2006 | 연구보고서

해외사례 연구를 통한 사설정보지 문제 대응방안 연구

치안정책연구소
POLICE SCIENCE INSTITUTE

해외사례 연구를 통한 사설정보지 문제 대응방안 연구

2006. 6.

연구자 : 김 상 회(국민대학교 교양과정부 교수)

치 안 정 책 연 구 소 장 귀 하

목 차

V. 해외사례 연구

V-1. 36개국 cross-country analysis

V-2. 5개국 사례연구(case-studies)

V-2-1. 미국

V-2-2, 영국

V-2-3. 프랑스

V-2-4. 일본

V-2-5. 싱가포르

V-3, 사례연구의 분석결과

VI. 정책과제

VI-1. 정책의 방향

VI-2. 공공재(public good)로서의 정보의 확대

VI-3. 산.학.정 (産.學.政) 공동체제

VI-4. 정부 정보공개의 확대

VI-5. 민영화와 외부제작(privatization and outsourcing)

VI-6. 자율규제에 의한 프라이버시 보호

VI-7. 사생활권과 공공성의 조화

V-8I. '국민의 알 권리' 와 '국가의 감출 권리'

I. 연구개요

I-1. 연구목적

현재 우리사회는 지난 '연예인 X파일' 파동이 보여주듯이 무분별하게 난립된 사설정보기관과 유사정보기관, 그리고 기존 연구소와 여론조사기관들의 정보수집과 유통 그리고 소비로 인하여 광범위한 개인적 선의의 피해자 양산은 물론 사회적 불신풍조의 만연에 따른 사회불안, 그리고 국가경제적 피해와 심지어는 국제적 분쟁까지도 야기되고 있는 실정이다.

흔히 지식정보화 시대 혹은 정보사회(information society)라고 불리는 현대사회에서 새로운 정보의 가치와 필요성, 그리고 그의 효과적 유통과 소비를 통한 소비는 사회경제 발전을 위하여 필수불가결의 요소로 인식된다.[1] 또한 민주화와 자유화의 세계적 추세에 따라 특정정보를 특정의 공공기관이 독점적이고 우월적 지위를 통하여 공급과 소비하는 것도 사회적으로 부적절한 시점에 도달하고 있다.

이러한 시대적 환경 속에서 폭발적으로 증대하는 정보가 사회적으로 순기능을 담당하고, 개인적 피해를 최소화하며, 동시에 새로운 정보의 가공과 창출에 기여할 수 있는 정보의 생산과 소비에 관한 사회적 합의와 제도적 장치마련은 현재 우리사회의 시급한 해결과제 중의 하나로 대두되고 있다.

본 연구는 이러한 우리사회의 시급한 필요에 부응하기 위하여 현재 우리사회의 정보이용과 수집, 그리고 유통과정의 문제점을 적시하고, 이에 바탕을 두고 그 해결방안과 법적, 제도적 보완책을 마련하는 하나의 준거틀을 제공하는 데 둔다.

I-2. 연구의 범위

사설정보산업(private intelligence service)이라 함은 공공정보(public intelligence)를 제외한 모든 사적인 영역에서 생산, 수집, 유통되는 정보의

---

1) James Bebiger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Harvard University Press, 1992)
Wendy Rurrie, *The Global Information Society* (Beacon, 2001)

통칭으로, 사설정보업의 발달은 위에서 살펴본 정보화, 세계화, 그리고 민간화(privatization) 시대에 수반되는 전세계적인 현상이다.

사설정보는 정치, 경제, 사회, 군사, 문화, 과학기술 등 전 영역에 걸쳐 발생하며, 특정 목적에 따라 자료수집(data warehousing), 경제정보(business intelligence), 정보 브로커(information brokerage), 독립 정보연구(independent information researching)등 다양한 명칭으로 활동하고 있으며, 사설경호(private security)와 사설탐정(private investigator; private detective) 역시 이 범주에 포함된다. 우리사회에서는 과거 전통적인 흥신소와 심부름센터 역시 이 범주에 포함된다.

권위주의 통치와 불확실성과 불안의 시대에 흔히 나타나는 과거의 소위 '카더라 통신'이라고 불리운 '유언비어'의 은밀한 확산도 인터넷 시대에 다양한 '소문 사이트(rumor site)의 형태로 과거와는 비교할 수 없을 정도로 신속하고 광범위하게 사회전체로 확산되고 있으며, 우리사회에서도 IT 매체의 급속한 발전에 따라 많은 미확인 소문들이 인터넷을 통하여 급속히 확산되고 있다. 이러한 rumor 역시 또한 넓은 의미에서의 사설정보에 해당된다.

최근 上記한 다양한 형태의 사설 정보업이 다양한 형식과 명칭으로 운영되고 있으며, 외국의 경우와 마찬가지로 대규모 기업형 사설정보기관으로 발전하고 있기도 하다.

현재 우리사회의 사설정보업은 외국의 경우와는 달리 독립적이고, 공식적인 정보연구소(information researching company)나 정보 브로커(information brokerage)로 운영되기 보다는 각종 온.오프라인상의 경제연구소, 혹은 기존 언론사와 대기업, 여론조사기관 부설 '연구소'가 이 기능을 담당하여 '사설정보를 생산, 수집, 유통하고 있는 현실이다.

사설정보의 문제는 크게 두가지 방향에서 연구되어야 한다.

1) 비밀정보와 공개정보

정보는 크게 검증된 정보(authorized information)와 감증되지 않은 오도된 정보(unauthorized information or dis/misinformation)로 구분된다. '정보'란 사실(fact)에 기반을 두고, 오도된 정보란 의도된 오보

(disinformation)과 의도되지 않은 오보(misinformation)로 다시 구분된다.[2)]

정보의 유통에서 문제가 되는 것은 비단 '오도된 정보'의 유통에 국한되는 것이 아니라 '검증된 정보'라도 공개가능한 정보(unclassified information)와 공개불가능한 정보(classified information)로 구분된다. 비록 검증된 사실에 기반을 둔 정확한 정보라 할지라도 사회적 목적상 '비공개' 원칙이 지켜져야 할 많은 정보들이 있으며, 통상적으로 정부차원에서 수집, 저장된 정보의 경우는 비교적 이러한 원칙들이 준수되지만, 민간부문에서 수집, 생산된 정보들은 수익창출의 목적에 따라 쉽게 정보시장에 유통된다.

공적영역에서 생산, 수집, 저장된 정보의 분류와 그 유통은 엄격한 정부의 내부 통제가 가능하며, 그 유통은 엄격한 법적, 제도적 장치로 통제되고 비교적 충실하게 운영되고 있다.

그러나 사설정보 시장의 경우 사회적 목적을 저해하는 사설정보의 수집과 유통은 표현의 자유(freedom of speech)와 언론의 자유(freedom of press)의 원칙상과 상업언론의 속성상 직접적인 통제가 힘들며, 이러한 정보유통에 의해 개인과 집단의 사생활에 중대한 경제적, 인격적 명예훼손의 피해를 야기했을 경우 역시 그 '고의성'을 입증하지 못하는 한 법적처벌이 용이하지 않으며, '고의성'을 입증하기란 현실적으로 쉽지 않아 그 실효적 통제에 한계가 있다.

따라서 선진국의 경우 정부의 직접적 통제(governmental regulation)보다는 사설정보 업체들의 자율에 의한 규제(self-regulation)에 의존, 호소하고 있으나 그 실효성은 매우 의심스러운 것이 각국의 현실이다.

사설정보가 사회적 문제로 대두되는 것은 1)검증되지 않은 오도된 정보들이 유통되는 경우; 2)검증된 정보일지라도 사회적 목적상 비공개되어야 할 정보가 유통되는 경우 등 2가지로 나누어 볼 수 있다.

정부차원의 정보의 생산과 유통은 일반적으로 상기 2가지 폐해를 어느 정도

---

2) Porat. M. A. *The US as an information society: International implications.* (1990)

통제가능하나, 민간화된 정보의 생산과 유통은 그 경제적 필요에 따라 위의 2가지 문제를 노정할 위험성이 상대적으로 높다.

오도된 정보의 생산. 유통과 공개되지 말아야 할 정보의 유통이라는 2가지 부작용의 피해 역시 1)개인적 사생활(privacy)의 침해; 2)사회경제적 혼란과 비용(social cost)이라는 2가지 방향에서 발생하게 된다.[3)]

2) 사생활 보호와 공익의 확보

'개인'과 '사회'는 상호의존적이지만, 그 가치가 항상 일치하지는 않아서 개인적 가치와 사회적 가치는 많은 경우 충돌이 불가피하다. 국가정책의 어려움은 개인자유의 가치와 사회적 가치 조화의 어려움에 다름이 아니다.

사설정보지의 효과적 관리 문제 역시 이 범주에서 논의되어야 한다. 사설정보에 대한 단속과 규제, 관리 일변도의 정책은 실효성을 담보하기 어렵다. 사회적 가치중심의 정책은 필연적으로 개인적 가치인 정보의 생산과 유통, 그리고 '언론'의 자유와 국민의 '알 권리'까지 위축시킬 수 있다. 또한 사설정보 생산을 폭넓게 '언론의 자유'로 해석한다면 사회적 가치인 공공의 이익은 위협받을 수밖에 없다.

따라서 이 문제는 모든 사회의 핵심적 가치인 개인적 자유와 사회적 가치의 바람직한 접점을 한국사회의 사회경제적, 역사문화적 '환경'속에서 찾아 구체적 방안이 마련되어야 할 것이다.

위와 같은 문제의 인식에서 본 연구는 사설정보의 폐해와 그 대응책 고찰에 있어 아래와 같은 연구의 관점과 범위를 설정한다.

- 오도된 정보의 생산과 유통
- 비밀정보(classified information)의 공개와 그에 따른
- 사생활의 침해
- 사회경제적 혼란

사설정보의 발달에 따라 야기되는 사생활의 침해와 사회경제적 혼란의 문제에 대한 대응은 지식정보화 사회에서 두가지 방향에서 고려되어야 한다.

---

3) Reeves, R. T*he Signal fires of the future*. (United Press Syndicate, 1983)

첫째, 검증되지 않은 오도된 정보의 생산과 유통에 의한 사회경제적 피해와 사생활의 침해를 방지하기 위한 인터넷 이용 실명제등은 오히려 한편으로 개인의 자유와 정보화시대의 자유로운 정보의 소통에 장애를 야기할 우려를 수반하게 된다.

현재 전 세계적으로 사생활의 보호를 가장 기본적인 인권으로 인식하고 있으며 전 세계적으로 많은 국가들이 사생활권의 신장을 위하여 포괄적 개인신상 정보 보호법을 채택하고 있다. 그러나 국가적 목적과 사회가치의 실현을 위하여 개인적 자유의 일정부분의 유보는 불가피하게 받아들여지고 있으며, 특히 정보화 시대에 정보의 오.남용, 그리고 왜곡에 의한 사회적 가치와 공공이익의 훼손의 우려가 점차 증대하면서 이러한 현상은 더욱 가속화되고 있다.

둘째, 사회적 목적을 위한 검증된 비밀정보(classified information)의 공개제한을 위한 조치들 역시 정보의 자유로운 소통을 위축시킬 우려가 있으며, 특정집단의 권력독점의 도구로 이용되기도 한다.

또한 '정보 비밀주의'의 확산은 사설정보에 대한 수요를 확대시키고, 유료화된 사설정보 접근 비용은 정보격차(information divide)를 확대시켜, 결국 지식정보화 시대에 사회 불평등의 주원인이 된다.

I-3. 연구의 방법

해외사례 연구

위에서 살핀 바와 같이 사설정보의 사회적 문제는 크게 사생활의 침해와 사회경제적 피해의 두 가지로 요약될 수 있으며, 우리사회에서의 그 대응책을 마련함에 있어서 참고사례 연구도 이러한 두 가지 방향에서 선택되어야 한다.
그러나 동일한 문제에 대한 문제의식과 그 대응방법이 항상 동일한 것은 아니다. 동일한 문제에 대한 대응책도 그 사회의 역사문화적 배경과 사회경제적 발전단계에 따라 상이하게 나타날 수 있다.

사설정보의 발전과 그에 따른 폐해의 대응 역시 그 사회의 문화적, 사회경제

적 배경에 따라 상이한 모습으로 나타난다. 예를 들어, 문화유형에 있어 '개인적 자유'와 '사회통합'의 가치조합에 있어 전자에 무게중심을 두는 문화와 전통을 보유한 사회에서는 전통적으로 사회경제적 비용보다는 사생활보호를 중심가치로 설정하는 반면, 후자를 중요시하는 사회에서는 사생활보다는 오히려 사회경제적 비용을 최소화하기 위한 정책적 목적을 중심으로 사설정보에 관한 통제와 법적 제도적 장치가 마련된다.

따라서 본 연구는 '사례 비교연구(comparative case studies)'를 수행함에 있어 ' method of agreement'와 'method of difference'를 채택하여 (John Stuart Mill, Logic), 우리사회와 ' 사회통합 '을 중심적 가치로 설정하는 동질적 문화유형을 보이는 싱가포르와 일본, 그리고 우리와는 달리 ' 개인적 가치 '를 우선시 하는 서구문화권의 미국, 영국, 프랑스의 사례를 비교 연구함으로써 우리사회에 적실성 있는 대안모색의 참고사례를 삼고자한다.

