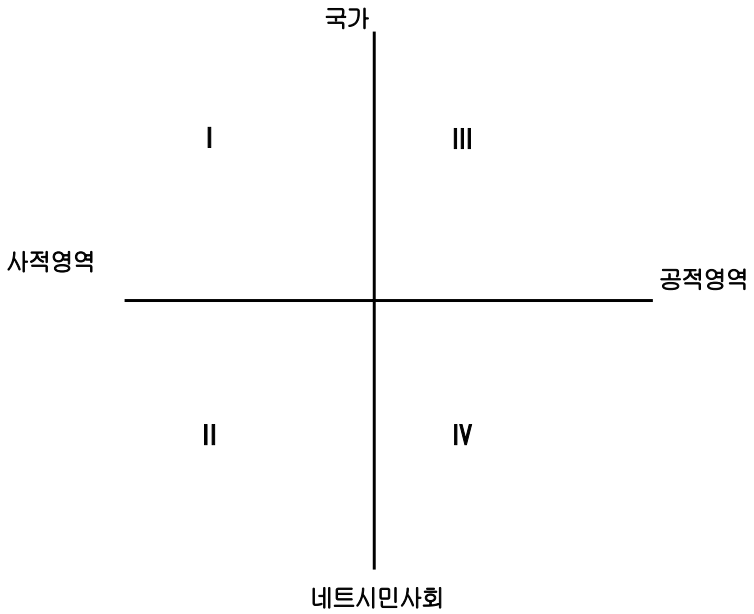
국가의 법적 규제가 네티즌의 규범과 대립할 수밖에 없는 이유에 대해 살펴보았다. 국가와 자본은 사이버스페이스의 규범을 길들여 현실세계의 법적 규제로 대체하려 시도한다. 이에 대해 네트 사용자들은 자신들의 주권과 규범의 수호를 내걸며 대항한다. 자유주의와 규제주의의 일방적인 주장이 아니라 이미 만들어져있는 네티즌의 규범과 국가의 법적 규제간에 협약과 합의 과정이 필요함을 인정한다면 사이버스페이스에 대한 규제가 갖는 위상을 이해하는 데 한걸음 더 가까이 접근할 수 있다.

그런데 네티즌의 규범이나 국가의 법률이 일방적으로 모든 영역에 걸쳐 관철되어야 한다는 식의 일방주의보다 각각의 영역별로 양자간의 관계가 변화하는 유연한 모델을 설정할 필요가 있다. 현실세계와 마찬가지로 사이버스페이스도 사적 영역과 공적 영역으로 이루어진다. 규범과 법률이 각각 어떻게 관철되고 있는가를 도식화하기 위해 사이버스페이스를 사적 영역과 공적 영역으로 구분한 후 네티즌의 자율적인 규범과 국가의 법률적 규제가 이루어지는 영역으로 분할해 보았다.

다음의 <그림 2>는 국가기관의 법적 규제와 네트 시민사회의 규범을 기준으로 하고 사적영역과 공적영역을 구분 축으로 설정하여 작성한 모형이다. 국가 규제가 우세한 사적영역 I은 이메일이나 개인정보에 관한 보호를 중심으로 이루어진다. 데이터베이스나 개인정보의 유출을 법적으로 보호하는 사적 정보의 보호 영역이기도 하다. 개인의 프라이버시가 침해당하거나 사적 정보가 공적으로 유출되는 것을 막는 일은 사회적으로 매우 중요하다. 프라이버시 보호를 중심으로 한 이 영역에서의 규제는 쉽게 사회적 합의를 얻어낼 수 있다. 이 영역에서 이루어지는 국가 기구의 규제는 사이버스페이스의 규범과도 크게 대립되지 않는다. 문제는 국가가 개인의 정보를 통제하거나 사적 정보를 정권의 차원에서 관리하거나 조작할 우려가 있다는 점이다. 이러한 우려를 막거나 감시할 사회적 안전망이 필요한 지점이기도 하다. 감시사회에 대한 우려는 데이터베이스 감

시(Lyon and Zureik, 1996)로 이루어지는 I 영역에서의 통제와 감시를 염두에 둔 것이다.

II 영역은 사적 영역에 대한 시민사회나 자율적인 협약이 이루어지는 영역이다. 일대일의 양방향적 의사소통이 동시적으로 이루어지는 쪽지글이나 대화방 등은 이 영역에 속하는 대표적인 사례이다. 이메일을 통한 비동시적 의사소통도 자율적인 행위를 통해 서로간의 의사교환이 이루어지는 사적 공간이다. 이메일이나 대화방에서 오고가는 이야기에 대한 개입과 규제는 사적 영역에 대한 감시만큼이나 위험하다. 그 이유는 그곳이 일대일의 대화와 의사소통이 이루어지는 공간이기 때문이다. 전화도청이나 감시가 불법인 것처럼 II 영역에 대한 감시는 그 자체로 프라이버시의 침해라는 문제를 낳는다. 시민사회 내부에서 이루어지는 자율적 감시와 통제도 위험하기는 마찬가지이다. 사적 영역에 대한 존중과 보호가 부실할 경우 개인 프라이버시의 유출에 따른 사이버스페이스의 황폐화가 확대될 우려가 크다. 개인 프라이버시에 대한 I, II 영역은 국가기관의 보호 정책을 중심으로 조심스런 개입과 규제의 틀을 모색할 필요가 있다. 단, 프라이버시를 침해하는 행위와 개인정보를 사익을 위해 활용하는 경우 이런 행위에 대한 법적인 규제가 강화되어야 할 것이다.



〈그림 2〉 규제주체와 대상 영역

III 영역은 공적 분야에 대한 국가의 규제 영역이다. 현재 인터넷 게시물의 내용을 규제하는 법안의 경우가 이 분야에 해당한다고 볼 수 있으며 규제에 관한 논란에서 핵심을 차지하는 분야이다. 음란물에 대한 규제책이나 불온통신물에 대한 규제책 또한 이에

속한다. III 영역은 II 영역과 달리 완결된 내용을 특정한 관점과 틀로 재단하여 규제하는 영역이다. 우리나라의 경우 규제 대상 내용이 주로 '불온통신'이나 '음란물'에 집중되어 있다 하지만 정치적인 이슈나 사상 자체를 통제하는 경우도 흔히 발생한다.

여러 가지 부작용과 사회적 문제 때문에 사이버스페이스에 대한 법적인 규제가 불가피하다면 '누가(규제주체), 무엇(규제대상)을, 왜(규제 이유와 근거), 어떻게(규제형성과정) 그것을 만드는가가 명확하게 밝혀져야 한다. 자율적인 합의로 만들어진 규제와 법적 강제에 따른 규제가 갖는 의미는 다를 수밖에 없다. 정부가 주도하는 법적 규제는 사회 공익을 대변한다고 하지만 실제로 특정 집단의 이해를 차별적으로 반영할 수밖에 없다.

또한 규제의 대상이 사업자인지, 사용자 개인인지에 따라 법적인 효력과 영향력도 달리 나타난다. 사업자를 통한 간접적인 규제와 사용자 개인에 대한 직접 규제가 동시적으로 병행될 수도 있다. 사용자 개인에 대한 규제보다는 사업자를 통한 간접 규제 방식이 이루어지는 경우가 많지만 개개인에 대한 직접적인 통제도 병행되고 있는 실정이다. 인터넷 사용자 전체를 규제하는 것인지 사업자만 규제하는 것인지 아니면 특정 연령대의 집단을 규제하는 것인지에 따라 상당히 다른 문제들을 낳을 수 있다.

IV영역은 사용자들의 협약을 통해 공공성의 새로운 공간이 만들어지는 곳이다. 이 영역은 공적인 영역을 만들어나가기 위한 사회적 합의가 이루어지는 공간이자 규제주체와 대상이 동일한 자율적 규제의 영역이다. 정보의 발신 주체들은 공적 영역에 자신의 생각과 사상을 자유롭게 펼쳐 보일 수 있어야 한다. 그래야 사이버스페이스에 공적 영역이 만들어질 수 있다. 만약 공적 영역에서 통제와 간섭이 이루어질 경우 사이버스페이스의 형성 자체가 위태롭게 된다. 새로운 공적 공간은 사상과 표현의 자유없이 만들어질 수 없다.

III. 네트와 인권 침해

(1) 사상과 표현의 자유

현실사회에서 민주주의를 형성하는 가장 기본적인 요소는 '사상과 표현의 자유'를 통한 참여와 연대이다. '민주주의'란 평등한 참여자들간의 의사소통 및 여론이 모아지는

과정을 거쳐 이루어진다. 사이버스페이스의 민주주의는 '컴퓨터로 매개된 의사소통'을 통해 이루어지는 '공론의 장'으로서 '네티즌'의 참여와 연대를 통해 만들어진다.

수많은 네티즌이 인터넷의 기본 철학과 이념으로 '제퍼슨의 자유주의'(Jeffersonian Liberalism)를 내세우는 이유는 제퍼슨이 민주주의의 다른 어떤 가치보다도 '사상과 표현의 자유'를 우선시했기 때문이다. 사상과 표현의 자유는 네티즌끼리 서로 연대하고 행동하는 자유로 이어진다. 연대하고 행동할 수 없는 사상과 표현의 자유는 아무런 의미가 없다. 사상과 표현의 자유는 '집회와 결사'의 자유로 이어질 때 온전한 의미를 갖게 되는 것이다.

네티즌의 집회와 결사는 현실세계의 그것과 다른 모습으로 이루어진다. 네트에서는 시간과 공간의 제약을 뛰어넘어 빛의 속도로 자신들의 의견을 이야기하고 결집할 수 있다. 새로운 네트의 힘은 '지위를 이용하여 남을 지배하는 힘'(power over others)이 아니라 '다른 사람과 함께할 때 생겨나는 힘'(power with others)이다. 이러한 네트의 힘은 자유로운 의사 소통과 결집을 통해 만들어진다. 스스로가 쟁점들을 이야기할 수 있을 만큼 충분히 교육받고 자유롭게 활동할 수 있을 때 전자민주주의의 이상이 실현될 수 있는 것이다.

초기의 인터넷 공동체주의자들은 인터넷의 기술적인 구조와 특성 때문에 규제가 불가능하다는 '규제불가론'을 주장하였다. 그러나 네트의 완전독립론이 헛된 꿈에 불과하듯이 규제불가론도 최근 들어 별로 근거 없는 이야기가 되어버렸다. 국가의 법적인 규제와 네트 사용자들의 자율적인 규범 간에는 마찰과 대립이 존재한다. 그런데 네트 사용자는 수동적인 소비자가 아니라 적극적 개입과 참여로 스스로 미디어의 내용과 형식을 창출하는 주체이기 때문에 이러한 네트 시민권운동의 성패는 온라인으로 이루어지는 '풀뿌리행동주의'(grassroot activism) 및 광범한 참여와 연대를 기반으로 한 운동을 어떻게 확산하는가에 달려 있다. 네트의 생활상의 이해 가운데 가장 중요한 것은 네트의 커뮤니케이션 틀에 주목할 경우 '사상과 표현의 자유'이고, 공동체적 성격에 주목하면 '집회와 결사의 자유'이다.

우리나라의 경우 인터넷에 대한 규제를 담고 있는 『정보통신망이용촉진등에관한법률』이 2001년부터 시행되고 있다. 이 법은 인터넷에 올라오는 내용에 대해 정부 행정기관이 직접 규제할 수 있는 법적 근거를 제공한다. 이 법 제42조는 정보통신부의 산하단체인 '정보통신윤리위원회'에게 인터넷 청소년유해매체물을 지정할 수 있는 권한을 부여하고 있다. 이 법의 시행령에서는 청소년유해매체물로 지정된 경우 차단용 소프트

웨어가 이를 인식하여 자동으로 그것을 차단할 수 있도록 전자적인 부호를 이용하여 청소년유해매체물임을 표시하도록 규정하고 있다.[33]

인터넷 내용 규제와 관련하여 가장 큰 문제가 되는 것은 국가의 법적 규제가 아키텍처와 코드를 통한 규제와 결합되어 활용되는 경우이다. 이는 레식의 규제 모형에서 법적 규제와 아키텍처 규제의 통합 방식에 해당한다. 이런 경우 네트 사용자의 합의와 규범을 통한 수평적이고 자율적인 규제와는 달리 국가가 법적으로 규제를 강제한다는 문제가 있고 코드를 활용한 규제이기 때문에 사용자의 입장에서 규제를 빠져나가기 힘들다는 기술적 강제의 문제점을 안고 있다. 이러한 법적 규제와 아키텍처 통합형 규제가 내용 등급제로 실현되고 있는 것이다.

전자 표식과 소프트웨어를 활용하여 특정한 등급 기준의 내용물을 걸러내어 사용자가 특정한 사이트에 접근할 수 없도록 만드는 내용등급제는 네가티브 검색엔진의 역할을 한다. 픽스(PICS)는 사용자가 자신의 필요와 선호에 따라 인터넷 내용물을 선별적으로 통제하려는 의도에서 만들어진 것으로서 그것 자체는 컨텐츠에 관한 메타정보를 활용하여 웹 페이지의 내용을 특정 범주로 분류하는 표기 기술에 지나지 않는다.[34] 이러한 네거티브 검색 시스템의 경우 문제는 누가 등급을 정하고 어느 정도의 등급에서 차단할지를 결정하는 일이다. 사용자 개인이 스스로 내용물 제한의 등급을 결정하는 것이 아니라 특정한 국가기구나 단체가 이를 타율적으로 규제할 경우 픽스 기반 등급제는 사상과 표현의 자유를 심각하게 위협하는 검열과 통제의 수단으로 전락할 우려가 있다.

보통 기계나 기술은 가치중립적인 것으로 받아들여진다. 그래서 기술 자체에는 가치지향이나 의도가 포함되어 있지 않은 것으로 생각한다. 소프트웨어 자체는 가치중립적인 것이고 그것은 순전히 사용하는 사람들의 의도에 달린 것으로 받아들이게 된다. 그러나 인터넷 검색 엔진은 선택과 배열을 통하여 내용물을 검열하고 규제하는 역할을 담당한다(Lucas, 1998).

---

33) 정보화촉진기본법시행령 제21조 [일부개정 1999.6.30 대통령령 제16458호]
제21조 (청소년유해매체물의 표시방법) ①법 제42조의 규정에 의한 청소년유해매체물을 제공하는 자는 당해 매체물에 19세 미만의 자는 이용할 수 없다는 취지의 내용을 누구나 쉽게 확인할 수 있도록 음성·문자 또는 영상으로 표시하여야 한다. ②제1항의 규정에 의한 표시를 하여야 하는 자중 인터넷을 이용하여 정보를 제공하는 자의 경우에는 기호·부호·문자 또는 숫자를 사용하여 청소년유해매체물임을 나타낼 수 있는 전자적 표시도 함께 하여야 한다. ③정보통신부장관은 정보의 유형 등을 고려하여 제1항 및 제2항의 규정에 의한 표시의 구체적 방법을 정하여 관보에 고시한다.

34) 픽스는 내용물의 성분을 표시하는 언어로서 검색 소프트웨어나 차단 소프트웨어와 결합하여 사용될 경우 자동적으로 등급 처리된 내용물을 차단하는 역할을 수행한다. 이때 픽스는 필요한 것을 찾아내는 검색엔진과는 반대로 불필요한 것을 걸러내는 역할을 수행한다. 공공장소의 컴퓨터나 피씨방 컴퓨터들은 '청소년유해매체물'을 기준으로 특정 사이트 차단이 설정되어있다. 픽스 기반의 인터넷내용시스템에는 RSACi와 ESRB, SafeSurf와 Medcertain, ICRA, 정보통신윤리위원회의 SafeNet, 등이 있다.

검색엔진의 용도와 기능은 그것을 사용하는 사람에 달려있다고 생각하기 쉽지만 검색엔진에는 정치적 의도와 상업적인 고려가 깊게 담겨있다. 검색엔진은 원하는 모든 것을 찾아주지 않는다. 야후(Yahoo)처럼 사업자가 카다고리를 스스로 결정하거나 홈페이지 주소를 등록해야하는 경우는 선별과 거름 작용이 반드시 개입한다. 사용자가 검색엔진을 쓰지 않고 스스로 찾아낼 수만 있다면 가장 이상적이겠지만 자신이 원하는 자료와 정보를 검색 없이 찾아내기란 불가능한 일이다.

이처럼 인터넷에서는 지식과 정보를 선택하고 배열하는 것 자체가 검열과 통제로 활용될 수 있다. 중립적으로 보이는 프로그램 뒤에는 선택과 배열을 통한 통제와 조작이 깃들어 있는 것이다. 자동화된 코드를 통한 규제는 내용에 대한 선택과 차단에 다름 아니다. 이러한 규제는 사상과 표현의 자유를 억압하고 사회구성원의 알 권리를 특정 집단의 이해에 따라 왜곡하거나 제한할 위험을 갖고 있다. 이상에서 사이버스페이스에서 규제가 이루어지는 구조와 그 구체적인 사례를 살펴보았다. 사이버스페이스의 규범과 아키텍처에 영향을 미치는 규제는 네트 사용자와 어떤 형태로든지 협약을 이루어야만 실제적인 효력을 발휘할 수 있을 것이다.

(2) 지적 재산권과 정보공유

월드와이드웹(WWW)을 비롯한 네트워크 관련 기술은 과학자간의 자료와 정보를 나누고 서로의 생각을 빛의 속도로 주고받는 공유의 정신에서 비롯되었다. 그러나 정보자본주의 아래서 인터넷은 빛의 속도로 상업화되고 있다. 상업화되고 상품화된 정보는 현실세계의 다른 상품과 마찬가지로 배타적으로 소유되어야 하고 그를 통해 이윤을 창출해야 된다. 그래서 디지털 정보에 대한 지적 재산권의 법적인 확립이 정보자본주의의 가장 핵심적인 관심사로 떠오른다. 이러한 지적 재산권의 일방적인 확립은 정보와 지식의 공유와 협동을 저해하는 요소로 작용할 가능성이 아주 높다. 따라서 이를 둘러싼 쟁점이 정보기본권이란 차원에서 제기된다. 정보와 지식에 대한 배타적인 소유권은 지식기반 사회에서 새로운 불평등을 낳는 원인으로 작용하기 때문이다.

네트 사용자가 아주 빠른 속도로 증가하고 자본과 국가의 통제와 개입이 늘어남에 따라 초기 네트의 특징으로 이야기되던 탈상품화와 탈중심화의 가능성이 채 실현되기도 전에 '재상품화'(recommodification)와 '재중심화'(recentralization)라는 정반대의 흐름이 몰아치고 있다. 자료와 정보의 공유를 주장하며 '자유 소프트웨어 운동'을 전개하던 흐름도 '지적 재산권'의 확대・강화라는 추세에 밀리고 있는 실정이다.

자본의 주도 아래 이루어지고 있는 미래의 '디지털 신경제'는 지적 재산권의 확장 없이는 불가능하다. 정보독점과 네트의 재상품화를 추구하는 자본의 목적은 네트에서 오가는 정보에 대한 사용료를 지구적 차원에서 법적으로 인정받는 법안을 확립하는 데 있다. 정보자본은 '디지털 지적 재산권'의 확보를 자신의 향후 운신을 위한 필요조건으로 보고 있다. 그래서 지적 재산권의 정치는 이해관계를 달리하는 사회집단간의 대립에 따라 상이한 전선을 만들어낼 것이다. 곧 디지털 컨텐츠 강국인 선진자본주의, 특히 미국과 제3세계 간의 대립, 거대 독점자본과 사용자 간의 대립, 컨텐츠 제작자와 기업 간의 대립 등 지적 재산권을 둘러싼 이해관계를 축으로 다양한 쟁점이 형성될 것이다. 사용자의 사용권을 어떤 수준에서 어떻게 확보하느냐가 지적 재산권을 둘러싼 네트 사회운동의 핵심적 내용을 이룰 것이다.

지적 재산권의 전반적인 적용은 정보접근권을 제한할 뿐 아니라 사상과 표현의 자유를 제한하는 도구로도 활용될 수 있다. 지적 재산권 보호는 사적 재산의 보호와 근본적으로 성격이 다르다. 지적 재산권은 지식과 정보의 독점을 낳고 이것이 지식과 정보의 불평등으로 이어질 경우 이것은 인권에 대한 침해로 작용할 가능성이 매우 크다.

헌법 23조에서는 재산권을 보장하되 재산권 행사가 공공복리에 적합하도록 하여야한다고 규정하고 있다. 그렇다면 사이버스페이스의 재산권인 지적 재산권은 인권과 관련하여 어떤 문제를 제기하는가? 자본주의는 재산권에 근거를 둔 사적 소유체제이다. 지적재산권이란 이러한 소유체제를 서비스나 지적 생산물에까지 확장한 배타적 소유개념의 확립을 의미한다. 그러나 자본주의에는 사적 소유뿐만 아니라 공적 이용이 공존하는 체제이기도 하다. 그래서 지적 재산권과 공유물(commons)간의 대립, 카피라이트와 카피레프트간의 대립이 존재한다.

그러나 남의 지적 재산권을 카피레프트의 입장을 내세워 무조건 무화시키는 것이 능사는 아니다. 디지털로 전화된 숱한 정보와 지식에 대한 원저작자의 권리는 여전히 소중하다. 그들은 나름대로 존중되어야 마땅한 것이다. 카피레프트의 진정한 의미는 남의 저작권을 부인하는 것이 아니라 자신의 저작권을 사회로 환원하여 공유하는 데 있다. 카피레프트 운동이 사회적 힘을 얻으려면 디지털 공유 운동으로 한단계 더 나가야 한다.

디지털 아카이브의 건설과 디지털 공유 운동은 카피레프트 운동을 구체화하는 밑바탕을 마련한다. 아카이브는 문명화된 공동체의 필수품이자 '꿈이 이루어지는 장소'이다. 리차드 스톨만의 프리소프트웨어 재단(FSF)에서 시작된 정보공유의 전통은 리눅스(Linux)로 이어지고 오픈 소스(open source) 운동으로 전개되고 있다. 그러나 소프트웨어는 전문적인 특정 영역에 제한되어 있기 때문에 엔지니어링과 무관한 일반 사용자들

에게는 아직까지 거리가 멀게 느껴지는 분야이다. 그러나 다양한 영역에 거쳐 만들어지는 디지털 내용물들의 공유 영역은 갈수록 확장되고 있다. 자신의 생각을 글, 그림, 영상, 소리로 표현한 갖가지 디지털 정보가 비트 저장고에 차곡차곡 쌓이고 있다. 이러한 소통의 결과들을 나누고 서로 커뮤니케이션하는 것 자체는 디지털 공유를 통해 가능하다. 네티즌은 자신의 말과 소리와 몸짓 하나하나에 지적 재산권을 거는 멍청한 짓을 하지는 않는다. 그러나 이것을 사회화하고 상업화한 후 사용 권한에 제한을 가하는 독점적인 카피라이트는 분명 네트의 열린 공간을 닫아버리고 공유의 정신을 독점의 욕심으로 눌러버리는 행위이다.

인터넷의 미래는 참여자들의 공공 정보를 얼마나 확보하느냐에 달려있다. 모든 정보를 상업화하고 상품화하는 나라와 공공의 정보를 나누는 나라간의 경쟁력은 엄청나게 달라질 것이다. 별 것도 아닌 오락정보를 돈주고 파는 나라와 문화유산을 공공의 정보로 제공하는 나라간의 지적 경쟁력은 갈수록 벌어질 것이다.

(3) 프라이버시와 정보공개

자본주의 사회에서는 국가권력과 자본에 의한 감시와 통제가 일상적으로 이루어지고 있다. 국가권력은 사회구성원의 활동과 사회적 환경을 토대로 하여 그들이 무엇을 생각하는지, 어떤 행동을 할 것인지를 예측하고 통제한다. 데이터베이스를 활용하여 개인의 생각과 행동을 감시하는 것을 전자감시라고 하는데, 이런 전자감시는 비단 국가권력에 의해서만 이루어지고 있는 것은 아니다. 정보기술이 생산에 도입되면서 각종 감시와 통제 기술이 발전하고 작업장에서는 각종 신기술을 활용하여 노동자의 작업과정을 낱낱이 감시하고 통제한다. 작업반장이나 감독의 부릅뜬 눈이 아니라 전자 눈으로 감시와 통제가 이전되고 있는 것이다.

이러한 전자 눈의 감시와 통제는 현실세계뿐 아니라 사이버스페이스에서는 더욱 공공연하게 이루어진다. 사이버스페이스는 컴퓨터 네트워크를 통해 이루어지는 정보와 생각의 나눔터이다. 이곳에서는 갖가지 생각이 오가고 공동체가 만들어지고 아이디어와 생각과 의견이 교환된다. 그러나 사이버스페이스는 전자기술을 활용하여 만들어지는 공간이기 때문에 전자기술을 활용한 감시와 통제가 일상적으로 이루어질 수 있다. 컴퓨터 네트워크 소프트웨어 기술을 이용할 경우 개인의 신상에 관한 정보와 사이버스페이스에서 이루어진 생각과 활동에 관한 정보를 손쉽게 추적할 수 있다.