본 연구에서는 첫째, 우선 정보화시대에 '사생활의 보호'와 '정보 생산과 유통의 자유'라는 상충하는 두 개의 가치의 조합점을 찾는 전세계적인 추세를 살펴보기 위하여 전세계 주요 49개국에서 정보화 시대에 이러한 상충하는 가치를 조화시키기 위하여 실행하고 있는 법적, 제도적 장치들을 살펴보며; .둘째, 사설정보지 범람의 폐해를 *감소*시키기 위한 제도적 장치 마련과 정비의 기본원칙을 제시한다. 사설정보지의 폐해는 우리나라의 '연예인 X파일' 사건에서 보여진 바와 같은 특정개인의 사생활 침해와 사회적(정치, 경제, 외교)혼란이라는 두 가지 측면이 존재하나, 본 연구에서는 연구의 목적상 개인적 피해 구제보다는 거시적 관점에서의 사회적 피해 구제의 방향에 맞추어 대안 논의를 진행한다.

I-4. 문제의 시대적 환경

I-4-1.지식정보화 사회

미래학자 앨빈 토플러(Alvin Toffler)는 '권력이동'에서 "앞으로 권력은 정보를 누가 정확하고 빠르게 많이 소유하느냐에 따라 이동하게 될 것"이라고 전망했다. 21세기는 '정보전쟁'이라는 진단이다.[4)]

교육수준의 전반적 향상과 정보매체의 발달은 필연적으로 가치의 분화와 다양화, 그리고 지식정보화 사회를 견인한다. 과거 엘리트 계층에 국한되었던 각종 지식과 정보의 창출, 그리고 향유는 모든 계층에 개방된 교육기회의 확대에 따른 지식수준의 향상에 따라 사회 모든 계층에서 지식과 정보가 창출되고 유통되며, 또한 향유된다. 그 유통의 속도와 소비계층의 확대 또한 정보기술의 발달과 전반적 경제수준의 개선으로 과거와는 비교할 수 없는 폭발적 상승과 증가를 보이고 있다.

이러한 지식정보 생산의 증가는 폭발적인 정보기술의 발달에 따라 사회 모든 부문에 걸쳐 급속도로 확산 유통된다

'www'라는 표기가 상징하듯 지식정보화시대와 인터넷 정보망을 상징하듯 현대사회를 흔히 ' web society'라고도 표현한다. 동시다발적으로 생산, 유통되는 수많은 정보를 취사선택 수집하여 활용하는 것이 곧 지식정보화 사회의 가장 중요한 경쟁력으로 자리 잡았다.

지식정보화 시대에 '정보'의 중요성은 농경시대의 '토지', 산업화시대의 '자본'과 마찬가지로 지배와 피지배의 결정적 요소(vital element)이다. 곧, 지식정보화 시대란 지식정보의 소유와 그 유통능력의 유무가 지배와 피지배의 분기점이 되는 것이다.[5] 따라서 새로운 지식과 정보의 생산 못지않게 그 수요도 폭발적으로 증가하고 있다.

그러나 정보생산의 증가와 유통은 검증받은 정보와 검증되지 못한 정보가 분리되지 못한 채 범람할 수밖에 없다. 정보화 시대의 경쟁력이 단순히 토플러가 지적한 대로 신속한 대량의 '정보의 수집과 소유'에서 창출되기보다는 '유효(effective)하고 신뢰할 수 있는(reliable) 정보의 소유'에서 창출된다. 유효성과 신뢰성을 담보하지 못한 정보는 정보화시대의 '쓰레기'에 불과하다.

또한, 자신이 수집, 소유한 정보가 많아도 그것을 유통시켜 활용할 수 있는 수단이 결여되어 있다면 그 정보는 무의미하다.

---

4) Alvin Toffler, *Power Shift*
5) Alvin Toffler, *The Third Wave*

지식정보화 시대를 관리하는 국가의 의무는 시민의 자유를 보호하면서도 이러한 정보화시대의 의미를 파악하고 정보의 생산과 유통, 그리고 소비가 사회의 합목적성에 부합하게 관리하여, 사회의 발전시키는 것이다.

그러나 모든 재화의 수요와 공급은 그 재화가 교환되고 유통되는 '시장'의 기능이 정상적으로 작동할 때 비로소 그 균형을 유지할 수 있으며, 사회공동체가 정상적으로 유지될 수 있다. 고전경제학자인 애덤 스미스는 시장기능의 정상적 작동을 전제, '보이지 않은 손(invisible hand)'에 의한 자연적인 수요와 공급의 균형을 기대하였으나, 경제의 역사는 ' 보이지 않은 손 '이 항상 기능한 것은 아니라는 것을 증명한다.

현재 우리사회에서 각종 사설정보지들이 유통되는 근본적 이유는 공식적 정보의 수요와 공급의 불일치에 기인하는 것이 아니라 공적 통로를 통한 '유효하고 신뢰할 수 있는(effective and reliable) 정보의 공급이 그 수요를 따라가지 못하는 균형의 붕괴에서 나타나고 있다.

정보화 시대에 유효하고 신뢰할 수 있는 정보의 공적인 공급이 그 수요을 따라가지 못하거나, 그 유통망이 투명하고 공정하게 정비되지 못한다면 사회구성원들의 사설정보지(혹은 '찌라시')에 대한 유혹은 향후에도 더욱 증대될 것이며, 예상되는 사회경제적 혼란과 정보격차(information divide) 혹은 정보 불평등(information inequality)문제는 더욱 심화될 것이다.

'자본'이 사회의 핵심적 가치인 자본주의 시대에 자본의 격차와 불평등(capital divide and inequality)을 완화하기 위하여 자본에 대한 국가의 통제와 그 시장에 대한 개입은 필연적으로 끊임없이 다양한 형태로 이루어져 '자본의 시대'의 파국을 제어할 수 있었다. 마찬가지로 정보화 시대의 핵심적 '재화'인 '정보' 역시 시장의 보이지의 않는 손에만 기대하기는 어려우며, 유효하고 적절한 수준의 국가의 '통제'와 '조정'이 필요하다.

정보화시대의 혼란이 필연적으로 야기하는 사설정보지 범람과 그 폐해에 대한 접근과 대책은 이러한 관점에서 이루어져야 할 것이다.

I-4-2. 세계화 시대

세계화는 흔히 '지구촌(global viallge)라는 말로 그 성격이 상징된다. 'village'란 말 그대로 운명공동체를 의미하며, 공동체 구성원들 간에 장벽이 없이 자유롭게 왕래하고 소통하고, 따라서 원활한 이해가 이루어진다는 의미이다.[6)]

과거 전통적인 지식정보의 창출과 유통, 그리고 소비는 개별 국가단위의 필요성에 따라 생산되고, 그 환경 속에서 유통, 소비되어왔다. 그러나 1960-70년대의 국제화(internationalization), 그리고 80년대 이후의 국가단위의 영역이 사라지고, 세계의 모든 개인과 집단이 독립적 주체(player)로 자리잡는 세계화(globalization)시대를 맞이하면서 지식정보의 생산과 소비 역시 세계영역으로 확장되고 있다.

세계화 시대란 본질적으로 국가간의 '국경'이 무의미해짐을 의미하며, 이러한 현상은 특히 국경을 자유롭게 통과할 수 있는 정보기술 혁명으로 정보의 영역에서 가장 현저히 나타나며, 정보의 세계화가 세계화를 견인하고 있다.[7)]

다시 말해서, 외부로부터 생산된 지식정보가 무차별적으로 국경을 넘어 전지구적으로 유통되고 소비되는 시대를 맞게 되었다. 국가단위를 초월하여 생산되는 지식과 정보의 종류와 양은 과거와 비교할 수 없을 정도로 폭발적으로 증가하고 있다.

국가간의 '정보 장벽' 이 사라진 세계화 시대에 확인되고 검증되지 못한 정보의 유통이 증가하는 것은 필연적인 현상이며, 모든 국가에서 그 사회경제적 비용도 기하급수적으로 증가하고 있다.

외국에서 생산된 정보의 경우, 그 진위의 검증과, 그 정보생산의 배경과 의도를 종합, 분석하여 적절하게 활용하기란 용이한 작업이 아니다. 만약 해외에서 생산되어 유입된 정보가 오도된 정보(mis-information,

---

6) Marshall, Macluhan, *Gutenberg Galaxy,* (Toronto University Press, 1990)

7) Robertson, R. 'Globalization, Politics and Religion,' in Beckfor and Luckmann(eds.) *The Chaging Face of Religion,* (Sage, 1989)

dis-information)일 경우, 그 정보의 신뢰성을 검증하지 않고 적용한다면 이는 커다란 사회적 혼란을 야기하고, 혼란을 가중하게 할 것이다. 이러한 정보의 세계화에 대응하여 각국의 국가정보기관들은 해외정보기능을 더욱 강화하고 있다. 한국의 국가정보원이 세계화시대에 맞추어 해외정보활동을 더욱 강화하는 것은 이러한 현상의 반영을 의미한다.

미국의 경우 국가정보기관이 사기업을 위한 해외정보활동의 정당성 문제를 놓고 오랜 기간 치열한 논쟁이 지속되었으나 1970년대 이후 CIA가 미국기업 활동을 보조하기 위한 해외정보 업무를 본격적으로 개시하였다. 이는 점차 치열해지는 세계경제전쟁 속에서 미국의 사기업들의 성공이 곧 미국의 국익으로 연결된다는 인식과, 유럽과 일본경제의 거센 도전에 직면하였던 미국의 선택이었다. 일본기업의 성공에 대한 분석에서 미국은 일본정부의 기업에 대한 적극적인 해외정보 제공이 주요 원인 중 하나라는 사실을 발견하였다.

MITI(Ministry of International Trade and Industry)와 JETRO(Japan External Trade Organization)으로 대표되는 일본정보부의 주된 임무는 기본적으로 경제정보 수집과 분석으로 정평이 높다. 이러한 경제정보들은 대부분 이들에 의해 수집되고 분석, 처리되고 있다. 일본정부 정보당국과 민간기업 사이에는 매우 심도 깊은 교류가 일상화 되어있다.[8)]

이는 정부의 정보업무가 '정부' 자체를 위한 것이 아니라 사기업으로 대표되는 민간의 필요에 의해 이루어지는 대표적인 사례라고 할 것이며, 이러한 정부의 정보업무 역량을 민간을 위한 서비스 차원에서 파악한 것이 일본경제성장의 원동력 중 하나라는 것은 아무도 부인 할 수 없다.

그러나 기업영역에서는 해외정보의 수집과 분석이 비교적 체계적으로 운영되고 있으나, 국가영역에서는 그 활동이 세계적 수준에는 미치지 못하며, 더욱이 국가정보기관을 통한 해외정보의 생산과 활용은 공공재로서 사회에 공개, 환원되지 않고 대부분 국가 활동에만 활용되고 있는 현실이다.

세계화시대란 지구촌의 개개인 모두가 지구촌의 주체(player)가 되는 시대를

---

8) Robertson, R. 'Globalization and Societal Modernization: A Note on Japan and Japanese Religion' *Sociological Analysis* 47:

의미하며, 그럴 때 국가경쟁력도 제고되는 시대이다. 따라서 국민 개개인이 지구촌의 진정한 '주체'로서 전지구적 영역에서 활동하도록 돕기 위해서는 국가가 수집, 분석한 해외정보를 국민들에게 가능한 한 광범위하게 공급해야하는 것이 세계화 시대의 국가의 책무이기도 하다.

세계화시대와 정보화시대에 한 국가가 다양한 정보를 수집하고 분석, 가공하고 필요에 따라 유통시켜, 국민들이 활용할 수 있도록 하는 것이 곧 국가경쟁력의 원천이다.

사설정보지의 범람에 따른 사생활의 침해와 경제사회적 혼란과 피해는 결국 세계화, 정보화 시대에 국가가 적정수준의 정보를 국민에게 제공하는 데 실패하여, 국민들이 사설정보에서 그 정보욕구를 해소하려는 현상에 다름이 아니다.

따라서 사설정보지의 문제 해결은 국가정보 생산성 제고와 효율적 유통과 분배에서 찾아야 할 것이다.

I-4-3. 국가의 쇠퇴

이러한 세계화시대와 지식정보화 사회가 수반하는 지식정보의 폭발적 증가와 대량생산, 유통, 소비는 새로운 양질의 지식정보를 통하여 가치창출의 기회와 삶의 질의 향상을 도모할 수 있는 새로운 지평을 열어주는 동시에, 반대로 통제되지 못한 왜곡되고 오도된 지식정보(dis-information and mis-information)는 언제든지 인간의 삶 자체를 파괴할 수 있는 위험성을 내포한다.

최근 인터넷 웹사이트 정보의 신뢰성에 관한 연구에서 발표된 한 논문에 따르면 인터넷에서 유통되는 30% 가까운 정보가 '검증'되지 않은 정보인 것으로 보고된다.[9] 또한 상기한 바와 같이 외부로부터 생산된 지식정보는 그 지식정보가 생산된 '지역'에서는 유효하고, 무해할지라도 전혀 상이한 사회경제적, 문화적, 역사발전 단계에 위치한 '지역'에서는 무의미하고 유

9) Haal Varian, Anticipate the Pace of Change: Information Revolution. (Stanford University Press, 1999).

해할 수도 있다.

그러나 이미 '국경' 이 무의미해진 세계화시대의 특성상 국경을 자유로이 넘나드는 지식정보를 개별국가가 외부와 내부의 사이에서 '검문소(interface)'의 역할을 수행하기는 거의 불가능에 가깝다. 오마에 게니치(大前研一 Omae Kenichi)가 ' 국가의 소멸 '이라고 지적하듯이 세계화와 지식정보화 시대는 필연적으로 국가역할의 위축과 축소를 수반한다(Kenichi, 1998).[10)]

과거 정치,경제,사회의 활동이 개별국가단위로 한정되고, 그 개별단위 국가에서 생산, 유통, 소비되는 지식과 정보의 양이 비교적 한정되고, 제한적인 상황에서는 그 대다수 정보를 국가차원에서 관리하고 통제하는 것이 상당부분 가능했으나 정보화와 세계화 시대에 다양한 정보의 '폭발(explosion)'을 맞이하면서 이미 사회구성원들이 요구하는 폭발적으로 증대한 다양한 정보를 국가가 생산하고 유통하는 것이 실질적으로 불가능하게 되었다.

이러한 정보의 수요와 공급의 불균형이 필연적으로 '사설정보' 의 공급을 견인하게 되었다. 사설정보의 확산은 국가의 쇠퇴가 야기한 전세계적이고 시대적인 흐름인 국가영역, 혹은 제 1 섹터(sector)의 축소와 과거 전통적으로 국가의 영역에 속했던 고유업무를 민간인 제 2섹터에 이양하는 '민영화(privatization)'의 대세 속에서 이해되어야 할 것이다.[11)]

현실적으로 '정보산업(information industry)'에 있어서, 과거에는 사설정보(private intelligence)가 국가정보의 유출에 의존하는 경우가 많았으나 점차 미국의 거대 사설정보 ChoicePoint의 사례에서 보듯 이제는 오히려 국가가 사설정보에 의존하는 방향으로까지 진행되고 있다.

따라서 정보화와 세계화라는 시대적인 흐름이 멈추거나 뒤돌아가지 않는한 사설정보의 발달 역시 필연적인 대세를 이룰 것이다.

상기(上記)한 3가지 주요한 시대적 환경과 흐름은 현실사회와 그 대응에 있어 사실상 상호모순적 성격을 내포한다: 우선 지식정보화 사회의 가치창출은

---

10) Omae Kenichi, 국가의 종말 (박길부 역, 한언, 1998).

11) Reich, Robert, *The Work of Nations: Preparing Ourselves for 21st Century Capitalism* (1993) 남 경우 외 역, 까치

자유롭고 다양한 가치와 주장의 막힘없는 생산과 유통을 요구하고, 세계화 시대에 필연적인 국가의 쇠퇴는 이러한 현상을 더욱 가속화시킨다. 그러나 일견 '국가'와 '개인' 사이에 존재해왔던 긴장과 균형관계가 개인자유와 가치구현의 방향을 잡음에 따라 그 균형이 무너지고 있으며, '국가의 쇠퇴' 현상은 무차별적인 지식정보의 생산과 유통의 '사회적 합목적성' 추구를 불가능하게 하며, 그 과정에서 발생가능한 지식정보의 피해자 구제에 한계를 노정할 수밖에 없다.

이러한 시대적 고민은 정보기술의 획기적이고 혁명적인 발달로 더욱 깊어진다. 도감청의 공포, 사이버 폭력, 인터넷 실명제를 둘러싼 사회적 논란이 모두 여기에 해당될 것이다.

한국사회에서 현재 시급한 문제로 대두되는 '사설정보지'의 고민도 여기에서 비롯되고 있다.

가치의 분화와 다양성을 근간으로 하는 지식정보화 시대에 국가이든, 집단이든 집중된 '권력'이 모든 다양한 지식과 정보, 가치를 창출할 수도 없고 검증할 수도 없다. 로버트 라이시가 지적한 바와 같이 '국가의 일' 자체가 근본적으로 변화하고 있는 것이다.[12] 이러한 시대적 상황 속에서 '사회적 합목적성'을 기반으로 검증되고, 통제되지 못한 지식과 정보의 생산과 유통은 크게는 사회파괴적일 수도 있으며, 작게는 사회공동체 구성원 개인에게 피해를 야기할 수도 있다. 그러나 무엇보다도 사회적 합의에 의해 선택된 권력인 '국가'가 아닌 사적 이익집단이 특정 사적 목적으로 생산, 유통하는 지식과 정보가 광범위하게 무비판적으로 통제되지 못하고 확산될 경우 그 결과는 가히 재앙에 가까우며, 사회의 방향성조차 상실될 우려가 있다.

여기에 '사설정보지' 문제가 발생한다. 지식정보의 자유로운 생산과 유통, 소비의 활력을 유지하는 가운데 사회적 합목적성을 견지하고, '자유'에 따른 사회적 선의의 피해자를 최소화시켜야 하는 어려운 해결책을 모색해야 하는 것이다.

본 연구는 위와 같이 지식정보의 자유롭고, 활력있는 생산과 소비라는 하나의 가치와, 지식과 정보의 사회공동체를 유지하기 위한 합목적성 부합이라는

12) Reich, Robert. *ibid* pp. 79-82.

또 다른 상반된 가치 사이에서 사회공동체가 합의할 수 있는 현실적 '접점'과 그 실천적 방안 연구에 둔다.

이상과 같은 문제의식 위에서 우선 현재 한국사회에서 노정되는 사설정보지의 정보수집, 생산, 유통 그리고 소비의 현황을 통해 '처방'을 위한 '진단'을 실시하고 문제발생의 원인분석을 하며, 생산적인 '사설정보' 활성화를 위한 대안 모색을 위하여 지식정보화 시대의 무제한적인 지식정보의 생산과 소비와 사회공동체 유지라는 동일한 고민 위에서 그 건설적 대안 모색을 하고 있는 외국의 사례를 고찰해 보기로 한다.

사설정보지에 대한 문제제기는 지식정보화 사회 속에서 사설정보지의 정보유통의 생산과 소비, 유통이 첫째, 개인적 인권의 주요영역인 '사생활'에 대한 침해의 관점과, 둘째, 다양성의 시대에 필연적으로 수반되는 역작용인 '사회통합 저해'와 '사회적 비용'의 증가의 관점에서 고찰된다.

외국사례는 의사표현과 다양한 가치의 '개인'적 자유에 무게중심을 두는 전형적 모델로서 미국사회와 '사회적 합목적성'을 강조하는 일본과 싱가포르, 그리고 개인적 자유와 사회적 합목적성의 조화를 추구하는 유럽(영국, 프랑스)의 모델 연구를 통하여 한국사회에 적실성 있는 대안 모색의 준거틀을 삼고자 한다.

II. 사설정보지 현황과 문제

II-1. 사설정보지 현황

II-1-1. 군소 사설정보업

넓은 의미에서 '사설정보지'의 범위에 각종 다양한 분야의 '생활정보지'와 언론자유화 조치이후 우후죽순격으로 출몰을 반복하는 각종 '주간지'와 소규모 '지역신문' 그리고 소위 말하는 각종 '찌라시', 그리고 인터넷상에서 유통되는 '미확인 정보'와 단순한 '소문'까지 포함한다면 우리사회의 '사설정보'의 범람은 아래에서 살펴보는 외국의 경우에 비교해서 그 개체수와 그 다양성에 있어 훨씬 높은 수준을 나타낸다.

넓은 의미에서 우리사회의 '사설정보지'의 현황파악은 매우 어려우며, 공

식적인 집계조차 이루어지지 않고 있어, 사설정보지에 대한 대응책 마련이 실효적으로 이루어지기 위해서는 그 현황파악이 급선무이다. 각종 사설정보업과 정보지의 성격과 유통과정, 그리고 규모에 따른 분류와 그에 따른 선별적이고 차별적이 대응책이 마련되어야 한다.

본 연구는 연구의 목적상 현황파악이 어려운 광의의 사설정보지를 대상으로 하기보다는 일정형태와 규모를 갖춘 등록된 '정규' 사설정보지의 문제에 국한한다. 이러한 범위의 사설정보지 중 상당수 역시 은밀히 생산 · 유통되기 때문에 정확한 실태 파악이 쉽지 않다. 사설 정보지가 수십 · 수백종씩 나돌고 사고팔기까지 하는 것은 전세계적인 현상이지만 우리의 경우 그 활동이 매우 활발하고, 또한 그 폐해가 다른 국가들에 비해서 심각한 수준이다.(비공식적으로 활동하는 등록되지 않은 정보지까지 포함할 경우 개체수 파악은 불가능하다).

이러한 사설정보업과 정보지의 특출한 확산은 우리 사회가 공식 경로를 통한 정보 공개가 불충분하고 커뮤니케이션 구조가 후진적이라는 것을 반영한다. 국가와 민간을 가릴 것 없이 사회적 활동이 법과 원칙에 따라 투명하게 이뤄지지 않기 때문에 '막후(幕後)'에 대한 궁금증이 일고 '이면(裏面)'을 들여다보고 싶은 욕구가 생긴다. 그래서 사설 정보지에 대한 수요가 끊이지 않고 그에 따라 공급도 활발한 것이다.

아래에서 살펴보는 바와 같이 외국에도 다양한 사설정보지는 존재한다. 그러나 우리사회 사설정보의 문제는 그 개체수 자체의 문제라기보다는 그 사회적 파장의 정도가 외국의 경우보다 심각하다는 데에 있다. 이는 첫째, 외국의 경우와 비교하여 '사설정보'의 유통이 사회구성원들에게 상당부분 '호소력'을 발휘하여 그 사회적 파장이 외국의 경우와 달리 광범위하고 깊게 나타난다는 점이며, 그 책임추궁과 피해구제가 제대로 이루어지지 않고 있다는 점이다.

사설정보지는 증권사나 기업의 '정보맨'들이 증시 주변에 떠도는 루머와 자신이 입수한 첩보를 모아 작성한다. 여기에 국회, 국가정보원, 검찰, 경찰 관계자들이 포함되는 경우도 있으나 외국의 사례에 비추어 비교적 소수에 머무는 것으로 보고된다. 이들은 개인적 친분관계에 따라 공식, 비공식의 회

의, 혹은 단순한 모임을 통해 가진 정보를 공유하고, 이를 모아 정보지를 만든다. 이 과정에 사설 정보제공업체가 개입하기도 한다. 제작자는 각계각층의 사람들인 셈이며, 이러한 수집과 가공의 특성상 정보의 일관성과 논리성이 현저히 약화되는 경우가 많다.

이렇게 생성된 정보를 바탕으로 현재 시중에 나도는 '이름' 있는 사설정보지는 10~15개 정도로 보고된다. 이들은 대부분 유료회원제로 운용하며 우편이나 e-메일 형태로 서비스한다. 정치권 루머나 기업 동향 등 '일정 수준' 이상의 내용을 담은 사설정보지는 월 30만~50만원의 구독료를 받고 있는 것으로 알려져 있다.[13)]

수많은 사설정보지 생산과 공급은 그만큼 수요가 있기 때문이다. 대표적인 것이 상부에 대한 업무보고다. 불확실성이 고조될수록 정제되지 못한 정보에서라도 판단의 근거를 찾으려는 심리는 확산된다. 어느 조직이고 공조직이 확고히 정착되고 작동하지 못하는 경우에 사조직에 의존하게 되고, 사적 라인에 정보와 판단을 구하는 경우 사설정보지의 영향력은 확대된다.

또한 사설정보는 어느 중소기업 경영자의"골프모임에서 '말빨'이 밀리지 않으려면 이를 볼 수밖에 없다"는 고백처럼 사교용 소비되기도 한다. 심지어는 국회의원들 조차 각종 정치정보와 판단의 근거를 사설정보지에서 구하는 사례가 빈번하다.

우리사회의 사설정보의 폭발적 증가는 1)80년대 중반 이후 본격적으로 전개된 세계화의 흐름에 따른 정보수요의 다양화, 대량화; 2)인터넷 시대의 본격적 전개에 따른 정보수집과 유통의 신속화; 3)IMF 경제위기 이후 미래에 대한 불안감과 불확실성의 증대와 4)지난 1997년 정권교체이후 사회주류세력의 급격한 교체와 변화에 따른 정치,경제 분야에서의 네트워크의 교체와 붕괴가 정보의 다양한 새로운 욕구의 창출; 그리고 마지막으로 90년대말 소위 '뉴 밀레니엄' 의 개막에 대한 막연한 불안감과 불확실성의 증가가 복합적으로 작용한 데에서 그 이유를 찾을 수 있다.

---

13) 국회정보위원회 2003년 보고자료(비공개), 한국경제신문, 매일경제

이렇게 수요가 확대되면서 사설 정보업체도 폭발적인 증가를 보이게 되었다. 제한된 회원에게만 정보를 제공하는 비밀정보은행도 생기고. 이 업체는 특히 정치인과 언론사, 정부기관은 철저하게 제외시키는 것으로 알려지고 있다. 정보가 대중화되면 이미 그 생명이 끝난 것이고, 정보는 극소수만 알고 있을 때 가치고 있다는 설명이다. 또 제공하는 정보도 루머와 사실을 명확히 구분해 최대한 신뢰도를 높이고 있다. 이 정보은행의 경우 사업의 목표를 기업 정보팀의 한계를 보완해 주는 것으로 설정하며 하루 25가지의 정보를 제공하고 월 50만원의 이용료를 받는 것으로 알려지고 있다.

최고경영자 대상의 인터넷 정보서비스를 제공하는 사설정보업체도 활발한 활동을 하는 것으로 보고된다.. 특히 'CEO경영정보'라는 정보서비스는 연간 100만원의 비싼 이용료를 내야 하는데도 회원이 1만명이 넘는 것으로 알려지고 있으며, 실제로 회원 80% 이상이 최고경영자와 재무담당, 기술담당 임원 등이다. 정보지와 시중자금 동향 및 자본유치 동향 등의 정보를 가공한 고급 정보를 '맞춤 보고서' 형식으로 매주 토요일 e메일로 제공한다.[14)]

다소 특이한 경우는 아예 언론사가 '정보지'를 제작하는 경우도 있다. '내일신문'은 기자들이 취재한 것 가운데 고급정보를 추려 'CEO리포트'라는 이름으로 판매하며, '머니투데이'는 증권가 소식을 수집해 유료정보로 고객들에게 제공하고 있다.