따라서 이에 대한 사회적 대책을 마련하지 않는다면 사이버스페이스는 감시와 통제가 판치는 인권유린의 공간으로 전락할 수 있다. 국가와 자본에 의한 프라이버시 침해뿐 아니라 사회단체나 개별 사용자에 의한 프라이버시 침해의 위험 또한 존재한다. 청소년 보호와 음란물 퇴치를 빌미로 벌어지고 있는 준정부기관 및 사회기구의 모니터링은 개인의 프라이버시에 치명적인 위협이다. 한편 사이버스페이스에서는 익명성의 뒤에 숨어 개인의 개인에 대한 근거 없는 음모와 인신공격도 손쉽게 이루어질 수 있다. 이렇듯 사생활의 비밀 보호는 정보기술과 관련하여 가장 쉽게 유린될 수 있는 인권분야이다.

개인의 프라이버시는 철저하게 보호하면서 의견의 위축을 가져오지 않고 그것을 활성화하기 위한 방안이 필요하다. 의견에 대한 공격은 자유롭게 펼치되 상대의 의사를 존중하는 토론문화가 만들어져야 한다. 인격과 의견을 분리하여 의견에 대한 비판이 한 사람의 인격 전체에 대한 비난으로 전환되지 않도록 새로운 공론체제를 만들어야 한다.

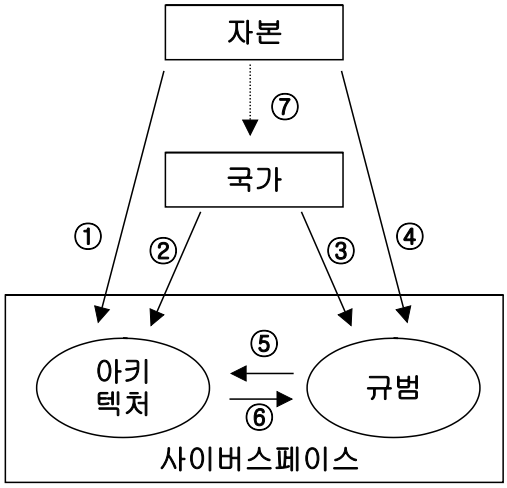
사생활 보호와 공공정보의 공개는 동전의 앞뒷면이다. 공공기관과 권력이 수집한 시민에 관한 정보와 시민의 세금으로 만든 자료와 정보 그리고 시민을 대상으로 수집한 통계자료 등은 공개되어야 마땅하고 모든 사회구성원에게 자유롭게 사용이 허락되어야 한다. 따라서 공공적으로 축적된 모든 정부관련 정보는 원칙적으로 공개되어야 마땅하다. 정보공개는 더 넓은 의미의 정보정의 실현을 이루는 기초가 된다. '정보정의'란 정보와 지식에 대한 보편적 접근과 활용에서의 평등을 실현하는 것을 의미한다. 정보의 독식과 독점은 정보불평등을 가져온다. 정보불평등은 새로운 빈곤의 씨앗을 뿌린다.

VI. 사이버스페이스에 대한 규제의 위상과 대응

레식(Lessig)은 사이버스페이스에서 이루어지는 규제를 ① 규범(norms)을 통한 통제, ② 법률(law)을 통한 통제, 그리고 ③ 소프트웨어의 구조(architecture)를 활용한 통제, ④ 시장(market)을 통한 정보 통제로 분류하였다. 물론 이러한 네가지 규제 방식은 서로 결합되거나 혼합되어 사용될 수 있다. 규제 관련 법률은 사용자들의 관습과 시장에 영향을 미칠 수 있고 사이버스페이스 전체의 아키텍처에도 영향을 미칠 수 있다. 국가주도의 규제는 법률을 출발점으로 그 규제 근거를 마련한다.

그러나 레식처럼 규제를 규범, 법률, 소프트웨어, 시장의 네가지로 구분하는 것은 통제가 이루어지는 근거에 관한 부분과 통제의 구체적 방식을 혼용하고 있기 때문에 혼

돈의 여지가 있다. 통제가 이루어지는 근거에 따라 국가주도의 타율적인 규제와 시민사회 주도의 자율 규제로 나누는 것이 논의를 분명하게 정리하는 데 도움이 될 수 있다. 사이버스페이스에 대한 통제를 위해 사용되는 구체적인 방식으로는 레식의 분류처럼 기술에 의한 통제와 시장을 통한 통제로 갈라 볼 수 있을 것이다. 다음의 <그림 3>는 사이버스페이스에 대한 규제 구조를 이해하기 위해 설정한 모형이다.



〈그림 3〉 사이버스페이스 규제의 위상

<그림 3>에서 보듯이 규제주체를 국가와 네트 사용자로 구분할 수 있다. 먼저 사이버스페이스 내부 구성원간의 합의와 협약에 의해 이루어지는 자율적인 규제(⑤, ⑥)를 설정할 수 있다. 그것이 코드를 사용한 등급제이건 혹은 특정 내용에 관한 필터링이건 관계없이 이런 경우 규제 주체와 대상이 큰 틀에서 일치하거나 규제 대상이 규제 주체에게 권한을 위임했다면 규제에 관한 논란이 크게 일어나지 않을 것이다. 그러나 사이버스페이스의 외부에서 내부로 향하는 규제(①②③④)에서는 규제 주체와 대상이 다르다. 이런 경우를 타율적 규제라 부를 수 있을 것이다. 그것은 코드와 기술적인 아키텍처를 통해 규제(①, ②)될 수도 있고 네티즌의 규범에 직접적인 영향(③ ,④)을 미칠 수도 있다. 국가 기구는 법률을 통하여 이러한 규제를 시행할 것이다.

자본도 마찬가지로 사이버스페이스의 기술적인 구조와 규범에 개입하거나 규제를 가할 수 있다. 자본은 법률을 통해 국가기구를 대행자로 내세워 규제를 가할수(⑦)도 있고 직접적으로 사이버스페이스의 아키텍처나 규범에 개입할수(①, ④)도 있다. '선물경제'와 같은 규범을 조장했다 급격하게 유료화를 통한 상업적 규범을 강요할 수도 있고, 느슨한 저작권을 퍼뜨리다가 강력한 저작권 보호로 선회할 수도 있다. 자본은 시장과

상품을 통하여 네티즌들의 소비규범을 조절하거나 변화시킨다(④). 이와 더불어 관련 정보통신 관련 산업체들은 실제 표준을 확보하거나 새로운 기술을 개발함으로써 사이버스페이스의 기술적 구조에 영향을 미친다(①). 이런 개입과 규제가 법률적인 형식을 통해서 전개될 수도 있고 그냥 시장의 자유로운 발전 속에서 전개될 수도 있으며 양자가 결합되어 진행될 수도 있다.

초기 인터넷의 기술적인 아키텍처와 네티즌들의 규범과 관행이 국가와 자본의 개입과 규제를 어렵게 만든 요인이었다. 국가와 자본의 입장에서는 사이버스페이스의 기술적 구조에 개입하거나 네트 사용자들의 규범과 관습을 변화시키는 것이 가장 일차적인 과제로 부각된다. 그러나 국가와 자본이 네티즌의 관습에 영향을 미칠 수 있는 간접적인 규제와 대책없이 인터넷의 기술적 구조에 개입하거나 사이버스페이스에 대한 직접적인 규제를 감행할 경우 네트 사용자들의 거센 저항에 직면할 수밖에 없을 것이다.

인터넷은 생각을 전달하는 미디어인 동시에 사람들이 만나고 참여하는 공동체이다. 따라서 인터넷에 대한 규제는 원칙적으로 네트의 주권을 가진 사람들에 의해 참여와 합의를 바탕으로 이루어져야 한다. 사이버스페이스에 대한 규제가 불가피하다면 법률 조항을 만드는 과정이 투명하게 이루어져야 하고, 사회적 여론과 합의를 거쳐야하고, 사상과 표현의 자유나 집회와 결사의 자유 같은 네트의 기본권이 보호되어야 할 것이다. 이러한 원칙들이 사이버스페이스의 규범과 국가 기구의 법률적 규제를 조정하는 협약주의의 근간을 이루어야 한다.

인터넷은 사용자의 참여를 통해 만들어지는 열린 공간이다. 수많은 생각과 표현이 이루어지는 이 공간의 규범과 질서는 자율과 참여를 통해 만들어져야 한다. 어느 정도의 규제가 불가피하다면 네트 사용자들의 수평적인 관계에서 만들어지는 협약을 통해 이루어져야 한다. 우리나라도 법적 기술적 강제보다는 인터넷 자율 규제 모델을 적극적으로 모색해야 한다. 인터넷 내용에 대한 규제와 이에 관한 법률 제정은 충분한 사회적 토론과 합의가 이루어져야 한다. 협약에 근거한 규제만이 실제적인 효능을 발휘할 수 있을 것이다.

「公共機關의 個人情報保護法改正案」
說 明 資 料

정 국 환
(행정자치부 행정정보화기획관)

순 서

1. 그간의 推進經緯 ·····107

2. 改正案 主要 骨子 ·····107

「公共機關의 個人情報保護法改正案」說明資料

정 국 환
(행정자치부 행정정보화기획관)

1. 그간의 推進經緯

○「공공기관의 개인정보보호법 개정계획」수립 : ’02.9
○「공공기관의 개인정보보호제도 발전방안」연구 용역 : ’02.11
※ 한국전자정부연구원
○ 입법계획 수립 및 법개정안 초안 마련 : ’03.5
○ 실무자 축조심의(3차) : ’03.6
○ 민변 주최 토론회 발표 및 의견수렴 : ’03.6.27
○ 개인정보보호 법제 정비 관련 토론회(정부혁신위 주관) : ’03.7.25
○ 관계부처 협의 : ’03.8.1 ~ 8.14
※ 向後 推進日程
○ 입법예고 : ’03. 8월말
○ 법제처 심사 : ’03. 10
○ 차관회의 및 국무회의 : ’03. 11,
○ 국회상정 : ’03. 12

2. 改正案 主要 骨子

(1) 總 則

○ 用語 定義 規定의 整備
- 電子政府에서는 네트워크를 통한 개인정보 유통이 활발함에 따라, 현행 ‘개인정보화일’ 등 컴퓨터 단말기 중심에서 네트워크·시스템 중심으로 개인정보가 규율될 수 있도록 정보통신망, 개인정보DB, 개인정보시스템 등의 규정 신설

* 네트워크를 통한 개인정보의 유통(예시)

・G4C사업, 인터넷 국세종합서비스 등 전자정부 11대사업 구축등에 따른 개인정보 DB의 공동이용 및 온라인상에서의 유통

○ 個人情報保護原則의 明示

- OECD 개인정보보호 8원칙 등 국제적인 개인정보 보호기준을 참고하여 개인정보 보호의 일반원칙을 명시적으로 규정

※ 수집제한의 원칙, 정보내용의 정확성 및 안전성 확보의 원칙, 목적명확화의 원칙, 이용제한의 원칙, 공개의 원칙 등

(2) 個人情報의 蒐集·保有

○ 個人情報蒐集의 엄격한 制限

- 정보주체의 동의 또는 법률의 규정 등이 있는 경우에만 개인정보 수집 가능하도록 제한

※ 현행법 규정

・사상・신조 등 개인의 기본적 인권을 현저히 침해할 우려가 있는 개인정보는 정보주체의 同意 또는 '다른 법률에 수집대상 개인정보가 명시'되어 있는 경우를 제외하고는 원칙적으로 수집 금지

○ 保有機關의 長은 個人情報 蒐集시 事前 告知

- 정보주체의 분명한 認識하에 개인정보가 수집될 수 있도록 개인정보 수집의 법적 근거, 수집・이용 목적 등을 인터넷 등에 게재

※ 다만, 국가안전・범죄수사・조세범측 조사 등의 경우는 제외

○ 개인정보 DB 보유, 개인정보시스템 구축시 事前協議 義務化

- 현행 개인정보화일 '事前通報制'가 형식적 운영에 그치고 있어, 개인정보 DB 구축 관련 통제 강화를 위해 '事前協議制'로 전환

※ 다만, 국가안전・범죄수사・조세범측 조사 등의 경우는 제외

안 제6조(개인정보데이터베이스등 보유시 사전협의 등) ③第1項의 規定은 다음 各號의 1에 해당하는 個人情報데이터베이스등에 대하여는 이를 적용하지 아니한다.