또한 최근 그 영향력이 날로 확대되는 각종 여론조사기관에서 자신들이 수행한 여론조사를 기반으로, 그리고 조사 수행과정에서 수집한 정보를 바탕으로 사설정보지를 발행하기도 한다.

II-1-2. 대기업 조직과 연계된 사설정보업

경영활동을 위해 자체적으로 정보지를 만드는 대기업도 속출하고 있다. 주로 비서실이나 구조조정본부에서 정보조직을 갖고 이를 운영하는 것이다. 하지만 각 기업에서는 정보조직의 실체를 대외비에 부치고 있다. "국가정보원과 같이 음지에서 양지를 위해 일한다"는 것이다. 기업의 이미지가 나빠질 수 있고, 정보맨들의 대외활동에 제약이 따를 것을 우려해서다.

---

14) 매일경제, 2003, 7. 16

그러나 이들의 정보력은 상상을 초월하는 것으로 알려졌다. 특히 모그룹의 정보력은 국정원 못지않다는 얘기가 증권가에는 심심치 않게 나돌고 일반인들 사이에서는 일종의 '신비감'으로 확대해석되기도 한다. 이들 대기업에서 수집하는 정보는 최고경영자와 최측근 임원들에게만 보고되며 외부 유출은 절대 금하는 것으로 알려졌다. 이들 기업이 만드는 정보지는 대체로 믿을 만한 것으로 정평이 나 있다. 때문에 주요언론 기자들조차 취재와 확인과정에 이 정보지의 정보에 의존하는 경우가 많으며, 심지어는 정부기관조차 이들 대기업의 사설정보에 촉각을 곤두세우기도 한다.

대기업의 경우 적게는 3~4명,많게는 7~8명 가량의 '정보맨'들을 운영하고 있는데 이들은 매주 1~2회 정도 정보기관의 담당자들과 모임을 갖고 정보를 교환하고 있다. 분량은 통상적으로 일주일에 A4 용지 10~20장, 많게는 70~80장까지 제작하는 것으로 나타난다.[15)]

특히 일부에서는 자신들에게 유리한 정책을 이끌어낼 목적으로 경쟁사나 정부 관료에 대한 음해성 허위정보를 만들어 정보지에 흘리기도 한다.

대다수 정보지는 주로 시중에 떠도는 입소문을 근거로 제작하기 때문에 신뢰도에 문제가 생길 수밖에 없다. 그럼에도 불구하고 공식적인 정보유통망이 왜곡되어 있는 경우 사설정보지의 차별화된 정보가 적중하는 경우도 있으며, 특히 정치관련 정보와 '정경유착'에 관한 정보의 경우에 이러한 경우가 다수 발생하여 사설정보에 대한 수요를 지속시키는 역할을 하기도 한다.

그러나 상기한 일부 대기업과 연계된 '연구소'의 사설정보의 경우는 상당정도의 초기 신뢰성을 확보하여 그 신뢰성은 쉽게 확대재생산되기도 하고, 일정정도는 과대포장되기도 한다.

II-1-3. 사설정보의 인터넷 유통

위와 같이 생산된 사설정보지들이 인터넷 매체와 도구의 확산에 따라 인터넷을 통하여 급속도로 확산되어 그 부정적 영향력이 더욱 확산되고 있는 것

15) 국회 정보위원회 보고자료(비공개)

이 새로운 현상으로 대두되고 있다.

사설정보지는 몇 년 전만 해도 대기업의 경우 정보담당 임원이나 최고경영자(CEO)만 접할 정도로 한정돼 있었지만 최근에는 이메일이나 메신저를 통해 순식간에 확대 · 재생산되면서 무차별적으로 유포되고 있는 실정이다.

최근 몇몇 인터넷 카페의 정치인 사이트에서는 간단한 회원 가입 절차를 거치거나 가입 절차 없이도 정보지를 공짜로 열람할 수 있다. 이들 카페 · 커뮤니티 등에는 '일일정보동향' '주간정보동향' 등의 제목으로 정보지들이 올라오고 있는데, 이들 정보지들은 주요 정치인 · 기업인 · 금융인 등에 대한 확인되지 않은 정보를 해당인의 실명을 명시해 나열하고 있다.

한 정치인 지지 모임 사이트에 지난달 올라온 한 글에는 '전직 대통령이 60년대에 일본에서 몰래 딸을 낳아 국가기관을 통해 수억원의 돈을 건넸다', '사채업계 '큰손'의 아들이 여자 연예인들과 스캔들을 일으키다가 뺑소니 사건에 연루돼 도피 생활을 하던 중 정신질환에 걸렸다'는 등의 내용이 담겨 있다.

이밖에 한 포탈 사이트의 '연예계뒷담화' 등 카페에서도 정보지에 나온 연예인 관련 소문을 사실인 것처럼 게재하고 있고, 싸이월드의 몇몇 개인 미니홈피에서도 '최신정보 드립니다'라는 제목으로 정보지 내용을 갈무리해 싣고 있다. 일부 네티즌들이 사이트로 방문자를 유도하려고 찌라시를 올리는 현상이 확산되고 있으며 확인되지 않은 소문들이 메신저 등으로도 빠르게 유포될 수 있어 인터넷상의 사설정보의 위험성은 점증하고 있는 추세이다.

또한, 특정 집단에 의해 악의적으로 유포되는 유언비어나 비방이 실명으로 실려서 명예를 훼손하거나 경제적인 피해까지 발생한다. 경쟁자나 경쟁기업에서 역정보를 흘린 것이 정보지에 실리는 경우도 종종 있다.

사설정보지의 내용은 정부의 정책 방향이나 인사 문제,정치권 동향,기업체 ·

언론사 내부 동향 등에서부터 모 재벌그룹 2세가 어느 술집에 자주 다닌다거나 특정 연예인의 사생활과 관련한 소문에 이르기까지 다양하다.

정보지 내용의 신빙성에 대해 이용자들은 30~40% 정도라고 말하고 있다.

실제로 현 정권 출범 직후 "청와대에서 모 그룹을 손 볼 것"이라는 정보지 내용이 실제 5~6개월 뒤 모 그룹 총수가 검찰 수사를 받으면서 사실로 확인되는 경우도 있었다.

하지만 사실보다는 허위,과장이 많을 뿐 아니라 그로 인한 피해가 매우 심각하다는 데 문제가 있다.

외환위기 때는 특정 기업의 부도,자금 악화설이 광범위하게 유포되면서 건전한 재무구조를 가진 기업들까지 금융기관들의 빚 상환 요청으로 부도 위기에 몰리기도 했고,증권가 '작전세력'들은 '코스닥 특정 종목에 작전이 들어갔기 때문에 주가가 몇월 며칠까지 몇만원까지 오른다'는 등의 정보를 유포시키며 주가를 띄우기도 했다.

사설정보지는 특히 정치권이나 정부, 경제계에서 자신과 이해관계에 있는 사람들을 궁지에 몰아넣기 위해 악의적으로 작성되는 경우도 많아 국가와 사회의 기본질서까지 위협하기도 한다.

개각을 앞두고는 후보에 오른 특정인에 대한 흠집내기가, 선거철에는 이른바 '공천 살생부'가 유포되기 일쑤였고 국책사업자를 선정할 때는 특정 기업의 정치자금 제공설, 여권 인사 개입설 등이 자주 등장한다.

최근에는 유명인이 아닌 기업체 직원이나 언론사 인사들의 사생활까지 정보대상에 오르면서 피해를 보고 있는 실정이다.

실제 지난해 모 부처 차관의 경우 산하기업 사장으로 간다는 음해성 소문이 몇 달 동안 정보지에 떠돌면서 결국 올해 초에 옷을 벗기도 했고 모 언론사 인사도 사생활이 노출돼 피해를 봤다.

이러한 무책임하고 확인되지 않은 정보의 일방적 유통은 첫째, 언급된 개인

의 명예와 재산, 사회생활, 사생활에 심대한 타격을 가하며, 둘째, 그 '개인' 이 '공인' 인 경우에는 사회적 파문과 파장으로 연결된다. 또한 의도된(intended) 왜곡정보이든 의도되지 않은(unintended) 왜곡정보이든 사회경제, 그리고 초래된 정치적 혼란은 막대한 사회적 비용의 지불을 야기하기도 한다. 그 사회적 파장의 '정도(degree)' 는 사회적으로 신뢰성 제로(credibility zero)에 가까운 속칭 '찌라시' 정보에서 보다는 어느 정도 신뢰성을 담보한 등록된 정규 사설정보기관의 정보일 경우에 더욱 심각하다.

또한 회원제로 운영되는 정보지보다는 인터넷상에서 무차별적으로 확산되는 경우 그 폐해는 더욱 심각한 양상을 보이기도 한다.

II-2. 사설정보 단속 현황

정부가 허위정보를 유통시키는 사설정보지(일명 '찌라시')와의 전쟁에 나선 것은 위와 같은 근거 없는 허위정보로 인해 개인은 치명적인 피해를 보고 경제 · 국가적으로도 대외 신인도가 떨어지는 등 그 폐해가 심각하다는 판단에서다.

2005년 5월 15일 법무장관과 정보통신부장관, 경찰청장은 15일 공동 명의로 된 담화문에서 "최근 사설정보지를 통해 근거없는 허위정보가 무분별하게 생산 · 유통되면서 명예훼손이나 개인 인권침해, 기업신용과 국가신인도 저해, 국론분열 등의 심각한 부작용을 초래하고 있다" 고 밝히고. 검찰(첨단범죄수사과)과 경찰(지능범죄수사과)을 주축으로 정통부 등 유관기관과 긴밀한 협조체제를 유지하면서 '허위정보 생산 · 유통 사범' 에 대한 특별단속을 벌이고 있다.

또한, 인터넷으로 유포되는 사설 정보지 등의 폐해가 심각하다고 보고, 지난 2005년 7월 청와대에서 대책회의를 열어 정보지와 인터넷상의 유언비어로 인해 피해를 본 사람들을 위한 신고센터를 설치했으며, 특별단속을 통해 허위정보 생산자나 악의적 허위사실 유포자 등은 구속수사하고, 국세청 등과 협조해 불법행위를 통해 얻은 경제적 이득은 철저한 환수조치 방침을 확정

했다..

또 근거없는 소문을 유포한 증권사 임직원들에게는 증권거래법상 제재조치를 병행하고, 인터넷을 통한 명예훼손 등 중대 사안 발생시에는 피해자 의사를 확인해 관련자에게 응분의 책임을 묻기로 방침을 정했다.

또한 사설정보와 인터넷 정보유통을 통하여 발생하는 명예훼손의 경우 친고죄이기 때문에 신고가 들어와야 처벌할 수 있는 특성을 고려하여 이를 전담하는 센터를 운영을 실시하고, 확인되지 않은 정보를 돈을 받고 유포시킨 2명의 사설정보사 대표를 구속하고 5명을 입건하기도 했다

이같은 정부의 전방위적인 조치는 명예훼손이나 인권침해 등 사설정보지의 피해가 심각한 수준에 이르렀다는 판단과 정보지의 폐해를 뿌리뽑겠다는 의지에 기반하고 있는 것으로 보인다.

II- 3. 정부 단속의 평가

그러나 검찰 등 관계 기관은 그동안 사설정보지에 대해 몇 차례 집중 단속했지만 단속 때만 잠잠할 뿐 '소나기'만 지나면 또다시 '독버섯'처럼 퍼져나가곤 했다. 특히 개인과 관련된 명예훼손죄의 경우 피해자의 고소·고발이 없으면 처벌하지 못해 수사기관이 적극적으로 수사에 나서는 것도 한계가 있다.

또 건전한 정보와 허위정보를 골라내는 기준이 모호하고 인터넷 상의 정보에 대해서도 표현의 자유인지, 음해성 정보인지를 가리는 잣대도 모호해 단속과 규제 그리고 사법적 처리가 용이하지 못하다.

또한 대대적인 단속은 사설정보업체들을 지하로 숨어들게 만들어 그 실체파악이 더욱 어렵게 되기도 하고, 위험요소의 증대로 말미암아 정보의 가격상승을 야기한 것으로 보고된다.

따라서 효과를 기대하기 어려운 단속일변도의 조치보다는 사설정보지 범람

의 사회구조적 원인을 파악하고 그에 따른 근원적 치유를 위한 대안 모색이 필요한 시점이다.

III. 인권과 사생활 침해

III-1. 사생활권의 정의

사설정보지 문제의 진단과 처방에 앞서 문제의 본질을 명확히 하기 위하여 사설정보지의 가장 큰 폐해로 지적되는 사생활과 인권침해의 개념과 사설정보지가 야기하는 사회적 비용의 개념을 명확히 할 필요가 있다.

모든 인권에 관한 국제적 합의에서 사생활권이라는 것은 가장 개념정의가 까다로운 것이다. 그러나 사생활권 보호란 사회가 개인적 영역에 어느 정도까지 개입하는 것이 용인될 수 있는지의 판단에 따라 결정되는 것이다. 사실상 인권이란 곧 사생활권이라고 보아도 무방하리만큼 사생활권은 현대 민주사회의 핵심적 가치라는 점에는 모두 동의한다.

1890년 미국의 대법관 루이스 브랜다이스(Lewis Brandeis)는 사생활권을 '홀로 있을 권리(right to be left alone)'라고 규정하고 민주주의 사회에서 개인이 누릴 수 있는 자유 중에서 가장 소중한 권리라고 규정하며, 이는 헌법에 반드시 명시되어야 한다고 주장하였다.[16]

미국의 헌법학자 앨런 웨스틴은(Alan Western) 1967년 그의 저서 '사생활과 자유(Privacy and Freedom)'에서 사생활권을 어떤 환경에서 어느정도로 자신을 타인에게 노출할 것인가를 자유로이 선택할 수 있는 권리라고 정의하였다.[17]

루스 개빈슨(Ruth Gavinson)은 사생활권의 요소를 구체적으로 비밀성과 익명성 그리고 독자성으로 규정하고 있으며, 영국의 '캘커타 커미티(Calcutta Committee)'는 사생활의 만족할만한 정의를 내리기는 어렵지만 포괄적으로 사생활권이란 '개인과 그 가족의 삶과 일상생활이 직접적인 물리적 방법이나 정보의 유출과 공개, 출판에 의해 침해받지 않을 권리'라고 규정한

16) Samuel Warren and Louis Brandeis, "The right to privacy," Harvard Law Review 4, 1890 pp 193 - 220.

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

다.[18]

프라이버시권에 대한 개념은 오래전부터 있었지만 정보화 사회로 진입한 현대에서는 '개인 정보에 대한 통제권'이라는 보다 적극적인 개념으로 바뀌고 있다. 이 권리의 개념은 미국에서부터 발전해 온 것이다. 즉 정보화 사회 진전에 따라 사생활 보호에 대한 권리가 소극적으로 "사생활의 평온을 침해받지 아니하고 사생활의 비밀을 함부로 공개당하지 아니할 권리"에서 나아가 적극적으로 "자신에 관한 정보를 관리, 통제할 수 있는 권리"를 포함하는 의미로 이해되고 있다. 이는 프라이버시를 침해받지 않을 자유권적 성격뿐만 아니라, 기록된 개인정보가 부정확할 때 당하는 부당함을 사전에 막기 위해 자신의 정보를 확인하고 정정할 수 있는 청구권적 성격도 갖게 된다는 의미이다 .

이처럼 개인의 프라이버시권 개념이 적극적으로 바뀌는 경향은 정보통신 기술의 발달로 쌍방적 의사소통이 가능해졌기 때문이다. 이제 더 이상 정보 수용자들은 정부에게만 정보 관리·가공을 맡길 필요가 없다. 수용자들 스스로가 통신상에서 다른 이들과 서로간의 정보를 나눔으로써 정보 자체를 보다 확장시킬 수 있게 된 것이다. 또 다른 이유는 정보를 공유하고 확장하는 과정에서 개인신상정보 유출 경로가 무한정 확장되고 있다는 점이다. 개인들이 다양한 정보를 적극적으로 수집, 활용하고 생산할 수 있게 된 반면, 자신들의 고유한 신상정보를 어떤 용도로, 언제 어떻게 공개되는지도 모른채, 그리고 어떻게 남용될지도 모른 채 내주는 경우가 많아졌다. 이러한 정보 유출로 겪는 개인적 피해는 사회 문제로 대두 되고 있으며, 개인 스스로가 자신의 개인 정보를 관리하고 통제하면서 자신의 권리를 적극적으로 주장해야 한다.

국제적인 ‘코드’로서 공인된 상기의 다양한 ‘사생활권’의 관점에서 본다면 사설정보지의 현황파악에서 살펴본 바와 같은 개인 신상의 정보유출은 당사자가 공개와 노출을 원하지 않는 개인적 정보와 삶의 모습이 외부에 ‘실명’으로 공개되어 사생활에 있어 피해와 위축을 가져온다는 점에서 명백한 사생활권의 침해로 판단될 수 있으며, 그러한 관점이 현재 우리사회의

18) Simon Davies, Big Brother: Britain's web of surveillance and the new technological order (Pan, London, 1996) p. 23.

사설정보지의 문제를 인식하는 기준이 된다.

III-2. 사회적 비용

사설정보지의 문제는 정보노출 대상이 된 개인적 피해만을 양산하는 것은 아니다.

사설정보지 현황파악에서 제기된 사례들을 통해 조작되거나, '의도한 오도', 혹은 왜곡된 경제정보는 소수의 특정 개인적 차원의 피해에 그치지 않고 다수의 선의의 피해자를 양산하기도 한다. 더욱 심각한 문제는 주식시장, 부동산 시장에 충격과 왜곡을 가해 시장의 기능을 중심으로 형성된 자본주의 사회 양식 자체에 타격을 주기도 한다.

왜곡되거나 조작된 '정치정보'는 국민의 합리적인 정치적 선택을 전제조건으로 하는 민주주의 질서 자체를 붕괴시킬 개연성도 존재한다. 사설정보지에는 원칙적으로 '사회적 책임'과 '공공성'을 기대하기 어렵다.

'정규' 언론의 경우, 정부와의 일정부분 '양해'와 '이해' 하에 비록 그 '정보'가 사실에 기반 한다고 해도 국가적 목적과 사회적 합목적성에 따라 '비보도' 원칙의 유도가 가능하고 '협조'를 구하는 것도 가능하다. 그러나 실체조차 파악되지 않는 사설정보지의 경우 사회적 합목적성의 판단에 따른 사설정보지 자체의 판단과 분별을 기대하기도 어려울 뿐더러, 정부차원에서의 협조요청

사설정보지의 이러한 속성이 그 사회적 폐단의 원천이 되며, 특히 '익명성' 뒤에 숨은 인터넷 사설정보일 경우 그 위험성은 더욱 가중된다.

IV. 한국사회의 사설정보 범람 원인 분석

위와 같은 우리사회의 사설정보지의 생산과 소비과정을 살펴보면 사설정보의 생산과 유통은 기본적으로 정보생산과 유통과정의 왜곡에서 그 근본적 원인을 찾을 수 있다.

정보 유통(flow)의 왜곡은 한국사회의 역사문화적 특성(historicol-cultural characteristics)에서 파악될 수 있다.

Ⅳ-3-1 '사회적 신뢰' 구축의 미비

우리문화는 전통적으로 개인주의(individualism)보다는 집단주의(collectivism)의 성향을 보이며 집단주의 문화는 혈연, 지연, 학연의 사회적 관계망(social networking)을 중시하게 된다.[19]

이러한 가치지향성은 비단 한국뿐만 아니라 집단주의 문화유형을 보이는 '아시아 문화권' 에서 비록 그 정도의 차이는 있지만 공통적으로 나타난다.

한백문화재단과 일본 덴츠(電通)연구소가 공동으로 수행한 한.중.일 3국 국민의식 조사결과가 보여주듯 이들 국민들은 '성공하기 위한 가장 중요한 요소' 로서 '사회관계망의 형성' 을 꼽는데 주저하지 않는다.

특히 한국인 조사대상자 30% 이상이 이러한 인간관계와 사회관계망의 중요성을 인식하고 있다. 한국인의 의식은 한국적 사회환경에 최적화되어 응답된 것으로 파악된다. 즉 한국사회의 각종 이권과 정보의 유통은 '관계망' 이라는 제한적이고 특수한 틀속에서 이루어지고 있는 것을 구성원들이 인식하고 있다.

(단위 %)

	한국	일본	중국
가 정	96.7	80.7	88.0
지역공동체	47.3	41.3	25.0
도·시단위의 공동체	21.0	8.0	21.0
국 가	53.3	10.0	48.3
세 계	19.7	5.3	17.0

19) 한백연구재단, 한국인의 원형에 관한 델파이 연구 (1998)

(출처: 포럼 21. 1998 가을)

도표 1: 한국인의 사회적 귀속의식

(단위 %)

	타인에 대한 신뢰도			좋은 인간관계를 위해 자신의 의견을 분명히 밝히는 것			전체를 위한 타인에게 협조			어려운 일을 혼자서 해결한다		
긍정	71.6	61.0	89.7	91.7	83.7	84.0	82.7	74.0	77.7	45.0	25.3	66.0
부정	26.7	38.3	7.3	7.3	14.7	13.3	13.7	25.0	15.6	54.3	71.7	9.6
무응답	1.7	0.7	2.7	1.0	1.3	2.3	3.7	1.0	6.3	0.7	3.0	3.3

(출처: 포럼 21, 1998, 가을)

도표 2: 한국인의 인간관계 인식

미국의 사회학자 프랜시스 후쿠야마(Francis Fukuyama)는 사회학적으로 사회적 신뢰도(social trust)가 낮은 사적 관계망을 중심으로 구성된다고 파악하며 특히 한국사회는 사회적 신뢰도가 구축이 안되어 사적 관계망이 발달한다고 본다(. 후쿠야마는 또한 지식정보화 사회에서 한 사회가 발전을 이루기 위한 가장 중요한 사회적 자원(social capital)으로서 사회적 신뢰도를 지적한다.[20]

이러한 관점에서 본다면 한국사회에서 '사설정보지'가 범람하고 그 폐해가 증가하는 것은 한국사회가 지식정보화 시대에 필수불가결의 요소인 '사회적 신뢰'를 아직 구축하지 못했다는 점을 경고하는 방증이기도 하며, 역으로 강력한 '연고주의'가 사회적 신뢰 구축의 핵심적 장애물이기도 하다.

이는 과거 권위주의 통치 시대에 국가가 정보의 생산과 유통을 사실상 독점했던 시절에 그 정보 내용의 신뢰성과 유통의 투명성 확보에 실패한 데에서도 크게 기인하는 것으로 파악된다. 통치의 목적상 오도된 정보가 정부에서 생산되어 일반에게 유통될 경우 사회구성원들의 '공적 정보'에 대한 신뢰는 저하될 수밖에 없다. 정부발표를 믿으면 바보라는 말과 정부발표는 그 반

20) Fukuyama, Francis, *Trust* (Waner and Bros, 1999)

대로 받아들이면 된다는 극도의 불신과 냉소주의는 여기에 기인한다.

정보가 곧 경쟁력으로 환원되는 정보화 사회에 있어서 국가가 제공하는 정보의 신뢰성과 투명성이 확보가 안된다면 사회공동체 구성원들은 제각기 '사적 관계망(private network)'을 동원하여 정보수집에 나서게 되며, 더 나아가서는 사설 정보업체(private intelligence service)에 의존하게 되는 악순환의 고리에 빠져들게 된다.

IV-3-2. 권력의 집중과 미분화

한국사회는 삼국시대 중앙집권 왕조체제의 확립 이후 전통적으로 강력한 중앙집권 체제를 이룩하면서 상대적으로 지방분권과 권력의 분산이 이루어지지 못했으며, 이는 봉건영주체제를 기반으로 발전하여 분권화의 전통을 간직하고 있는 유럽사회와는 다른 모습을 보인다.

권력이 하나의 정점으로 집중된 사회에서는 통상 공동체 구성원들의 삶의 조건에 대한 결정이 이루어지는 '중앙'에 대한 정보를 갈망하고 민감할 수밖에 없다. 또한 권력이 정점에 집중된 사회에서는 대다수 구성원은 핵심정보 접근성이 떨어질 수밖에 없어 '소문'과 '풍문'에 의존하는 경향도 수반되며, 그 소문의 확산도 소문이 검증되고 소멸할 수 있는 제동장치로서의 공인된 기관이 중앙을 제외하고는 전무한 상태에서 '발없는 말이 천리를 간다'는 속담처럼 신속하고 광범위하게 된다. 이는 마치 방화벽(fire wall)이 존재하지 않는 상태에서 화재의 확산과도 같은 현상으로 인식된다.

이러한 한국사회의 전통은 현대사회에 접어들어서 권위주의 정치체제가 장기간 지속되면서 더욱 고착화되어 왔다. 사설정보지 폐해의 현황에서 살펴본 바와 같이 사회적 파장을 불러일으키고, 심대한 폐해를 야기하는 '왜곡된 정보' 중 상당 부분이 '권부의 핵심'을 둘러 싼 정보인 것이 이를 증명해 준다. 이는 우리사회가 그만큼 권력이 과도하게 집중되고, 분산되지 못했다는 방증이기도 하다.

최고권부에 관한 '정보'를 그 최고권부 이외의 여타 기구가 '교차검증'할 수 없는 상황에서는 그 '왜곡된 정보'가 정정되기 어렵기 때문에 일단

생산된 정보가 검증을 통하여 통제되지 못하고 확산되며 따라서 그 피해도 확산된다.

또한 한국사회가 가치의 분화와 다양화, 그리고 지식정보화 시대에 부응한 발전을 이룩하기 위하여 반드시 해결해야할 과제이기도 하며 법적, 제도적 장치 마련 역시 이러한 관점에서 접근되어야 할 것이다.

사설정보지 범람과 사회적 폐해 문제는 한국의 역사문화적 관점에서 사적관계망에 대한 의존에 따른 사회적 신뢰의 결여와 더불어 과거 한국사회의 권위주의 통치체제에 따른 정보유통의 왜곡과 불투명성에서 찾을 수 있다. 과거 권위주의 통치에 따른 언론기능의 왜곡은 일반국민들로 하여금 국가와 언론을 통하여 공개되는 정보에 대한 사회적 불신을 가중시키고, '공식적 정보' 이외의 '비공식적 정보'를 추구하게 되고 그러한 정보들을 오히려 신뢰하고 의존하는 소위 '유비통신' '카더라 통신'을 범람하게 만들었다.

어느 사회에나 '소문(rumor)'의 횡행은 발생하나, 공신력을 담보한 정부기관이 그 소문의 진위를 판명해 줄 경우에도 그 소문의 확산이 멈추지 않는 것이 우리사회의 특징으로 이는 기본적으로 정부가 신뢰성을 구축하지 못했기 때문이다.

또한 일반적으로 '비상식적'으로 여겨지는 '소문'들 중 일부는 추후에 정부의 공식적 '부인'에도 불구하고 '사실'로 증명되곤 하는 상황에서 사회적 비상식성은 더욱 증폭되어 왔으며, 민주화시대를 맞이하여 언론과 정보의 자유화가 이루어지면서 자연히 '사설정보지'에 대한 수요가 증대하고, 그 불확실성에 대한 '신뢰'가 증대하게 된 것이다.