1. 國家의 安全 및 外交상의 秘密 기타 國家의 중대한 이익에 관한 사항을 記錄한 個人情報데이터베이스등
2. 犯罪의 搜査, 公訴의 제기 및 유지, 刑의 執行, 矯正處分, 保安處分과 出入國管理에 관한 사항을 記錄한 個人情報데이터베이스등
3. 租稅犯處罰法에 의한 租稅犯則調査 및 關稅法에 의한 關稅犯則調査에 관한 사항을 記錄한 個人情報데이터베이스등
4. 삭제
5. 삭제
6. 保有機關의 내부적 業務處理만을 위하여 사용되는 個人情報데이터베이스등
7. 삭제
8. 기타 이에 준하는 個人情報데이터베이스등으로로서 大統領令이 정하는 個人情報데이터베이스등

(3) 個人情報의 利用·流通

○ 개인정보의 統合·管理시 事前協議 義務化

– 수집된 개인정보를 다른 개인정보와 統合하고자 하거나,

– 이미 구축·운영 중에 있는 개인정보 DB를 연계·활용 가능함에도 불구하고, 別途의 개인정보 DB를 구축·운영하고자 하는 경우에는

– 행자부장관과 사전협의를 의무화함으로써 개인정보가 지나치게 통합 관리되지 않도록 함

○ 보유기관의 장은 개인정보의 수집 目的外 利用 또는 제3자에게 提供할 경우

– 이용 또는 제공목적, 법적근거 등을 인터넷 등을 통해 공시토록 함으로써,

– 개인정보 관리의 투명성 강화

○ 個人情報의 責任性 具現

– 個人情報保護責任官制度 신설, 당해 기관의 개인정보관리업무의 총괄·감독 등의 기능 수행

⑷ 個人情報主體의 權利 强化

○ 대규모의 個人情報 保有·流通에 따른 個人情報管理의 透明性 강화

– 행자부장관은 보유근거·목적, 제공기관 등이 포함된 공공기관의 개인정보DB 목록을 인터넷에 공개(년 1회이상)

– 수집목적외로 개인정보를 가공하는 경우 그 가공목적 등이 포함된 '개인정보보호방침'을 인터넷에 게재

○ 情報主體의 閱覽·訂正 請求權 强化

– 종이문서외 인터넷을 통해서도 개인정보의 열람·정정 및 삭제 가능

○ 個人情報侵害申告센터의 설치·운영

– 정보주체의 개인신상 정보 침해, 주민등록번호 도용 등 개인정보의 오·남용, 유출 등으로 야기된 피해 신고 접수·처리

⑸ 個人情報保護審議委員會의 機能 强化

○ '事前審議方式'을 통한 위원회의 권한 강화

– 개인정보에 관한 법령 제·개정시 위원회 사전 심의

– 개인정보 DB 구축 및 DB 통합의 경우 위원회의 사전 심의 등

3. 개인정보의 투명한 수집·관리를 위한 기업의 의무·개인의 권리

○ 기업의 의무 : 개인정보가 정확하고 투명하게 수집·관리·이용될 수 있도록 개인의 동의에 의한 개인정보 수집 및 목적 외 이용금지 등 의무

※ 현재, 기업에서는 고객의 개인정보를 보호하고 개인정보 관련 이용자의 불만을 처리하기 위하여 개인정보관리책임자제도를 운영 중에 있음

○ 개인의 권리 : 동의·열람·정정요구·동의철회권 등

※ 기업은 동의철회 요청 시 지체 없이 개인정보를 파기하도록 규정하고 있으며, 오류정정 요청이 있는 경우에는 오류를 정정할 때까지 정보를 이용하지 못하도록 규제하고 있음

II. 개인정보보호의 현황 및 문제점

1. 개인정보 침해사례의 증가

- 개인정보의 이용 증가와 함께 개인정보 침해 사례가 크게 증가하여 사회문제로 대두

〈 개인정보 침해 및 불법 스팸관련 신고 처리 실적 〉

구 분	2001년	2002년	2003.1~5.	계
개인정보	388	1,237	1,706	3,331
불법스팸	254	90,786	91,991	183,031
총 계	642	92,023	93,697	186,362

< 개인정보침해사례 >

○ H할인카드회사가 도산하자 관리하던 개인정보를 1인당 1만원씩 받고 판매(2003, 1.22, 한국일보)

○ 개인의 신용정보가 결혼정보업체, 스포츠센터, 각종 클럽 등에서 불법적으로 이용되고 있음 (2003.4.20, inews24)

○ 울산지역 유선방송 가입자인 A사 가입자 6천여 명의 신상정보가 인터넷을 통해 무방비로 노출 (2003. 5.3, 세계일보)

○ 보험사 및 보험대리점이 불법으로 개인정보를 수집해 영업에 활용 (2003.5.14, 중앙일보)

○ 결혼정보회사 듀오의 회원가입자 30만 명의 개인정보 유출(2003.5.14, 중앙일보)

2. 개인정보보호를 위한 대책 현황

○ 민간분야의 개인정보보호를 강화하기 위해 정보통신망법을 두 차례에 걸쳐 전면 개정(2000.1, 2001.1)하여 개인정보보호를 위한 법·제도적 기반 구축

- 개인정보보호지침(2002.4), 쇼핑몰 개인정보보호가이드라인(2002.10), 개인정보의 안전한 취급을 위한 가이드라인(2003.3)등 세부가이드라인을 제정·보급
- 개인정보 처리를 위탁받은 자에 대한 의무강화, 쿠키 등을 통한 개인정보 수집·이용 규제, 분쟁조정위원회 기능 강화 등을 마련하기 위해 정보통신망법 개정을 추진 중(2003. 7)

○ 개인정보침해 및 불법 스팸메일에 대한 민원업무를 수행하기 위해 한국정보보호진흥원내에 개인정보침해신고센터 및 스팸대응센터를 설치운영

○ 개인정보 침해로 인한 정보통신서비스제공자와 이용자간의 분쟁을 신속·간편하게 조정하기 위해 개인정보 분쟁조정위원회를 운영 중

※ 운영실적 : 2002.1~2003.5월 매월 1회 개최하여 총 1,363건 조정 처리

- 향후 분쟁조정 신청이 증가할 것에 대비하여 On-line을 통한 분쟁조정제도의 도입을 추진 중

○ 법제도에 의한 규제만으로는 급변하는 정보이용환경의 변화에 대응하기 어려우므로 민간기관에 의한 자율규제를 지원 중

- 개인정보보호 수준이 우수한 사이트를 심사하여 마크를 부여하는 개인정보보호마크(e-Privacy마크)제도를 도입(2002.2)하여 운영 중

※ 2003.5월 현재 91개 웹사이트가 마크 취득. 일본 및 미국 등과 마크 상호인정을 추진 중

- 민간 기업체 주도의 개인정보보호 협의체인 개인정보관리 책임자협의회 구성운영(2002.7~)

※ 개인정보관리책임자협의회는 4개분과(쇼핑몰/C2C, 포탈/컨텐츠, ISP/이동통신, 금융/보험) 42개사가 참여 중

III. 정보화시대의 개인정보에 대한 접근 방향

1. 정보화의 진전에 따라 개인정보의 이용이 증가

○ 공공부분에서는 행정의 능률성 향상 및 대국민 서비스 증대를 위해 개인정보의 공동 활용이 증가

○ 민간부분에서는 기업의 마케팅 강화 및 전자상거래 등 경영전략 차원에서 개인정보의 수집·이용, 제3자 제공이 증가

○ 개인정보의 이용 급증에 따라 침해사례도 급증하고 있으며, 컴퓨터기술의 발달로 인해 개인정보가 인위적으로 조작될 수 있어 개인정보의 오·남용 등 개인정보 침해문제는 더욱더 사회문제화 되고 있음

2. 정보사회에서 개인정보의 규범적 가치

○ 개인정보보호는 고전적 의미의 Privacy권에서 출발

- 프라이버시권은 개인적 공간에서 타인의 침해로부터 자유로울 수 있는 권리로 이해(침해로부터 무조건 보호해야 할 기본권)

○ 정보사회에서의 개인정보보호 문제는 그 중요성이 더욱 강조되는 상황이나 고전적 의미의 프라이버시권과 다른 시각에서 검토할 필요가 있음

- 왜냐하면, 정보사회에서 개인정보는 대부분 개인의 동의(허락)에 의해 형성되는 것이며
- 다수인의 정보가 집적되어 재산적 가치를 형성한다는 점에서 고전적 의미의 프라이버시 보호문제와는 차이가 있기 때문임

※ 다음, 옥션, 등과 같은 닷컴기업은 가입회원수로 기업가치가 결정되며 기업의 인수합병시 그 재산적 가치는 대부분 관리하고 있는 집적된 개인정보에서 형성

○ 따라서, 개인정보보호를 사생활의 비밀보장과 같은 인권차원에서만 접근할 것이 아니라, 개인정보를 재산권적 가치 차원에서 접근하여 개인정보를 보호하는 동시에 개인정보의 이용도 증가시켜 경제적 사회적 효율성도 증가시킬 수 있는 법적·제도적 방안을 검토하는 것이 바람직

※ 물론 생명, 신체, 사상과 같은 민감한 정보는 재산적 가치와는 다른 인권적 차원에서 접근한다는 기본적인 인식이 필요

Ⅳ. 개인정보보호를 위한 바람직한 정책방향

1. 국민·기업체의 개인정보보호에 대한 인식제고

- 최근 조사에 따르면 개인정보 보호에 대한 국민의 인식이 저조하며, 기업체도 관련 법률에 대한 인식 및 실천의지 부족으로 개인정보 관련 고충을 외면하거나 방치하는 사례 빈발

※ 인터넷이용자 95.4%가 프라이버시 침해를 우려하면서도, 45.9%가 개인정보 제공 전에 사업자의 개인정보보호방침을 확인하지 않음(KISA, 2002. 12)

※ 기업의 개인정보 보호를 위한 장비와 인력에 투자한 2000년도의 규모는 약 60%가 매출액의 2%이하라고 응답(KISDI, 2001. 12)

2. 개인정보의 투명하고 공정한 관리를 위한 법제도 확립

○ 정보사회에서는 개인정보가 정보통신망을 통해 수집 및 대량처리, 유통이 이루어지고 있다는 점을 고려하여, 정보통신망에서 수집 및 유통되는 개인정보를 공정하고 투명하게 관리하기 위한 정책수립, 법 및 제도를 수립해야함

3. 개인정보보호를 위한 보호기술(Privacy Enhancing Technology) 개발 및 보급

○ 개인정보보호는 법·제도와 더불어 기술적 보호조치가 수반되어야 실효성이 극대화될 수 있으므로

– 전자서명, 인증제도, 암호기술 등을 통하여 주민번호의 오·남용 방지, 민감한 정보 등 중요정보의 암호화 등을 통해 법·제도상의 미비점을 상호 보완해 나가야함

4. 기존 법률에 의해 보호되지 못하는 개인정보보호의 사각지대 해소를 위한 법개정

○ Off-line 사업자중 여행업·호텔업·항공업·학원·교습소(5개 업종)

※ 국내 5인 이상 민간사업체의 약 50%가 정보통신망법의 적용을 받고 있음

⇒ 법률에 의해 보호를 받지 못하는 사각지대가 존재

※ 패스트푸드, 이·미용실, 비디오가게 등과 같이 회원제 형태로 운영하는 기업이 Off-line상에서 디지털 형태로 관리하는 개인정보

※ 동창회·향우회 등 비영리 목적의 단체가 관리하는 개인정보

⇒ 법률의 보호를 받지 못하는 사각지대 및 개별법에 의해 불완전하게 보호되고 있는 영역에 대해서도 개인정보보호가 충분히 보호하기 위해서는 정보통신망법 확대 개정 또는 기본법 제정 필요

5. 민간부문의 개인정보보호와 공공부문의 개인정보보호 방향

○ 민간부분에서 개인정보의 수집·이용 및 제3자 제공은 본질적으로 개인의 자발적인 합의(동의)에 근거하여 이루어지고 있으므로 “개인정보의 자기결정권”이 이미 행사되었다고 볼 수 있음

- 궁극적으로는 미래에 개인의 개인정보를 재산권적인 가치를 붙여 거래하는 시장이 형성될 것으로 전망
- 따라서, 민간부분에서의 개인정보보호는 시장에서 기업과 개인의 공정한 질서가 유지되고, 기업과 개인이 대등한 관계에서 거래를 할 수 있도록 정부의 정책방향을 수립할 필요가 있음

  ※ 즉, 개인정보의 불법 수집 및 유통, 오·남용 등 불공정 행위를 방지하기 위해 사전적 예방과 사후적 규제를 어떻게 하느냐에 규제의 초점을 맞추어야 함

○ 공공부분에서는 개인정보의 수집·축적 및 이용이 개인의 동의여부에 상관없이 법률에 의해 강제된다는 점에서 민간부분과 본질적인 차이가 있음

- 따라서, 공공부분에서 개인정보의 수집·축적 및 이용은 민간부분보다 더욱 엄격하게 법률에 의해 강제되어야 하며, 개인에게 "개인정보의 자기통제권"을 더욱 철저히 보호할 필요가 있음

○ 이와 같이 똑같은 개인정보라 하더라도 민간부분은 자율적 규제를 통한 개인정보의 이용 및 보호를 통해 경제 및 사회의 효율성을 제고하는 한편 법제도를 통해 개인의 인권을 보호하는 균형 잡힌 정책을 추진하고, 공공부분에서는 보다 강력한 규제를 통해 개인정보를 접근하는 시각이 바람직할 것으로 생각함

프라이버시 보호와 관련 법제도 개선 필요성

강 달 천
(한국정보보호진흥원 선임연구원)

순 서

1. 정보사회와 개인정보 ·····123

2. 현행 법제도의 체계적 정비 필요 ·····125

3. 정보사회의 변화와 국제사회의 요구 확대 ·····127

프라이버시 보호와 관련 법제도 개선 필요성

강 달 천
(한국정보보호진흥원 선임연구원)

1. 정보사회와 개인정보

정보화사회에서 국가행정을 비롯하여 거의 모든 분야에서 컴퓨터와 인터넷을 사용하고 있다. 정보사회에서 어디에서든지 존재하고 있는 것이 컴퓨터이며 이 안에는 Bit(이진수 단위)와 byte(8bit) 단위롤 이루어진 헤아릴 수 없을 정도의 개인정보가 저장되어 있다. 국가의 컴퓨터 안에는 국민의 가족사항, 재산상태 등에 관한 기록이 담겨있으며, 또한 국민이 어디에 주거하던지 그의 이동경로가 담겨있기도 하다. 심지어는 운전경력이나 범죄기록 등도 저장하고 있어서 개인에 관한 거의 모든 정보를 저장하고 있다고 보아도 과언이 아니다. 나아가 현대에는 국가보다도 민간부문에 더 많은 개인정보가 유통되고 있다. 이제는 누구라도 슈퍼마켓, 약국, google.com, daum.net 등 각종 웹사이트 등 개인이 접촉하는 곳이면 어디에서나 개인정보를 수집할 수 있게 되었다.