범람하는 사설정보지의 사회경제적 폐해에 대응하기 위한 사회적 장치 마련 역시 이러한 문제의식과 분석을 기반으로 이루어져야 할 것이다.

상기 사설정보지 현황파악에서 지적되었듯이, 사설정보지에 대한 검경의 대대적인 단속은 일면 표면적으로 긍정적인 효과를 나타내기도 하지만, 내면적

으로 살펴보면 단속의 여파로 그러한 '사설정보' 의 유통이 공개적인 경로를 통해 이루어지지 못하고 '1대1' 의 밀실 대화의 방식을 택하는 '음지화' 를 조장하기도 한다.

정보화 시대에 우려되는 대표적인 '부작용' 으로 흔히 '디지탈 디바이드(Digital Divide)'가 지적된다. 정보화 시대의 ' 수단 '을 확보한 계층과 그렇지 못한 계층간의 격차를 의미한다. 이러한 연장선상에서 ' 인포메이션 디바이드(information divide)' 역시 지식정보화 시대의 경계하여할 부작용이라면, 단속을 통하여 양지의 '사설정보' 를 음지로 숨어들게 만든다면 위에서 살펴 본 바와 같이 정보의 '가격' 만을 상승시키고, 또한 더욱 은밀하게 유통되어 일반인들은 정보의 접근성에 더욱 취약하게 되며 정보의 '부익부 빈익빈' 현상을 초래하게 될 것이다.[21]

이는 곧 지식정보화 시대가 가장 우려하는 점으로서, 지식정보화 시대에 오히려 지식정보로부터 소외되는 계층을 양산시키고, 특정계층에 의한 지식정보의 독점과 'information divide'를 가속화시킬 우려가 다분하다.

현재 추진되고 있는 사설정보지 업체의 등록제는 사설정보 업체들에게 '문제' 를 야기하는 정보에 대해 차후 책임소재를 명백히 할 수 있다는 점에서 업체들이 정보의 수집, 생산, 유통에 있어 정확성과 신뢰성에 신중을 기하게 하는 효과는 기대할 수 있다.

그러나 '정보 유통' 의 속성상 왜곡되거나 오도된 정보로 인한 개인적, 사회적 피해는 현실적으로 적절하게 구제되기 어렵다는 현실적 문제를 예방하기에는 한계가 있다. 특히 IT(Information Technology)산업의 발전이 세계 최고수준을 자랑하는 한국사회에서 정보공개와 유출에 따른 문제를 인지하고 법적, 제도적 구제조치를 취할 시점에는 이미 그 정보가 광범위하게 확산되고 '저장' 된 이후가 되며, 피해 정도에 따른 '보상' 과 '배상' 은 말할 것도 없고 '명예회복' 도 불가능할 정도로 '엎질러진 물' 인 경우가 태반이다.

---

21) Drucker, Peter, *Post-Industrial Soceity,* (Stanford University Press, 2001)

Ⅳ-3-3. 공론의 장의 미발달

공론의 장이 아닌 사회적 관계망 속에서만 유통되고 소비되는 사설정보 흐름의 특성은 해당 정보의 교차검증(cross-checking)과정을 원천적으로 봉쇄한다.

Ⅴ. 해외사례 연구

연구의 필요성에서 제기한 바와 같이 '사설정보지' 문제에 대한 생산적 대응책 마련은 지식정보화 사회의 당위성과 개인의 사생활 보호와 사회의 합목적성이라는 양면성의 접점에서 이루어져야 한다.

가치교환적(trade-off of values) 상황의 사회적 문제를 자칫 단면적 고찰에 기반한 대응책은 이면적 가치의 중대한 훼손으로 이어질 수 있다. 사회적 합목적성과 기능주의적 관점만을 강조한다면 지식정보화 시대가 요구하는 새로운 지식정보의 창출이라는 활력을 훼손하게 될 것이며, 또한 가치의 다양성을 담보하기 위한 '자유'와 '시장 논리'만을 보호한다면 역시 사회적 기능의 현저한 훼손이라는 대가를 지불하게 될 것이기 때문이다.

본장에서는 1) 정보화 시대에 개인의 사생활 보호와 정보 수집과 생산, 유통, 그리고 소비의 자율성의 최적점을 찾기위한 전세계 36개국의 간략한 현황을 통해 세계적 추세의 파악을 위해 살펴보고; 2)이들 국가 중 한국사회에 시사점을 줄 것으로 판단되는 5개국(미국, 영국, 프랑스, 일본, 싱가포르)에 대한 심층적인 사례연구(in-depth case-studies)를 통하여 사설정보지 문제에 대하여 한국사회의 적절한 대응책 마련의 하나의 준거틀(framework)을 알아본다.

상기 5개국을 사례연구 대상으로 선정한 근거는 지식정보화 사회에서의 지식과 정보의 생산, 유통, 소비의 이율배반적 가치의 갈등 대처에 있어 이들 5개국이 이러한 가치조화에 있어 차별성을 보여주는 것으로 판단되기 때문이다.

세부적인 내용에 있어서는 국가별로 편차를 보이나 대별해 본다면 '개인적 가치와 자유'를 중시하는 역사문화적 전통을 보유한 미국은 사설정보(private intelligence)와 그의 유통(private intelligence report, service, agency)의 자유를 최대한 보장하는 방향성을 잡고 있으나, 사회통합적 가치를 중시하는 일본과 싱가포르등 국가는 지식정보화 시대를 관리해주는 기제로서 무제한적인 정보생산과 유통에 일정부분 제약을 존치시키는 경향성을 보인다. 반면에 개인과 전체의 '균형'을 강조하는 사회적 합의의 전통을 지닌 영국과 프랑스등 유럽국가들은 대체적으로 자유와 책임의 균형 속에서 해법을 찾고 있는 것으로 파악된다.

V-1. 36개국 cross-country analysis

한백연구재단과 일본 덴츠연구소(電通研究所), 그리고 노무라증권연구소(野村證券研究所)가 공동으로 다음 36개국가의 사생활 보호와 정보통신 관련 입법조치 사례들을 수집하였다:

사례국가 선택기준은 첫째, 사설정보와 사생활권의 침해, 그리고 사회통합의 가치의 연구와 한국사회에 시사점을 제공이라는 본 연구의 목적상, 첫째, 사설정보의 문제는 상기한 바와 같이 세계화, 정보화 시대의 필연적인 현상이라는 인식에 따라, 세계화와 정보화 정도가 일정수준 도달하여 우리사회와 유사한 고민을 공유하거나, 혹은 이미 그러한 문제를 경험하고 발전적 대안을 마련하여 효과적으로 작동하고 있는 국가들을 기준으로 하며; 둘째, 역사문화적 차별성과 유사성의 파악을 위하여 대륙별 안배를 기한다.

전체적인 조망의 결과는 정보기술의 발달에 따라 거의 모든 국가에서 사생활의 노출과 그에 따른 개인적 권리의 일부분인 사생활권이 침해되는 것이 전세계적인 현상으로 확인되며, 둘째, 정부와 대규모 기업군에 의해 개인정보의 유출과 저장이 광범위하게 발생하고 있음을 확인할 수 있다. 그리고 셋째 흥미로운 사실은 이러한 추세에도 불구하고 다소의 편차는 보이지만 많은 국가의 경우 개인정보보호를 위한 법적, 제도적 장치는 오히려 완화되고 있다는 점이다. 많은 국가의 경우, 기존의 개인정보보호법을 강화하기 보다 오히려 축소해석하는 경향을 보이며, 정보화 시대에 개인정보보호를 위한 새로운 입법은 시도되지 않고 있다는 점이다.

더욱 흥미로운 사실은 이러한 개인정보 유출에 따른 사생활 침해에 대해 시민사회의 문제제기는 꾸준히 이루어지지만 그 정도는 예상치를 밑돌고 있으며, 사회 전체적으로는 그 불가피성을 인정하는 방향으로 나아가고 있다는 점이다.

세계 각국의 이러한 추세는 최근 들어 더욱 두드러지고 있는 바, 그 원인 중 하나는 '테러' 위협의 증가에서 찾을 수 있다. 1989년 동서냉전 구조의 해체 이후, 냉전시대에 비교적 단순화되고, 획일화되었던 '외부의 위협 요소' 가 사라진 대신, 불특정 다수를 향한 무정형(無定型) '테러' 의 위협이 점증하고 있다. 이는 '바로 내 이웃이 위험인물' 일 수도 있다는 불안감의 확산으로 이어지고, 자신의 안전보장을 위해서는 '평범한 이웃' 까지도 의심해야 하며, 따라서 모든 개인에 대한 국가의 기본신상정보 파악을 불가피하게 받아들이는 경향을 보이게 되었다.

이 새로운 현상은 9.11테러 후의 미국과 런던지하철 테러 이후의 영국, 동경지하철 테러 이후의 일본에서 두드러지는 사회현상으로 보고된다. 이 사례를 한국사회에 적용해 본다면, 우리사회에서는 북한의 대남 위협의 정도가 국가의 일반 시민들에게 대한 정보파악에 대한 반응에 영향을 미치는 요소로 작용하게 됨을 유추할 수 있다. 현재 인권시민단체들을 중심으로 국가의 개인신상정보 수집에 대한 문제의 제기는 따라서 그간 진행되어 온 남북간 긴장완화에 따른 결과라는 점도 인식할 필요가 있으며, 이러한 주변여건에 따라 정부의 정보정책이 탄력적으로 운영되어야 함을 시사한다.

개괄적으로 아시아 국가들, 특히 사회통합을 강조하고 공동체주의를 강조하는 유교문화권 국가들은 국가의 개인신상정보 수집과 저장에 대해 관용적인 태도를 보이는 반면, 개인 중심으로 사회를 파악하는(국가는 개인을 위해 존재) 문화를 지닌 서구 국가들은 이 문제에 대해 민감한 반응을 보이고, 국가의 '감시(eye)'로부터 사생활 보호를 위한 강력한 통제와 규제장치를 요구하고 있다. 그러나 세계화에 수반되는 ' 문화의 세계화 '의 추세에 따라 ' 개인가치(individual values)'를 강조하는 서구적 가치가 전세계적으로 확산되면서 아시아적 가치(A냠n values)를 중심으로 하는 유교문화권의 아시아 국가에서도 점차 사생활과 개인정보의 비밀성을 요구하는 목소리가 높아지고 있다는 점 역시 우리사회의 정보정책을 입안하는 데 있어 시사하는 바가

있다.

그리스(Greece)

그리스 헌법은 프라이버시와 통신비밀법을 보장한다.
개인정보 보호법은 1997년 발효되었으며, 그리스는 유럽의회의 개인정보 보호법을 채택한 마지막 유럽 국가이며[22], 유럽의회의 명문규정을 원안대로 채택하였다.

그리스 프라이버시 보호법은 정부의 일반시민에 대한 도감청을 기본적으로 금지하고, 법원의 허가를 요구하지만 아직까지 정부에 의한 불법 도감청 사례는 빈번하게 야기되고 있다.[23]

남아프리카 공화국

1996년 남아프리카 공화국 헌법은 사생활권을 보장한다.
1996년 이후 남아프리카 공화국 헌법재판소는 수차례에 걸쳐 음란.퇴폐 사진의 보유 문제에 관련된 사생활권의 해석에 관한 재판을 실시하였는데, 이 재판들에서 재판소는 개정 헌법이 아닌 구헌법에 의거한 판결을 하였다.

정보접근법은 2000년에 제정되었으며, 이 법은 정보에 대한 접근권과 유출제한은 물론, 공기관과 사기관에 저장된 개인정보에 대한 정정 요청 권리까지 인정하고 있다. '열린 민주 법안(Open Democracy Bill)'로 명명된 이 법은 포괄적인 정보 보호 장치까지 포함하고 있었으나 1999년 의회의 결정에 의하여 제외되었다. 남아프리카 공화국의 사생활과 개인정보 보호법은 아직까지 초기단계에 머물러 있는 것으로 평가된다.

남아프리카 공화국은 사생활 보호 위원회는 두지 않고 헌법 9조에 의거한 인권보호 위원회를 설치 운영하고 있으나 이 위원회는 정보 접근법에 관한 권한은 거의 갖지 못하고 있다.[24]

---

22) The Reuters European Community Report, June 10, 1997.
23)The Guardian, May 22, 2000.
U.S. Department of State, Greece Country Report on Human Rights Practices for 1997, January 30, 1998. See also Greece Report, Human Rights Watch World Report, 1998.
24) Report of the Ad hoc Committee on Open Democracy Bill [B 67-98], Parliament of the Republic of South Africa, January 24, 2000.

1996년 남아프리카 공화국 경찰이 수천건의 국내외 전화 통신을 법원의 영장없이 도청한 사실이 적발되었으며, 2000년 정부는 독일 대사관에 정보 카메라를 비밀리에 설치한 사실을 공식 사과하기도 하였다. 또한 1999년 야당은 정부가 국회내 야당 사무실과 중앙당사에 도감청 장비를 설치한 것을 적발하였다고 발표하기도 하였다.[25]

현재 남아프리카 공화국에는 개인정보 보호를 위한 특별한 법적 장치가 마련되어있지 않고, 단지 헌법상 명시된 사생활권 뿐이며, 이 조항은 사생활권의 보호를 단지 개인 신체(injury to the personality)의 위해 정도로만 규정하고 있다.[26]

노르웨이

노르웨이 초기 헌법인 1814년 헌법에는 사생활권 보호 규정이 명확치 않다. 단지 102조에 범죄의 경우가 아니면 개인 주거를 검문할 수 없다는 조항만 있으며 110조에서 정부는 시민들의 '인권을 존중' 해야 한다는 일반론적 언급만 있을 뿐이다. 노르웨이 대법원은 1952년 개인에 대한 보호를 사생활권 보호로 확대해석 해야 한다고 판시하여 사생활권에 대한 보장이 이루어졌다.[27]

개인정보등록법은 2000년 제정되었는데 이는 EU 규정을 따르고 있다. 또한 새로운 등록법은 비디오 감시와 유전자 감시 등 특수한 규정까지 두고 있으며 1978년의 개인정보등록법을 대체하였다.[28]

도감청은 법원의 영장을 얻어 4주간의 제한된 시간내에만 실시할 수 있다. 1994년 국회 조사위원회가 설치되어 2차대전 이후 노르웨이 경찰과 보안당국의 시민 감시 실태조사가 이루어져 사복경찰의 좌익 세력등에 대한 적절치 못한 감시행태에 대한 논란이 야기되었다.