최근에서야 많은 사람들이 정보기술이 거대한 능력을 발휘한다는 사실, 국가를 포함한 공공기관과 사업자들이 자신에 관한 다양한 정보를 가지고 있다는 사실, 그리고 타인이 자신의 정보를 오남용함으로써 치명적인 손해를 입을 수 있다는 사실을 깨닫기 시작하였다. 즉 자신에 관한 상세한 개인정보가 제3자의 관리 하에 놓여있고, 이로 인하여 피해를 입을 수도 있다는 가능성을 이해하기 시작하였다. 그러나 이것은 막연한 이해와 깨달음일 뿐이다. 우리들은 누가, 언제, 어느 정도의 피해를 입을 것인지 알지 못하는 두려움을 가지고 있다. 인터넷을 비롯한 정보통신의 혜택을 누리고 있으면서도 많은 사람들이 타인의 컴퓨터 안에 자신에 대한 정보가 어떠한 경로를 통해 얼마나 저장되어 있는지, 타인이 자신의 정보를 수집하고 사용함에 대하여 과연 통제가 가능한 것인지에 대한 막연한 두려움만을 가지고 있는 것이다.

정보사회에서 정보의 지배는 자유의 조건이자 동시에 권력의 원천이다. 특히 개인정보의 지배는 그 정보주체에게는 인격의 존엄과 자유의 불가결한 조건이 되지만, 동시에 타자에게 있어서는 무한한 권력의 기초가 된다. 이 때문에 한 개인의 자신에 관한 정보를 스스로 통제하지 못한다는 사실은 프라이버시 보호를 주장하는 사람들의 주된 관심사였다.

이러한 정보프라이버시(information privacy)의 문제를 지적하기 위하여 많은 사람들이 조지 오웰의 소설 「1884」에 묘사된 “Big Brother"의 예를 들기도 한다. 이 소설 속의 시민들은 Big Brohter가 수집한 방대한 양의 정보에 대하여 통제를 하지 못한다는 사실과 그 정보가 그들에게 어떻게 사용되는지에 대하여 두려움을 가진다. ”Big Brother“가 정부의 감시체체를 묘사한 것이기에, 학자들은 민간부문에서 개인정보를 수집하는 자를 "Little Brother"라고 칭한다. 이와 비슷한 맥락에서, 정보수집과 지배의 문제를 또한 Jeremy Bentham의 ”Panopticon(원형감옥)“에 비유하기도 한다.

한편, 예일대학 Solove 교수는 개인정보 문제는 Big Brother나 Panopticon보다 독일의 작가 Franz Kafka의 미완성 장편소설인 「심판(The Trial)」[1]에서 더욱 잘 묘사하고 있다고 지적한다. 소설 The Trial은 거대조직, 기업 또는 개인이 우리의 정보를 수집하고 이것을 그 개인의 이익에 반하여 사용하는 경우에 우리가 경험할 수 있는 무대책(helplessness)과 나약함(vulnerability)을 묘사하고 있다.

이와 같이 정보수집은 개인의 자유의지를 제한할 수 있으며, 이러한 사실은 모든 개인이 사생활에서 경험하게 된다. 개인정보(databases)의 문제는 힘의 균형이 정보주체로부터 개인정보를 수집하고 통제하는 실체(entities) 쪽으로 전환되는 것에서 나타난다. 즉 개인정보 문제는 개인의 자유를 제한하고, 고용인, 정부, 보험회사 및 기타 개인정보를 가지고 있는 주체들의 권능을 강화하는 감시의 일종이라고 볼 수 있다. 계속적인 감시를 통해서 언제든지 감시당할 수 있다는 가능성 하에서 생활하고 있다면, 사람들은 권력자가 원하는 행동을 하게 될 것이다.

---

1) 1914~1915년에 쓰여졌으며, 1925년 발간되었다. 은행원인 K. Joseph는 어느 날 아침, 잠자리를 급습당하고 자신이 체포되었다는 사실을 통고받는다. 혐의사실이라고는 전혀 짐작조차 가지 않았고, 또 당국에서도 아무런 말이 없었다. 행동의 자유는 허용된 상태였으므로 그는 여전히 은행원 생활을 계속하지만, 소재(所在)를 알 수 없는 재판소와 자신의 혐의를 알아내어 무죄를 입증하려는 안간힘 속에서 점차 기진맥진한 상태로 빠져든다. 그는 누가 그에 대한 정보를 가지고 있는지 그것이 무엇인지, 어떻게 사용되는지 알지 못했다.

이렇게 “개인정보가 어떠한 목적으로 사용될 것인지”에 대한 관심 때문에 정보프라이버시(database privacy 또는 information privacy)에 대한 정의로 가장 자주 인용되는 것이 “개인정보자기결정권(the right to control information about ourselves)”이다. 개인정보자기결정권이란 자신에 관한 정보가 언제 어떻게 그리고 어느 범위까지 타인에게 전달되고 이용될 수 있는지를 그 정보주체가 자율적으로 결정할 수 있는 권리를 의미한다.

2. 현행 법제도의 체계적 정비 필요

정보사회에서 정부 뿐만 아니라 기업과 개인 모두는 개인정보의 보호에 많은 관심을 기울이고 있다. 그럼에도 불구하고 많은 사람들이 자신의 정보처리에 대해서 보안이 미흡하며, 큰 도움이 되고 있다고 느끼고 있다. 이러한 감정은 현행 개인정보보호법제의 충분하지 못한 효율성에 대한 비판을 반영하고 있다고 보아도 과언이 아니다.

이제까지의 개인정보보호법제는 제한된 범위에 고착되어 있었다. 개인정보의 새로운 형태나 그 정보처리들을 충분하게 받아들이지 못하였으며, 정보처리의 새로운 기술들에 대한 위험과 기회들도 충분히 고려하지 못한 것이었다. 나아가 이제까지의 개인정보보호법제은 그 구성에 있어서 많은 모순점을 껴안고 있으며, 많은 특별법의 규범화에서도 일목요연하지도 않으며 집행하기도 어려웠다. 이러한 관점에서, 현대의 개인정보보호법제는 특정한 분야에 한정된 규정에 우선하는 일반법이 제정되어야만 한다. 이러한 일반법은 개인정보처리에 대한 원칙적이고 상세한 규정을 포함하여야 하고 가능한 한 자유재량 조항의 제정을 피해야만 한다.

현재 개인정보보호법제는 공공부문의 공공기관의개인정보보호에관한법률(이하 ‘공공기관개인정보법’이라 한다)과 민간부문의 정보통신망이용촉진및정보보호등에관한법률(이하 ‘정보통신망법’이라 한다)이 주축을 이루고 있다. 그러나 이 법들은 각각 공공·민간 부문에서 “불완전한” 일반법으로서의 역할을 담당하고 있을 뿐이다.

기술한 바와 같이 무엇보다도 어떤 법이 일반법의 역할을 다하기 위해서는 무엇보다도 해당 분야에서 통일적이고 체계적인 적용을 가능하게 하는 일반적 대원칙이 포함되

어 있어야 한다. 그리고 전문성이 요구되는 등 특별한 경우에 특별법 또는 개별법에서 예외가 인정될 수 있을 것이다. 이는 특별법으로서의 개별법은 가능한 한 이 일반원칙의 범위에서 벗어나지 않으면서 그 특수성을 발휘할 수 있어야 하며, 일반법의 원칙은 특별한 경우에만 그 적용의 예외가 인정되어야 함을 의미한다. 그 이유는 일반법의 기본원칙이 보장되고, 개별법에 산재하고 있는 예외 규정을 최소화됨으로써 법적 안정성과 법집행의 실효성을 확보할 수 있기 때문이다. 만약 일반적 원칙이 무시되고 주먹구구식의 개별법이 우선적으로 적용된다면 오히려 혼란만을 야기하게 될 것이다.

"개인정보 보호의 일반적 원칙"은 개인정보의 수집단계부터 그 이용 및 제3자 제공에 이르기까지 전 과정에 걸쳐 정보처리의 투명성을 확보할 수 있는 내용을 포함하고 있어야 한다. 그리고 이러한 기본원칙은 개인정보 보호에 관련한 모든 사항에 적용될 수 있어야 한다.

이러한 의미에서 공공기관개인정보법은 공공부문에서 일반법의 역할을 다하고 있지 못하다. 공공부문에서의 개인정보 수집과 사용 등은 개인정보보호에 관한 일반원칙이 통일적으로 적용되어야 할 필요성이 민간부문에서보다 더욱 요구되는 분야이다. 그럼에도 불구하고 개인정보 보호원칙이 통일적으로 적용되지 않는다 함은 일반법으로서의 성격의 존재를 의심케 한다.

한편, 정보통신망법은 민간부문에서의 일반법적 역할을 수행하기 위하여 OECD 가이드라인의 개인정보보호 원칙을 대부분 반영하여 규정하고 있다. 그러나 이 법 역시 일반법으로서의 역할을 제대로 수행하지 못하고 있다. 신용정보의이용및보호등에관한법률 등 각 개별법은 개인정보 보호에 관한 일반원칙을 규정하고 있지 않기 때문에 개인정보 보호 정도와 위반시 제재 정도의 균형이 맞지 않을뿐더러, 이들 개별법에 특별한 규정이 있는 경우에는 정보통신망법은 적용되지 아니한다(법 제5조). 즉 민간부문의 개인정보보호에 있어서도 일반원칙이 적용될 여지가 그만큼 축소되어 있다. 예컨대, 전자상거래등에서의소비자보호에관한법률(2002. 7. 1. 시행) 제11조는 소비자의 정보수집시 정보통신망법의 관련 규정에 따르도록 하고 있지만, 이를 위반한 경우에 대한 아무런 제재조항을 두고 있지 않다. 신용정보보호법 제13조는 신용정보업자 등이 신용정보를 수집·조사하는 경우 필요한 범위 안에서 합리적이고 공정한 수단에 의하도록 규정하고

있지만, 위반한 경우에 대하여 제재조항이 없다. 또한 전자서명법 제24조는 최소한의 정보를 수집하도록 하고, 이를 위반한 경우 500만원 이하의 과태료를 부과하고 있어 정보통신망법(1천만원 이하의 과태료)과 제재 정도가 상이하다. 결국 우리나라의 개인정보 보호 법제에서는 정보통신망법과 일부 관련법령을 제외하고는 개인정보의 수집시 정보주체의 동의여부에 관한 사항 등 개인정보의 일반원칙을 두고 있지 않으며, 유사한 사항에 대한 제재 내용도 상이하여 형평에 어긋나고 있다.

그리고 현행 법제 하에서 개별법의 규제대상에서 제외되고 있는 개인정보취급자(예컨대 비영리단체, Cable TV 사업자, 기업적 학습지 판매업자 기타 off-line 사업자 등)들에 대하여는 마땅한 제재수단이 없는 것이 현실이다. 또한 반대로 한 사업자가 여러 개별법의 규제대상에 해당하여 동일의 규제사항에 대하여 이중, 삼중으로 각기 다른 의무를 부담하여야 하는 불합리한 결과를 초래할 수 있음을 간과할 수 없다. 결국, 현행 정보통신망법은 민간부문에서의 개인정보보호의 일반원칙을 규정하고 있음에도 다른 법률에 의해 그 법적 효력을 상실하고 있는 것이다. 그리고 일반법이라고 하기에는 그 규율대상이 매우 한정되어 있다.