비밀경찰의 새로운 감시규정이 1995년 제정되어 경찰과 군 보안당국의 시민

---

25) "Newspaper Uncovers 'Unlawful' Tapping by Intelligence Units," The Star, 21 February 1996.
26) David Shapshak, "SA services get 'smart'," Mail & Guardian, April 24, 1998.
27) Government of Norway report to the UN Human Rights Commission, CCPR/C/115/Add.2, 26 May 1997.
28) "Judicial Inquiry into Norwegian Secret Surveillance," Fortress Europe, FECL 43 (April/May 1996).

감시체제를 규제할 '규제위원회(Control Committee)'가 구성되었다.

1971년 제정된 정부정보 접근법은 매우 폭넓게 실행되고 있으나 의회와 감사원 문건은 여기에서 제외된다. 또한 내무부의 정보중 국가안보와 대외관계에 위해를 가할 우려가 있는 정보도 이에서 공개와 일반열람에서 제외된다.[29)]

네덜란드(Kingdom of Netherlands)

네덜란드 헌법은 명시적으로 프라이버시 보호를 규정한다. 2000년 '디지털 시대의 헌법적 권리(Constitution rights in the digital age)'를 위한 정부위원회는 네덜란드 헌법개정을 청원하였다. 이 위원회는 e-mail의 비밀을 개인서신의 프라이버시 포함 여부에 관한 혼란과 논쟁 이후에 설치되었다.[30)]

2000년 의회 승인절차를 마친 개인정보보호법은 1998년 정보등록법을 수정 보완 한 것으로, 이는 유럽의회의 정보보호 규정(European Data Protection Directive)을 네덜란드 법체계에 일원화 시킨 것이다.

통신의 절취(interception)는 형사범으로 다루어지며, 1998년 승인된 새로운 정자통신법은 모든 인터넷 서비스 제공자는 2000년까지 법원의 요청에 의해 모든 인터넷 사용자의 신원추적이 가능하도록 하고, 로그인 사용자의 정보를 3개월간 보존하도록 하고 있다. 이 새로운 법안은 네덜란드의 한 인터넷 서비스 업체인 Dutch ISP가 가입자에 대한 광범위한 신원조회를 거부한 직후에 마련되었다.

네덜란드 정보기관은 정보수집 행위에 있어 법원의 허가를 필요로 하지 않지만 각 유관부처 장관의 위임을 받아야 한다. 현재 계류 중인 새로운 정보법은 정보기관에 더욱 많은 권한을 부여하고 있다. 만약 이 법안이 통과된다면 정보기관은 모바일 폰을 비롯한 모든 무선통신에 대한 검색이 가능하게 된다.

1996년 네덜란드 법무성 조사에 따르면 네덜란드 경찰은 미국, 영국, 독일보다도 많은 전화감청을 실시한 것으로 나타났다. 의회 조사 위원회는 경찰

---

29) "Parliament says people can see files," Statewatch bulletin, May-June 1997, vol 7 no 3.
30)Reuters World Service, November 20, 1996.

감시에 대한 법적 제한에 대하여 부정적인 견해를 나타내고 있다. 네덜란드에서 유난히 많은 도감청이 실시되는 이유는 네덜란드가 다른 수단에 의한 검색을 불법화하고 있기 때문이기도 하다.[31)]

뉴질랜드(New Zealand)

뉴질랜드의 프라이버시 보호권리는 1993년 제정되어 수차례 개정되었다. 뉴질랜드 프라이버시 법(Privacy Act)은 공공분야와 사적분야에서의 개인정보의 수집과 이용, 그리고 유출을 통제하며, 또한 개인들에게 모든 정보수집기관에 의해 수집, 저장된 본인의 정보에 접근할 수 있는 권리를 보장한다. 프라이버시 법이 규정하는 '개인정보(personal information)'이란 자동, 수동으로 처리된 모든 개인의 신분이 노출되는 정보를 망라하고 있다. 그러나 미디어에 의한 보도는 프라이버시 법에서 제외되는 특징을 갖고 있다.

뉴질랜드 프라이버시 법은 12개의 정보 프라이버시 원칙으로 구성되어 있는데, 이는 기본적으로 1980년 OECD의 가이드라인과 1988년 호주의 프라이버시 법 원칙에 기반하고 있다.[32)]

정보 프라이버시 원칙 이외에, 이 법안은 정부 기관에 의해 운영되는 정보일치 프로그램에 관한 절차와 가이드라인을 제시하며, 특별 정부기구들이 법집행 과정에서의 개인정보 공유에 관한 특별 조항을 두고 있다.

덴마크(Kingdom of Denmark)

1953년 덴마크 헌법은 사생활권과 정보보호에 관한 두가지 조항을 담고 있다. 1992년 유럽인권 헌장(the European Convention of Human Rights)이 덴마크 헌법에 적용되었다.[33)]

'정보관찰기구(Registertilsynet)'라는 독립된 기관이 이 두가지 법률 조항을 관할한다. 이 기구는 개인 정보의 등록과 공개의 조건을 확정하며 개인과 정부 공공기관의 정보 이용에 관한 특별 경우의 해석도 담당한다.[34)]

---

31)Personal Data Protection Act, Staatsblad 2000 302, 6 July 2000. (unofficial translation), <http://www2.unimaas.nl/~privacy/wbp_en_rev.htm>.

32) Constitution of the Kingdom of the Netherlands 1989,

33) "Denmark: Surveillance of political activity admitted," Statewatch bulletin, vol 8 no 2, March-April 1998.

34) "Envoy to Denmark: We're Not Spies," Associated Press, April 3, 2002.

도청은 형법으로 규제되며, 1988년 정보기관(PET)이 1960년대와 80년대에 걸쳐서 이미 1968년 불법화된 도청을 좌익 급진주의자들에 대해 실시한 사건에 대한 조사가 이루어지기도 하였는데, 이 조사에서 정보기관 관리가 좌익 정치 기구에 대한 도청을 시인하였다.[35]

독일(Federal Republic of Germany)

독일기본법 10조 1항: 사신과 통신의 프라이버시는 침해할 수 없다. 2항, 예외사항은 헌법조항에 위배될 때만 가능하다.

1983년 독일연방법원은 공공 이익에 대한 현저한 위해요소가 인정될 경우 프라이버시에 대한 제한을 인정하고 있다.

독일 헤센주는 1970년 세계최초의 개인정보 보호법을 발효시켰으며, 1990년 연방 개인정보 보호법이 발효되었다.[36]

독일의 프라이버시 보호법은 유럽공동체의 규정과 마찰을 보여 2000년 유럽인권보호 위원회로부터 제소당했으나, 독일은 국내법을 유럽규정에 맞추는데 여전히 미온적인 태도를 견지하고 있다. 1998년 독일의회는 12년간의 지루하고 치열한 논쟁 끝에 마침내 법원의 영장이 발부된 경우에는 개인 가정에 대한 도청장비 설치를 합법화하는 법안을 통과시켜 프라이버시와 공익성의 조화점을 추구하는 '조직범죄 대응능력 향상법'을 통과 시켰다.[37]

독일연방법은 아직까지 정보이용 자유에 대한 법률을 제정하지 않았지만, 1998년 브란덴부르그주를 시발로 슐레즈비히, 홀스타인주등이 일반시민의 정부기록 열람의 권한을 허용하였다.[38]

러시아

---

35) "Denmark: PET involved in "illegal" surveillance," Statewatch bulletin, vol 8 no 5, September-October 1998.

36) Federal Act on Data Protection, 27 January 1977 (Bundesgesetzblatt, Part I, No 7, 1 February 1977), Amended 1990.

37) Federal Act Establishing the General Conditions for Information and Communication Services - Information and Communication Services Act - (Informations- und Kommunikationsdienste-Gesetz - IuKDG) 13 June 1997

38) "New Powers For The Border Police: Checks Anywhere At Any Time," Fortress Europe, FECL 56 (December 1998).

러시아 헌법 23조는 프라이버시의 권리와 개인정보 보호, 그리고 통신상 비밀보장, 개인의 명예 보호를 규정하고 있다. 또한 24조는 본인의 동의없이 개인 사생활에 대한 정보를 수집, 저장, 유포하는 행위를 금지하고 있으며, 정부 기관과 지방자치정부, 그리고 그 공무원들은 법률에 저촉되지 않는 한 개인에게 영향을 줄 수 있는 모든 정부 정보에 대한 접근허용을 의무화하고 있다.

1995년 러시아 의회는 개인 정보 보호와 처리에 관한 연방법을 제정하였으며, 이 법은 정부와 사영역에서의 정보보호와 사영역에서의 개인정보 취급자에 대한 면허증 제도를 법제화하고 있다.[39]

그러나 러시아 정부는 개인정보 보호를 위한 중앙 주무부서를 두지 않고 있어 그 실효성은 의문시되고 있다. 또한 인터넷 사용자들에 대한 프라이버시 보호도 매우 제한적으로 적용되고 있다.

통신비밀은 1995년 통신법에 의해 보장되었으며, 수사 방법상의 개인 정보와 사생활 침해 방지 역시 법으로 명문화 되었다.[40] .

리투아니아

리투아니아는 개인정보 보호법을 1996년 발효시켜 1998년 그 보호영역을 사기관에 저장된 개인정보까지 확대시켰다. 또한 정보에 대한 접근과 수정요청권까지 포함시켰다.

1996년 국가 개인정보 보호 위원회(State Data Protection Inspectorate)가 설치되어, 이곳에서 개인정보 취급자들을 등록시키고 정보처리와 취급에 관한 교육과 관리를 담당하고 있다. 이 위원회는 622명의 정보 취급자들을 보유하고 있다.[41]

---

39) Regulation on Statistical Data Collection and Public Competence in Data Processing, Law N. 71 of 23 May 1995.

40) Decree N. 7 of 13 March 1984, “Establishment of a State Data Bank as provided for by Article 5 of Law N. 27 of 1 March 1983”; Decree N. 7 of 3 June 1986, “Integration to Decree N. 7 of 13 March 1984, Establishing a State Data Bank”; Decree N. 140 of 26 November 1987, “Procedures for the Establishment of Private Data Banks.”

41) United Nations Human Rights Committee, Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Initial reports of States parties due in 1993, Addendum, Lithuania, 1996.

리투아니아도 정보접근법을 갖고 있으나 이는 매우 제한적으로 인정되어, 공공문서에 대한 열람은 정당과 정치, 공공기관, 노동조합등에게만 부여되고 있다. 현재 리투아니아 인권센터에 의해 제안된 포괄적인 정보 접근법이 의회에 계류되어 있다.[42]

말레이시아

말레이시아 헌법은 사생활 보호권을 규정하지 않는다.

말레이시아 에너지, 통신, 다매체성(The Ministry of Energy, Communications, and Multimedia)은 개인신상정보 보호를 국가전자상거래 계획의 일환으로서 다룰 법안 초안을 준비중인 것으로 보고되고 있으나 현재 수년간 지연시키면서, OECD와 홍콩, 뉴질랜드등의 사례를 연구하고 있는 것으로 보고된다.[43]

말레이시아 정부는 개인신상정보 보호를 자율규제(self-regulation)의 방식과 정부개입(government intervention) 두가지 방안의 절충을 시도하고 있다.[44]

멕시코

1917년 멕시코 헌법 16조는 '개인의 신체, 가정, 가옥, 문서, 그리고 개인 사물은 적절한 법절차에 의해 책임 있는 당국에 의해 발부된 영장 없이는 외부로부터 침해받지 않을 권리' 를 보장하고 있다.

멕시코 형법 214조는 정부에 의해 수집된 개인정보의 유출을 법으로 금지하고 있다. 멕시코 '국민법(General Population Act)는 국민등록과 개인 신상정보 수록 작업을 관장한다. 등록의 목적은 국가를 구성하는 모든 개인 정보를 정리함으로써 그들의 신원 신뢰성을 제고하는 데 있다. 그 궁극적인 목적은 국민 모두에게 ID 카드를 발급하여, 그 ID 카드에 실린 정보는 모두가 신뢰할 수 있게 하는 데 있다.[45]

---

42) Memorandum on the Submission of ARTICLE 19 Critique - Lithuanian Draft Law on "The Right to Receive Information"

43) Shamsul Yunos, "Legal need to protect privacy on the Net," The Malay Mail, June 9, 2000.

44) "Draft of Bill on Personal Data Protection ready by year-end," New Straits Times. October 2, 1998.

45) "Spy Network Stuns Mexicans, Raid Opens Door to Exposure of Government Snooping," The Washington Post, April 13, 1998.