마지막으로 지적할 사항은, 개인정보처리의 투명성을 보장할 수 있는 독립적인 개인정보보호의 지도감독·권리구제 총괄기구의 설치를 위해서는 일반법 제정이 기본전제가 되어야 한다는 점이다. 현행법제의 개정만으로는 독립적으로 그 임무를 수행할 수 있는 개인정보보호를 위한 지도감독·피해구제 총괄기구를 설립할 수 없기 때문이다.

3. 정보사회의 변화와 국제사회의 요구 확대

정보통신기술의 발달은 국경을 초월한 상거래의 활성화를 이루었고, 이와 더불어 국가간 거래에서 개인정보의 유통이 자연스러운 현상이 되고 있다. 그러나 개인정보 유통의 글로벌화로 인하여 개인정보보호 수준이 무역장벽으로 등장하고 있다. 예컨대, OECD는 국가간 상이한 개인정보 법제도의 조화를 위해 "개인정보보호가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)"을 제정하여 이의 채택을 권고하였고, EU(유럽연합)은 OECD의 가이드라인을 한층 더 강화한 "개인정보의 처리 및 자유로운 전송에 관한 개인보호 지침(Directive 95/46/EC

on the protection of individuals with regards to the processing of personal data and the free movement of such data)"을 제정하여 EU회원국이 자국의 국내법에 이 지침의 내용을 입법화하는 것을 강제하였다. 미국은 EU회원국와 무역을 위하여 국제적 협약은 아니지만 합의사항으로서 "Safe Harbor 원칙"을 제정한 바 있다. 이처럼 세계환경에 있어서도 개인정보보호에 대한 국제적 협력과 적극적 참여가 중요한 과제로 부각되고 있다. 이에 따라 선진화된 개인정보보호법제의 정비는 국제무역과 국가위상에도 깊은 관계가 있다.

개인정보 보호시스템과 관련된 기술적 조치에 대해서

임 종 인
(고려대학교 정보보호대학원장)

순 서

E-gov. Act of 2002 ·····131

GAO Report on Privacy Act (June. 2003) ·····131

제언 ·····132

개인정보 보호시스템과 관련된 기술적 조치에 대해서

임 종 인
(고려대학교 정보보호대학원장)

E-gov. Act of 2002

- E-gov. Act를 통한 정보의 공유로 인하여 행정과 대국민 서비스의 효율이 향상되는 반면에 privacy 측면에서 커다란 우려가 제기됨.
- IT 기술개발, 제품구입, 개인 식별 정보 수집을 시작 할 때는 반드시 privacy impact assessment 와 information security를 우선 고려하도록 의무화.
- 2003년 4월까지 이와 관련한 implementation guideline을 발표하도록 OMB에게 의무화 시켰지만 현재까지 미발표.

GAO Report on Privacy Act (June. 2003)

- 정부 보유 문서 중 약 70%(2400종 가운데 12% 순수 전자형태, 58% combination)가 전자문서 형태를 띠고 있다.
- 문서의 전자화는 행정 효율을 크게 높여 주지만, 공유를 통한 타 부처 문서 획득시 최소 수집 원칙등 guideline 준수에 어려움 야기.
- 특히 cost-benefit라는 모호한 guideline은 computer-matching과 관련하여 수사권의 남용우려 제기.
- Privacy Act가 공포 된지(1974) 30년 가까이 지났지만, 환경과 기술의 변화로 여전히 실행부서 책임자들은 OMB의 leadership 부족, low priority, insufficient training to employee를 최우선 과제로 지적함.

제언

- 사적 영역과 공적 영역은 추구하는 목표와 가치가 다르다.
  부의 형성(사유재산권) ↔ public services
  Smith v. Phillsbury(1996) ↔ O ′ connor v. Ortega(1987)
- IT 관련 설비 보유와 수집정보량에 있어서 민간 영역은 정부를 압도하고 있음. (민간 80% 이상)
- 민간 영역에 개인 정보를 이용한 e-commerce의 발전은 지식 정보화 사회 발전의 가장 큰 추진력의 하나이다. 따라서 초기단계에서 너무 이상적이고, 과도한 규제를 도입하면 시장에 큰 장애가 될 수 있다.
- 사적 영역과 공적영역의 구분이 모호해지고, 수사기관 등의 민간 수집 정보에의 의존도가 커지고 있는 현실에 비추어 볼 때 견제와 균형이라는 대원칙을 살릴 수 있는 지혜 필요.
- Miller/Smith case에서 보듯 민간의 자발적 협조는 헌법상 보호를 받기 어렵기 때문에 data-mining 기법을 이용한 수사기관의 남용을 견제할 필요.
- 전통적인 법적 규제, 국제 협력을 통한 외교적 접근만으로는 부족
- 영국의 의료정보 project(BMA Model), Maryland 전자투표 시스템의 예에서 보듯
- 암호화, 접근 제어와 같은 기술 개발을 통한 접근, ISO, OECD ICCP, CCRA등 기술 정책적 접근이 반듯이 병행되어야 한다.
- 이와 같이 종합적이고 전문적인 접근을 요구하기 때문에 새로운 독립 위원회에 맡기는 것은 한계가 있다.

정보화사회에서의 인권
(토론요지문)

김 영 홍
(함께하는시민행동 정보인권국장)

순 서

1. 참여정부의 전자정부 로드맵에 대한 견해 ……135

2. 발제문에 관한 보충적인 견해 ……137

3. 맺는말 ……139

정보화사회에서의 인권 [토론요지문]

김 영 홍
(함께하는시민행동 정보인권국장)

1. 참여정부의 전자정부 로드맵에 대한 견해

국가인권위원회가 8월 19일 주최하는 '정보화사회에서의 인권' 토론회는 최근 발표된 참여정부의 전자정부 로드맵(이하 로드맵) 에 대하여 논하는 자리는 아니기 때문에 많은 이야기를 할 수 없지만 사회적인 현안이기 때문에 몇 가지 지적을 하고자 한다.

8월 14일 로드맵이 발표된 이후 정부혁신지방분권위원회(innovation.go.kr)는 문서 전문을 홈페이지에 올려놓았다. 전문이라고 불리우는 문서는 전자정부로드맵.ppt라는 문서명과 확장자를 갖고 있다. ppt 문서는 고가의 MS 소프트웨어를 구입하지 않은 이용자는 볼 수 없는 형태이며 , 뷰어프로그램을 설치하기 위해서 새로운 시간이 소비가 되고 프린트하기 위해서는 ppt 문서의 그래픽 특성상 과도한 잉크 낭비를 가지고 온다. 파워포인트만으로 제공되는 문서는 보편적인 정보 접근권을 가로막는 것이다. 보편적 정보접근권에 대한 별 고민 없어 보이는 문서 였기에 그 내용을 의심의 눈으로 볼 수 밖에 없었다. 윈도우 사용자들을 위한 전자정부시스템이 아니며 네이스와 같은 갈등들이 로드맵에서는 나타나지 않을 수 있을까? 우리는 8월 14일 참여정부의 "세계최고수준의 열린 전자정부 구현"이라는 로드맵이 기존의 의구심을 해소할 것이라는 확신을 갖고 있지 못하다. "프라이버시 문제는 '행정의 효율성' '경제성' '기업활동'의 이해관계로 인하여 뒷전에 밀리는 경우가 많았기 때문이다.

국가에는 수많은 정보를 수집하고 그 정보들을 취합, 분석하여 새로운 정보들을 생산하며, 전자화된 사회에서는 더더욱 이러한 정보를 바탕으로 개인과 대중을 통제하는 강력한 수단으로 삼을 수 있다. 그러나 개인을 충분히 보호 해주지 못하는 관습과 관행, 법제를 갖고 있는 상태에서 무리하게 전자정부를 추진하는 해왔던 것이 수년째이다. 정보통신부의 '정보화촉진기본계획'이나 행정자치부의 '행정정보화촉진시행계획' 등은 행정의 효율성과 투명성을 강조하고 산업의 활성화 청사진을 그리지만 개인의 사적 정보

의 집적과 연계, 공동이용이 가져오는 위험에 대하여 중요하게 다루지 않아 왔다.

로드맵은 보다 많은 행정정보 공유, DB간의 연계계획을 내놓고 있다. 또한, 2007년부터는 금융기관과 전산망을 공동이용하는 계획도 세우고 있다. 모두 면밀히 살펴 볼 것들이지만 고용, 취업종합서비스 로드맵 중 '학교-직장간 이동경로 분석 서비스'를 하겠다는 계획이 유독 눈에 띈다. 그 자세한 내용을 확인할 수는 없지만 심히 우려스러운 계획이다. 국가가 국민을 통제하려는 의도로 전자정부 계획을 세우고 있다고는 생각하지 않는다. 그러나 의도와 다르게 왜곡이 심각하게 예견된다면 사전적인 위험들은 제거가 되어야 할 것이다. 취업을 도와주고 노동시장의 안정을 위한 계획이겠지만 '학교-직장'간 서열화, 그릇된 관행의 고착화, 프라이버시권의 심각한 훼손이 우려는 없는지 사전적으로 검토되어야 한다.

함께하는시민행동에서는 현재, 정부가 공개한 개인정보화일 분석 작업을 하고 있으며 이와 별개로 참여정부의 로드맵에 대하여 추후 의견서를 제출할 예정이다. 그러나 시민단체가 모니터하고 감시하기에는 부족한 것들이 많다. 어떤 부분은 자세한 문제제기와 대안을 내놓을 수 있지만 한정된 자원으로 로드맵을 명쾌히 분석하기에는 역부족일 것이다. 즉, 로드맵은 어떤 단체의 모니터 대상에 앞서 프라이버시 영양평가의 대상이라는 것이다. '네이스' 문제처럼 이미 예산을 투여한 후 아까워서 발동동 구르며 갈피를 못잡는 정부 모습은 다시 보고 싶지 않다. 국가인권위원회는 "헌법 제10조 및 제17조, 헌법 제31조, 헌법 제37조, 세계인권선언 제12조, 시민적·정치적권리에관한국제규약 제17조, 아동의권리에관한협약 제16조, 개인데이터의국제유통과프라이버시보호에관한가이드라인(OECD가이드라인) 및 전자화된개인정보와관련된규정을위한UN가이드라인과 현행 공공기관의개인정보보호에관한법률(개인정보보호법) 등에 의거하여 네이스에 대한 권고안을 제출한 바 가 있다. 로드맵은 인권위가 조사 했던 것 보다 더 많은 관점과 조사, 분석이 필요할 것이다. 프라이버시 영양평가는 로드맵이 가지는 프라이버시 차원의 정치, 사회적 함의를 조사하고, 개인 프라이버시에 어떠한 영향을 주는지를 밝혀 계획에 충분한 영향을 주워야 한다. 설계에 대하여 안전진단도 없이 올라가는 빌딩이 있다면 사회구성원들은 막아야할 권리가 있다. 로드맵도 마찬가지이다. 계획 세워놓고 시간에 맞춰 일사천리로 진행된다면 곤란하다. 다양한 함의를 조사할 수 있는 전문가들이 적절한 논의 틀, 시간과 권한을 가지고 로드맵에 관한 '프라이버시 영양 평가'를 수행해야 한다.

2. 발제문에 관한 보충적인 견해

1) '공공기관의개인정보보호에관한법률' 제7조(개인정보화일의 공고)에 의하여 2002년 개인정보화일 목록집을 발간한 바가 있다. 이 목록집에는 중앙행정기관 114건, 지방자치단체198건, 교육청 및 각급학교 20건, 정부투자기관 및 기타 260건 이 수록되어 있다. 이 목록집은 공공기관이 보유하고 있는 전체 개인정보화일을 보여 주고 있지는 않다. 목록집으로 보면 국방부, 법무부, 국정원 등에 어떤 종류의 개인정보화일목록이 존재하는지 알 수 없다. 공공기관이 보유하고 있는 개인정보화일을 무척 방대하지만 모든 개인정보 화일에는 개인 아이디인 주민등록번호가 수록되어 있기 때문에 보다 쉽게 개인 정보를 분류할 수 있는 조건을 갖고 있다. 동법 6조(사전통보)를 통하여 공공기관의 장이 개인정보화일을 보유하고자 하는 경우에는 중앙행정기관의 장은 다음 각호의 사항을 행정자치부장관에게 통보하게 되어 있지만 예외조항을 두고 있다. 특히, "국가의 안전 및 외교상의 비밀 기타 국가의 중대한 이익에 관한 사항을 기록한 개인정보화일", "보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보화일" 등등은 추상적이기 때문에 자기정보통제권이 무시되는 광범위한 사각지대가 존재하는 것이다. 주민등록법은 인격체 마다 고유 번호를 부여하는 법으로 위헌적인 법이라는 지적을 받아왔다. 주민등록번호 변경의 권리, 주민등록번호를 부여를 거부할 수 있는 권리, 다른 신분 인증 방법 활성화, 주민등록번호 사용 목적의 명확성, 주민등록번호를 통하여 생년월일-성별-지역을 확인 할 수 없는 체제로의 전환, 지문날인 거부권 등등을 고려하여 주민등록법을 폐지, 혹은 개정해야만 한다. 주민등록법이 현재처럼 존속되는 상태에서의 프라이버시권은 언제나 위협받게 될 것이다.

2) 프라이버시권의 핵심 중의 하나는 익명권이다. 개인이 선택적인 판단에 따라 실명과 익명을 사용할 수 있어야 한다. 익명권은 개인의 자유의지 영역이기 때문에 보장받아야 하며 익명권은 사회적으로 차별받는 소수자의 권리 향상이나 내부자 고발을 보호하는 등의 순기능을 가진다.

현재, 수많은 커뮤니티에서 회원서비스, 실명서비스를 통하여 많은 게시판이 실명화 되어 왔다. 공공기관의 경우 수많은 게시판 중 일부만 익명성을 부분적으로 보장하고 있을 뿐이다. 그러나 정보통신부에서는 '인터넷게시판 실명제'라는 인권 침

해적인 정책을 펴고 있는 중이다. 법의 보호가 필요한 거래와 같이 신분을 증명해야만 이용할 수 있는 서비스들은 광범위하게 실명화 되어 있다. 인터넷에 익명만이 존재하는 것처럼 정보통신부는 주장하지만 실제로는 실명과 익명이 공존하고 있다. 익명과 실명이 공존하는 것이 자연스러운 것이다.
특히, 인터넷에서의 익명성은 네트워크의 기술적 특성상 IP추적을 통하여 쉽게 익명성을 침해받을 소지가 있기 때문에 공공영역은 오히려 익명성을 보호하고 보장하는 규범과 제도를 연구해야할 입장에 있다.

3) 현재 함께하는시민행동은 경찰 및 지방자치단체에서 운영되고 있는 CCTV 현황을 파악중에 있다. 공공의 안전을 위해 감시카메라가 필요한 부분은 사회적 합의와 공감대에 따라 운영되어야 하며 제도적 안전장치가 꼭 필요하다. 현재, 카메라 서버같은 기술적 진보는 카메라의 네트워크를 가능하게 하고 있다. 그렇기 때문에 화상정보의 데이터간 매칭을 엄격히 제한 해야할 것이다. 그리고 첫째 설치, 관리, 유지와 관련하여 그 주체를 분명히 밝혀야 하며, 둘째. 목적이 명확한 규정, 셋째. 촬영할 수 있는 범위를 제한, 넷째. 운영 권한, 촬영된 자료에 대해서 접근할 수 있는 권한 및 저장된 자료의 관리에 대한 구제척 규정 필요. 다섯째. 설치에 대한 사전, 사후 고지 의무 및 동의절차에 대한 규정 필요. 여섯째. CCTV 운영에 대한 역감시권이 보장되어야 한다. 위와 같은 내용들이 제도적으로 보장되어야 할 것이다.

4) 개인이 갖는 사적 정보들은 기업에 의해서 재산적 가치를 갖게 된다. 아마존 닷컴의 프라이버시 보호정책을 보면 고객정보는 자신의 자산이라고 말하고 있다. 특히, 학술적 목적으로 이용되는 개인의 의료, 유전적 정보들은 기업에 의해 지적재산권으로 가공되기도 한다. 즉, 정보를 독점하는 시스템은 이미 구조화되어 있다는 것이다. 학술적 목적으로 수집된 정보라도 독점적인 점유를 획득 할 수 있기 때문에 개인이 가지는 생체 정보마저도 어떤 특정 개인, 기업에게는 경제적 가치가 된다. 학술활동에서 혹은, 의료활동에서 얻게된 개인의 특별한 정보들은 지적재산권으로 변화되어 프라이버시의 어떤 부분을 침해하고 있다고 볼 수 있다. 공공의 이익, 기업의 이익, 개인의 이익이 균형을 이루지 못하고 지적독점, 정보독점과 같은 일방에 흐른다면 필연적으로 갈등이 심화 될 것이다.

3. 맺는말

‘정보사회’라는 것은 다분히 현재진행형이고 변화가 매우 빠르기 때문에 법과 현실의 괴리가 계속되고 있다. 특히, ‘개인정보’를 재산권 측면에서 다루는 정통망법이나 ‘개인정보’의 전자화된 부분만을 다루는 ‘정보보호법’은 프라이버시에 관한 사회적 가치를 혼란스럽게 하고 있다. 공공영역과 민간영역을 구분하지 않고 ‘인권’에 기반한 개인정보보호 일반법이 필요하며, 독립적인 위원회로 하여금 개인정보보호를 위한 호민관 역할을 부여해야 한다. 호민관의 역할 중의 하나는 프라이버시에 관한 사회적인 사안을 조사하고 프라이버시 영양평가제를 실시하여 인권을 위협하는 시도들은 중단시켜야 할 것이다.

한국사회의 정보인권의 현실

장 여 경
(진보네트워크센터 정책국장)

순 서

1. 기술적 차원 ……143
2. 권력관계의 차원 ……144
3. 역사적 차원 ……146
4. 제도적 과제 ……148

한국사회의 정보인권의 현실

장 여 경
(진보네트워크센터 정책국장)

'정보사회 세계정상회의'(WSIS) 파리 임시회의에서 인권 활동가들은 "기본으로 돌아가라"(BACK TO BASICS: WSIS and HUMAN RIGHTS)는 제목의 성명을 발표했다. 결국 정보 인권은 정보화 시대에도 세계인권선언 이하 인권이 보장받아야 한다는 매우 소박한 주장이다. 그러나 네이스를 둘러싼 논쟁의 진동폭이 격렬한 것처럼 한국 사회에서 정보 인권을 보장하기 위한 길이 순탄해 보이지는 않는다.

정보 인권에 대한 위협은 기술적 차원, 권력관계의 차원, 역사적 차원의 현실이다.

1. 기술적 차원

이를테면 신체의 자유가 처한 상황을 보자. 국민을 체포·구속·압수·수색할 때에는 법관이 발부한 영장을 제시해야 한다는 것이 영장주의 원칙이다. 하지만 이제 경찰은 국민을 수색할 때 굳이 영장을 제시하지 않는다. 카메라와 데이터베이스를 사용하기 때문이다.

2001년 미국 경찰은 얼굴인식기술을 사용해 미식축구 결승전을 보려고 모여든 수천 명의 관중 가운데 19명의 수배자를 아주 간단하게 검거했다. 경찰은 관중이 경기장에 입장할 때마다 얼굴을 촬영하여 경기가 진행되는 동안 데이터베이스와 신속하게 대조했고 경기가 끝났을 때 퇴장하는 관중 가운데 수배자를 손쉽게 골라내었다. 이 과정은 수배자를 검거한다는 명목으로 수천 명의 사람들을 혐의자 신분으로 수색하고 조사하는 과정이었지만 "실례합니다. 잠시 검문 있겠습니다" 따위의 양해조차 필요하지 않았다. 한편 정보통신부가 추진하려다 중단한 인터넷 실명제는 표현의 자유 문제와 별개로, 문제 소지가 있는 글에 대해서 글쓴이를 추적하겠다는 것에서 영장주의 원칙이 역시 문제가 된다. 여기서 추적이란 실명과 주민등록번호를 사용해 신원을 파악하고 조사하겠다는 것이다. 이는 일종의 수색 과정이지만 역시 영장 없이 진행된다. 은밀하고 편

리하다. 상황을 다소 과장해보자면 시청 앞에 모인 집회 군중을 감시하기 위해 과거에는 불심 검문을 하고 사복 경찰을 동원했지만 이제는 그럴 필요가 없다. 그저 시청 앞에서 잡히는 핸드폰 위치 정보만 수집하면 이들의 신원을 자동으로 파악할 수 있기 때문이다.

즉 오늘날 정보통신 기술은 신체의 자유와 밀접한 문제이며 신체의 자유 뿐 아니라 모든 인권에 위협적인 존재가 되어가고 있다.

그러나 이와 같은 경향이 일반화되어 가고 있는데도 그에 대한 사회적 제지는 물론 문제 의식조차 미미하다. 기술이 너무 빠른 속도로, 이미 '실질적 수준'에서 인권의 원칙을 무시하고 고안되고 생산되고 사용되기 때문이다. 무엇보다 우리 사회를 지배하고 있는 기술경제주의적 경향이 인권을 매우 부차적인 것으로 치부하고 있다. "빠르고 편리하다"는 논리가 "인권을 침해한다"는 논리와 나란히 비교되거나 심지어 압도한다.

물론 이와 같은 반인권적 상황의 도래는 기술 그 자체 때문은 아니다. 기술은 사회적으로 형성되는 사물이기 때문이다. 그러나 한번 정착한 기술은 내재한 정치성을 발휘하는 견고한 사물이 된다는 점에서 기술의 반인권적 잠재성에 대해 충분히 경계할 필요가 있다. 무엇보다 기술의 논리 - '속도의 논리'와 '경제성의 논리'가 인권 침해를 정당화하고 있다는 점을 간과해서는 안된다.

2. 권력관계의 차원

최근 CCTV로 인한 인권침해 논란이 한창이다. CCTV가 침해하는 것으로 지목받은 인권은 프라이버시권이다. 세계인권선언에서 프라이버시권은 사생활을 침해받지 않을 권리와 자유로운 통신과 그 비밀을 보장받을 수 있는 자유를 소극적으로 의미했다면, 1980년 경제협력개발기구(OECD)가 <프라이버시 가이드라인>을 발표한 이후 프라이버시권이란 자기 정보를 수집하고 저장하고 전달하는 행위에 대한 정보 주체의 결정권으로 정리되었다. 그래서 '감시'란 일반적으로 정보 주체의 동의를 받지 않고 개인정보를 수집하고 집적하는 행위를 일컫는다. 이런 점에서 우리 사회는 분명 감시 무법지대이다. 어디에 카메라를 설치하건 테이프나 파일을 어디에 얼마동안 보관하건 누구에게 넘기건 그저 카메라 주인 맘이다. 공공장소에, 특히 수사 목적으로 CCTV를 설치할 때는 까다로운 요건을 갖추도록 제한한 다른 나라의 경우와 너무 차이가 난다. 따라서 찍히

는 사람의 자기정보통제권을 보장하는 법과 제도를 마련하는 것은 대한민국에서 프라이버시권을 보호하기 위한 최소한의 사회적 장치이다.

그러나 만일 CCTV에 의해 감시당하는 것을 기꺼이 선택한다면? 그렇다면 CCTV는 정당화될 수 있는가? 강남구 주민들의 80%가 CCTV 도입을 찬성했다고 한다. 이들은 CCTV에 촬영되는 대가로 자기 재산에 대한 안전을 보장받길 원한다. 자기 정보를 제공하는 대신 경제적인 보상을 받는 것이다. 여기서 감시는 선택적인 문제인 것처럼 보인다.

하지만 감시는 순수한 개인적 선택의 영역에 있는 문제가 아니다. 감시에 대한 수용 여부는 사실 권력에 대한 태도에서 유래한다. 똑같은 카메라 감시의 문제인데도 강남 CCTV에 대한 반응이 얼마 전까지 문제되었던 카메라폰에 대한 대응과 매우 다르게 전개된 것도 이 때문이다. 카메라폰에 대한 규제 입법 논의는 매우 신속하게 이루어졌다. 하지만 경찰이나 지방자치단체의 CCTV에는 같은 논리가 적용되지 않았다. 다른 개인이 나의 프라이버시를 침해하는 것은 용납하지 못하지만 경찰이나 지방자치단체의 권력에는 순응할 수 있기 때문이다.

감시에 대해 동의하거나 거부할 수 있는 권리도 권력관계에 의해 제한된다. 고용관계에 매여 있는 노동자는 CCTV를 '선택'할 수 없다. 단지 강요받을 뿐이다. 감시의 효과 또한 권력 관계로 나타난다. 우리보다 먼저 CCTV 논쟁을 겪었던 영국의 경우 '범죄 이전' 효과에 대한 논쟁이 아직도 계속되고 있다. 분명 CCTV는 특정 지역에서의 범죄율은 저하시켰지만 전체적인 범죄율은 변화가 없었으며 결국 범죄를 다른 지역으로 이전시켰을 뿐이라는 주장이 제기되었던 것이다. 그런데 이런 범죄 이전 효과는 결국 '청정구역'과 '우범 지역'을 철저하게 나누는 결과를 가져 왔다고 한다. 이는 곧 신보수주의 영국 사회에서 사회 계층의 분리와 양극화 현상의 한 지표이기도 하다.

결국 감시의 궁극적인 효과는 사회적 분리와 배제, 그리고 차별이다. 비록 지금은 추진이 중지되었지만 천호동에 설치될 뻔한 CCTV가 가져왔을 효과는 성매매 여성들의 영원한 사회적 격리이다. 호주 정부가 1980년대 전자주민카드를 추진했을 때 그들이 내세웠던 명분도 '불법 이민'에 대한 철저한 적발과 소탕이었다.

하지만 감시를 거부하는 것은 쉽지 않은 문제이다. 정보사회 프라이버시의 문제는 내가 감시망에 포함되어 있지 않으면 존재하지 않는 것으로 간주되는 역설에서 발생한다. 미국은 얼마전 유학생・교환방문자 정보시스템(SEVIS)에 등록되지 않은 사람은 입국을 불허한다고 발표했다. SEVIS에 등록되어 있는 사람은 향후 준테러범으로 미국 정부에

의해서 감시받겠지만 등록되지 않으면 아예 미국에 입국할 수 없다. 데이타베이스에 들어가면 감시받고 데이타베이스에 들어가지 않으면 차별받는 것이다. 그리고 나는 나의 결백을, 기록으로서만 입증할 수 있다. 프라이버시 학자들이 경고한 바로 그대로, 나는 오로지 감시당함으로써 나의 결백을, 더 나아가 나의 존재를 주장할 수 있는 상황이 된 것이다.

그래서 CCTV 감시의 문제는 단지 한 지역의 문제가 아니라 궁극적인 권력관계의 문제이기도 하며 더 나아가 이 사회 전체의 민주주의와 진보에 대한 문제이기도 하다. 감시가 많아질수록 얼마나 많은 사회적 배제와 차별이 생겨날지를 생각해 보아야 한다. 프라이버시권 또한 더이상 23년전 OECD가 천명한 자기정보에 대한 개인적인 결정권의 문제로 국한되지 않는다. 감시를 거부할 수 있는 사회적 권리가 꼭 필요한 시대가 되었기 때문이다.

3. 역사적 차원

NEIS를 비롯한 전자정부를 추진하는 데 있어 정부는 정보화의 '효율성'에 가장 큰 우선 순위를 두고 있다. 정부가 펴낸 전자정부에 대한 해설자료에서 전자정부의 미래상으로 "문서의 생산에서 보존까지 전자화를 통한 종이 없는 행정, 전자화된 행정정보가 물 흐르듯 유통되는 신속한 행정, 행정정보의 축적 활용을 통한 지식행정 등에 의한 '생산성 있는 행정'"을 첫 번째로 꼽고 있는 것이 그 예이다. NEIS에서만 하더라도 똑같은 '개인정보 보호'라는 화두에 대하여 정부는 효율성에 뒤따르는 개념으로 치부하거나 사후에 기술적인 '보안' 조치를 통해 해결할 수 있는 것으로 생각하는 것 같다.

물론 프라이버시권 등 헌법에서 보장하고 있는 국민의 기본권은 정보화 과정에서도 보장되어야 하며 인권이 행정의 효율성에 뒷전일 수 없다. 하지만 우리의 정보화 정책 대다수가 국민의 정보 인권은 커녕 어떤 경우엔 현행 법률로 보장해 온 권리조차 무시하면서 오로지 앞만 보고 달려온 것이 사실이다. 한국의 정보화는 세계 1,2위를 다툴 만큼 빠른 속도로 확산되어 왔지만, 정보 사회에서 국민의 인권을 어떻게 보장할 것인가에 대한 사회적 고민과 토론, 그리고 제도 개발은 전무하다시피 하다.

인권을 후대시한 것이 어찌 최근에서만의 일이랴. 정보화는 한국의 압축적이고 왜곡된 근대화 과정의 연장선이자 반복선 상의 과정이다. 실제로 정보화에 대한 국가적 이

니셔티브는 “산업화는 늦었지만 정보화는 앞서가자”는 캐치프레이즈였다.

현재 국민의 프라이버시보호를 가장 중대하게 위협하고 있는 것은 방대한 주민(국민)등록제도와 주민등록번호이다. 이미 개인정보 유출에 대한 두려움은 국민적이다. 정부는 이 문제를 무지에 의한 것으로 폄하하거나 기술에 의해 해결될 수 있는 문제로 말할 수 없다. 한국의 개인정보 유출 사고는 개별적으로는 기술적 오류 때문에 발생하기도 하지만 전체적으로 박정희 독재정부 때 도입한 주민등록번호를 토대로 한 개인정보 수집 구조에서 기인한, 전세계 유래없는 빈발성과 규모를 자랑한다. 주민등록번호는 국민마다 고유하게 부여되는 국민식별번호로서 한번 유출되면 그 피해를 돌이킬 수 없기 때문에 다른 나라에서는 아예 비공개하거나 복지 등 제한적인 목적으로만 사용하는 ‘민감한 개인정보’이다. 그런데 우리는 누구나 주민등록번호를 수집하도록 방치하고 있기 때문에 비싼 보안 기술을 도입해 봐야 개인정보가 유출될 수 밖에 없는 구조인 것이다. 시장과 전자정부 모든 곳에서 주민등록번호가 기준자(matching field)로서 여러 개인정보 데이터베이스를 서로 연동하고 통합하면서 인권 침해가 확대재생산되고 있다.

결국 한국사회의 정보 인권을 가장 크게 위협하고 있는 것은 우리의 역사성이다. 효율성으로만 따지자면 독재보다 더한 것이 있을 수 없다는 경고가 있다. 민주주의와 인권의 원칙을 고려하지 않는 기술 집중적 시스템은 독재나 마찬가지이다. 인권을 고려하지 않는 정보화란 민주주의와 괴리된 기술이 불균형하고 비대하게 발달하는 상태이며 더 나아가 민주주의 그 자체에 대한 위협일 수 있다.

이런 상황은 정보화 시대에 국민의 정보 인권이 보장되지 않을 경우 민주주의의 가치 자체가 위협받을 수도 있음을 의미한다. NEIS를 둘러싼 논란에서 우리가 배워야 할 교훈은, 이제 우리 국민은 자신의 권리를 무시하는 정보화를 더 이상 방관하지 않는다는 것이다. 국민의 정보 인권을 무시한 눈먼 정보화는 결국 국민 개개인에 대한 불행이자 이 사회의 커다란 재앙이 될 것이기 때문이다. 이 점을 전자정부를 추진하는 정부 입안자들은 명심해야 한다.

정보화 시대의 인권은 정보화 시대에도 개인의 자유와 평등을 보장받기 위한 최소한의 권리이기도 하지만 정보화하고 있는 우리 사회를 민주화하기 위해 매우 중요한 이념이기도 하다. 따라서 정보화의 목표는 이 사회의 민주주의를 증진하고 인권을 옹호하기 위한 것임이 우선적으로 설정해야 한다. 인권은 정보화라는 명분으로도 희생되거나 양보될 수 없으며 오히려 정보화가 인권의 원칙 하에서 철저한 평가의 대상이 되어야 한다.

4. 제도적 과제

정보 인권은 정보화와 커뮤니케이션과 관련이 있기 때문에 국민이 정보화 시대에 자유롭고 평등하기 위해서 필수적으로 보장받아야 하는 권리이기도 하지만 정보화로 인하여 위협받고 있는 권리이기도 하다.

원래 인터넷 등 디지털 매체가 확산되면서 표현의 자유나 정보 공유의 권리는 더욱 확장될 것으로 기대되었다. 표현의 자유나 정보 공유의 권리는 정보화 이전에도 세계인권선언 등 인권 관련 국제 협약에서 인정되어 온 기본적 인권이고 대부분의 나라는 이를 국민의 기본권으로서 헌법적 수준에서 보장하고 있다. 하지만 최근 확산되고 있는 국민의 표현을 통제하려는 권력의 의지가 오히려 표현의 자유를 위축시키고 있으며 디지털 지적재산권을 강화하려는 산업 논리가 그간 마땅한 것으로 인정되어 온 정보의 비영리적이고 사적인 공정한 이용(fair use)조차 위협하고 있다. 특히 국가의 기반시설(infrastructure)이나 다름없어진 운영체제(OS) 소프트웨어가 특정 국가의 특정 업체에 의해 독점되고 있는 현실은 단순히 시장 논리로는 정당화되기 힘든, 국민의 권리에 대한 위협이다.

한편 프라이버시권과 알 권리, 그리고 접근권은 기존의 권리 개념을 정보화 시대에 더욱 발전시킬 것을 요구받고 있는 권리 개념이다. 예컨대 정보의 접근권은 과거 통신시설 등 국가의 기반시설에 대해 국민 누구나 저렴한 비용으로 제한 없이 사용할 수 있어야 한다는 보편적 서비스(universal service)의 개념이 정보통신기술의 발전으로 다양해진 미디어에 대해 보다 적극적인 국민의 공적 접근(public access)을 보장하는 개념으로 변화·발전하고 있다. 특히 공공 정보에 대한 국민의 알 권리를 보장할 것이 요구되고 있다.

올해 12월 UN은 처음으로 정보 사회 세계정상회의(WSIS)를 개최하고 이 자리에서 세계 정상들의 정보 사회에 대한 선언문을 발표할 계획이다. 그런데 지금까지 정보 사회 세계정상회의 준비 과정에서 나온 여러 문서에서 정보 사회가 인권을 보장해야 한다고 명시하고 있다는 점은 주목할 만 하다. 선언문 초안에서는 제1항에 “정보 사회를 건설하는 데 있어 UN 헌장과 세계인권선언에 명시된 원칙을 전제”한다고 천명하고 있다. 또한 정보 사회 세계정상회의가 민주주의를 증진시키고 표현의 자유와 정보 획득과 전달의 권리 등 국제적으로 인정된 인권과 기본권을 보장해야 한다고 확인하고 있다. 이제 정보 사회에 있어서 인권의 문제는 국제적 과제인 것이다.

하지만 1997년 전자주민카드, 그리고 2000년 전자건강카드 논쟁을 거쳤음에도 우리 사회가 정보 인권에 대해 비슷한 논란을 반복하고 있는 것은 정보 인권을 보장하기 위한 제도적 노력이 부족했기 때문이다. 정보 사회의 인권 침해를 방지하기 위해서는 이를 위한 법과 제도가 개발되어야 하는 것이다. 특히 최근 많은 국민들이 관심을 보이고 있는 프라이버시권 침해에 대해서는 한시바삐 프라이버시를 보호하기 위한 법률과 기구를 마련해야 한다.

우리와 달리 여러 나라가 이미 1980년대부터 프라이버시보호법과 기구를 도입해 왔고 전자정부 또한 이런 원칙 하에서 추진되고 있다. 이를테면 프랑스에서는 정부가 구축하는 모든 국민의 개인정보 데이타베이스가 프라이버시위원회의 심사를 받는다. 우리처럼 전자주민카드의 도입을 두고 정부와 시민사회가 맞섰던 호주는 이 논쟁의 끝에 프라이버시보호법을 제정하고 프라이버시위원회가 활발히 활동하도록 하여 NEIS를 국민의 정보 인권과 조화시키도록 노력했다. 여러 나라에서 전자정부나 정보화 기술이 국민의 정보 인권과 사회에 미치는 영향을 평가하고 심사하는 제도를 도입하고 있다.

물론 우리나라의 일부 법률들에서는 OECD 프라이버시 가이드라인의 원칙을 부분적으로 도입하고 있다. 그러나 NEIS에서 기본적인 개인정보 수집에 대한 원칙조차 논란의 대상이 된 것은, 무엇이 개인정보이고 개인정보보호란 무엇을 의미하는지에 대한 사회전체적인 총론과 합의가 없다는 것을 반증한다.

여러 사회인권단체들이 NEIS 문제가 불거지기 이전부터 주민등록제도, 노동감시 등 증가하고 있는 여러 프라이버시 침해 문제에 대해 대응해 오며 프라이버시보호를 위한 법과 기구의 도입을 주장해 왔고 구체적인 법률적 논의도 진행해 왔다. 이제 이에 대한 국가적인 검토와 토론을 시작할 때이다. 정보화를 국민의 인권 영역으로 돌리기 위한 시도는 더 이상 늦춰질 수 없다. 전자정부에 대한 법률 등 기본적인 정보화와 관련한 법률들에서도 인권과 민주주의를 보장하기 위한 원칙을 구체적으로 명시해야 한다.