그러나 이 법은 멕시코 인권단체들로부터 헌법 16조에 위배된다는 반대에 직면하고 있다. 그들은 집권당 PRI에 의해 전화도청이 반대파들을 견제하는 수단으로 광범위하게 사용되어 왔다고 주장한다. 1997년에는 얄리스코 주 대법원(Jalisco State Supreme Court) 전화내역이 도청된 것으로 드러나기도 하였다. 이에 따라 신임 비센테 폭스(Vicente Fox) 대통령은 모든 불법 도청의 핵심으로 지목되었던 공안경찰의 폐지를 약속하였다.[46]

벨기에

벨기에 헌법은 프라이버시의 권리와 개인통신 비밀을 보장한다.
개인정보의 이용은 1002년 발효된 정보보호법에 의해 제한되며, 개인정보 보호법의 수정은 1998년 유럽 규정에 따라 의회에서 통과되었다.[47]
그러나 많은 전문가들은 이 법안이 정부의 개인신상 정보 파일 관리와 처리에 대한 보호장치가 불충분하다고 비판한다. 이에 따라 1990년 벨기에 정부는 1944년 수집되어 그동안 보관하고 있던 5만7천명에 대한 개인신상정보를 파기하였다.[48]

개인통신에 대한 감시는 1994년 법에 의해 통제된다. 1994년 법 이전에는 개인통신 감시에 대한 법적제한이 존재하지 않았다.

2000년 벨기에 의회는 컴퓨터관련 범죄에 관한 법안을 통과시켰는데, 이 법안은 범죄수사에 필요할 경우 사법당국이 암호해독 전문가의 협조를 구할 수 있고, 관련 전문가는 국가의 요청을 거부할 수 없는 제도를 마련하였다. 이 법안은 개인의 프라이버시에 중대한 위협을 가할 수 있는 여지를 남겨 논란이 계속되고 있다.

브라질

1988년 브라질 헌법 5조는 사생활권의 보호를 명시하고 있다.
사영역과 공영역 공히 개인정보 보호를 위한 OECD 규정이 1996년 상원에

---

46) See United Nations Commission on Human Rights, Question of the follow-up to the guidelines for the regulation of computerized personal data files: report of the Secretary-General prepared pursuant to Commission decision 1995/114
"Anger as Big Brother spy tactics exposed," The Guardian (London), April 14, 1998.

47) Constitution of Belgium,<http://www.fed-parl.be/constitution_uk.html.>.

48) Act concerning the protection of privacy with regard to the treatment of personal data files, December 8, 1992., as amended by the Act of December 11, 1998 transposing EU Directive 95/46/CE of October 24, 1995

제청되어 통과되었다. 이 법안은 '어떠한 개인정보 유출도 금지되며, 부득이한 경우 반드시 법원의 허가와 당사자에 대한 통보와 고지'를 명문화하고 있다.[49]

브라질의 1988년 민주화 헌법 제 5조는 사생활권의 보호와 개인 서신과 정보를 본인의 동의 없이는 어떠한 경우에도 열람할 수 없도록 규정하고 있다.

개인정보 신장을 위하여, 사적영역에 대한 정보보호는 OECD 기준을 채택하고 있으며, 이 법안은 이러한 정보는 법원의 명령이나 본인의 동의 절차를 거치지 아니하고는 어떠한 경우에도 비밀을 보장하도록 하고 있다. 또한 모든 국민은 국가기관이 수집한 본인에 대한 정보를 열람할 권리를 보장받는다.

1996년에는 도청에 관한 법안이 채택되어 중범죄 예상의 경우에 한하여 15일간 제한적인 도청이 허용되며 법원의 명령에 의하여 15일간의 연장이 가능하다.

브라질은 1992년 전미 인권 협약(The American Convention on Human Rights)에 가입하였다. 그러나 여전히 불법 도감청 사례가 적발되어 사회, 정치적 물의를 야기하고 있는 바, 1966년 상 파울로 시장선거 후보였던 셀소 피타(Celso Pitta)는 자신의 집무실 전화회선 2개가 도청되고 있다는 사실을 발견하였으며, 그 이전에는 브라질의 부통령도 도청 당한 것으로 보도된다.[50]

불가리아

1991년 불가리아 헌법은 사생활권, 통신비밀법, 그리고 정보접근법을 인정하였다.

1996년에는 EU 가입을 위한 준비작업의 일환으로 포괄적인 정보보호법이 발효되었다. 불가리아의 개인정보 보호법은 EU의 정보보호법에 의거하고 있다. 이는 공영역과 사영역에서의 개인정보의 책임있고, 공평한 취급을 규정하고 있다. 이에 따르면 개인정보를 다루는 기관은 개인에게 당사자의 정보

---

49) "President transfers control of new intelligence agency to military," Agencia Estado news agency, Sao Paulo, BBC Summary of World Broadcasts, April 11, 1996.

50) "Brazil vice-president claims his phone was tapped," Reuters North American Wire, September 9, 1992.

를 취합하는 이유를 명백히 설명하고, 취합된 정보의 요처를 고지해야한다. 또한 모든 개인이 기관에 저장된 자신의 정보를 열람할 수 있어야 한다.[51]

그러나 1997년 유럽 위원회(European Commission)는 불가리아의 정보보호법이 유럽연합 수준에 이르는 실효를 거두기 위해서는 보완해야 할 점이 여전히 남아 있는 것으로 평가하였다.

1999년 미국 국무성 인권보고서는 불가리아 내무성 장관 기관의 도청이 광범위하고 불법적으로 자행되고 있으며, 경찰에게 개인의 금융정보와 기록이 적법절차에 의하지 아니하고 이루어지고 있다고 발표하였다. 실제로 2000년 불가리아 검찰총장의 아파트에서 도청장비가 발견되기도 하였다. 또한 불가리아 군 검찰은 1996년 야당 당사에서 불법도청 사례를 적발하여 고발하기도 한 사례에서 보듯 민주화 이후 불가리아에서 개인정보와 사생활권에 대한 제도적 장치는 정비되었으나 그 실효적 운영은 여전히 미진한 상태이다.[52]

스웨덴

여러개의 법조문의 종합으로 구성된 스웨덴의 독특한 헌법은 개인정보 보호와 사생활권 보장에 관한 여러 개의 조항을 담고 있다.

스웨덴은 1998년 개인정보 보호법을 발효시켜 개인정보 보호에 관한 EU의 규정과 일치시켰다. 이 법안은 공공기관과 사기관의 개인정보 수집과 이용에 관한 규제를 법제화시키고 있다. 이 법안은 이미 1973년 세계 최초로 제정된 '사생활권 보호법'을 대체하고 있다.[53]

스웨덴의 정보감찰국은 독립된 기관으로서 정보법을 관할하며, 1999년 새로운 법에 의하여 정보관찰국은 409건의 민원을 접수하여 298건에 대한 수사를 실시한 것으로 집계되는데, 이는 해를 거듭할수록 수사 건수가 늘어나는 추세를 보여주고 있다.

---

51) Act concerning the protection of privacy with regard to the treatment of personal data files, December 8, 1992., as amended by the Act of December 11, 1998 transposing EU Directive 95/46/CE of October 24, 1995. <http://www.law.kuleuven.ac.be/icri/papers/legislation/privacy/tabel/index.html>.

52) Bulgarian Helsinki Committee, Human Rights in Bulgaria in 1997.

53) "Sweden: The personnel control system 1969-1996," Statewatch Bulletin, vol 9 no 1 (January-February 1999).

감찰국은 1998년 스웨덴의 경찰과 보안당국이 장기간에 걸쳐 주로 좌파 정치인 수천명에 대한 은밀한 내사를 벌여온 사실을 적발하였다. 스웨덴 검찰총장은 그 사실을 부인하였으나 동시에 내사에 관한 비밀 보고서를 작성한 것이 적발되기도 하였다. 54)

또한 이전에 스웨덴 통계국은 1953 출생한 1만5천명의 시민에 대한 음주, 종교, 성적취향등에 대한 개인정보를 감시한 것으로 나타나 감찰국에 의해 정보폐기를 명령받기도 하였다.55)

스웨덴은 전통적으로 정부 보유 정보에 관한 자유접근을 강조하는 노르딕 전통을 갖고 있어, 세계 최초의 정보 자유법인 "1776년 언론 자유법 '을 갖고 있다.

스위스

스위스의 1874년 헌법 36조는 서신과 전보의 비밀을 보장하였으며 1999년 국민토표에 의해 개정되었는데, 새 헌법에서는 사생활권 보호를 대폭 강화하였다. 헌법 13조는 '모든 국민은 사생활과 가정생활, 가정, 서신, 통신의 비밀을 존중받을 권리를 지니며 개인의 정보가 남용당하지 않을 권리가 있다' 고 명시하고 있다.56)

1992년 연방 정보보호법은 정부와 민간부문에서 취합하는 개인정보를 규제한다.

1999년 유럽의회 위원회는 스위스가 유럽의회 기준에 부합하고 있음을 결정하였다. 2000년 유럽위원회는 이러한 판단을 확정하였으며 앞으로 스위스에 유럽의 모든 개인정보를 이전하는 것을 허락하였다.

그러나 스위스에서는 심각한 정도의 도청사례가 적발되고 있다. 1993년 언

54) International Helsinki Federation for Human Rights, Human Rights in the OSCE Region: the Balkans, the Caucasus, Europe, Central Asia and North America, Report 2000.

55) Wayne Madsen, Handbook of Personal Data Protection, (New York: Stockton Press, 1992).

56) Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 5/99 on the level of protection of personal data in Switzerland, 7 June 1999

론인들과 장관들의 전화내역이 스위스 의회에서 도청된 것이 발견되었으며, 정보보호 위원회는 스위스 전화회사인 국영 Telecom PTT에 그 책임이 있는 것으로 판단하였다. 또한 1996년에는 연방정부가 언론인들에 의해 도청된 사실도 적발되었다. 1997년에는 국영 PTT가 개인의 휴대전화 위치 추적을 상당기간 한 것으로 드러나기도 하였다.[57]

슬로바키아

1992년 슬로바키아 헌법은 통신비밀과 개인정보보호, 그리고 사생활권을 보장하고 있다.

통신체계상에서의 개인정보 보호법이 1998년 2월에 제정되어 그해 3월 실시되었다. 이 법은 1992년 제정된 체코슬로바키아의 법률을 대체하는 것으로 유럽의회의 정보보호안을 준수하며 모든 경우에 공공기관과 사적기관의 개인정보 수집에 제한을 가하고 있다.[58]

개인에 대한 종교, 인종, 민족, 정치적 견해, 철학적 신념, 건강, 논조가입여부, 성등에 대한 정보의 수집, 저장, 유통이 법률에 의해 금지되고 있다.

이 법안에 따라 정보보호 위원회가 신설되어 이 법안의 적용과 관리를 담당하고 있다. 이 외에 정부정보에 대한 일반인들의 접근성도 보장되어 2000년 5월 정부정보 자유접근법이 통과되었다.[59]

아일랜드

아일랜드 헌법에는 명시적인 프라이버시 보호 조항이 포함되지 않았지만, 대법원은 헌법 40조 1항이 이를 대변한다고 판시하였다.[60]

아일랜드는 인권보호와 기본자유에 대한 유럽선언(European Convention for the Protection of Human Rights and Fundamental Freedoms)에 서명하고 비준했지만 다른 유럽국가들과는 달리 이 유럽선언을 국내법에 적용

---

57) "Commission adopts decisions recognising adequacy of regimes in US, Switzerland and Hungary," July 27, 2000.

58) Act No. 52 of February 3, 1998 on Protection of Personal Data in Information Systems. <http://www.statistics.sk/webdata/english/acts/act5298/act5298.htm>. Decree of the Statistical Office of the Slovak Republic of 11 May 1999 <http://www.statistics.sk/webdata/english/acts/155decre/155decre.htm>.

59) Act on Free Access to Information <http://www.infozakon.sk/zakon-schvalenyvnrsr.htm>

60) Department of Justice, Consultation Paper on Transposition into Irish Law, November 2002.

시키지는 않는다. 그러나 아일랜드 정부는 이 선언을 영국과 아일랜드의 평화협정의 일부분으로서 아일랜드의 헌법에 포함시킬 것이라고 발표하였다.[61]

2000년 개인정보 보호법이 발효되어, 개인신상 정보의 수집, 처리, 저장과 사용이 공공부문과 사적 부문 모두에게 적용되어 규제를 받게 되었다.

아르헨티나

1999년 아르헨티나 부에노스 아이레스 항소심 법원은 개인신상 정보처리는 당사자의 동의나, 당사자에게 통지된 경우에만 가능하도록 명시하였다. 또한 신용정보기관은 개인의 신용정보에 대하여 일정기간 동안만 정보를 저장하도록 명시하고 있다.[62]

1998년 아르헨티나 대법원은 개인정보 보호법을 인정하였는데, 이는 아르헨티나 헌법 43조와 유럽 개인정보 보호법에 기초하고 있다. 이 법안은 전자정보와 기록문서의 개인정보를 모두 망라하고 있다. 또한 이 법안은 개인정보를 수집, 처리, 저장, 제공할 경우 당사자에게 신속한 동의를 구할 것을 의무화하고 있다. 일반적인 정보 이외에 '민감한(sensitive)' 정보일 경우는 법에 의해서 규정되지 않은 경우는 수집 자체를 금지하고 있다.

1998년 부에노스 아이레스 시는 정부정보 공개법을 승인하였다. 이 법에 따라 모든 부에노스 아이레스 시민은 정부관리에 의해 수집된 정보와 재판과정의 문서를 열람할 수 있도록 하였다.

1984년 아르헨티나 정부는 미국의 인권선언(American Convention on Human Rights)을 국내법에 적용하였으며, 1994년 이후 이 인권선언은 헌법화되었고, 아르헨티나 대법원의 판결의 기준이 되었다.[63]

오스트레일리아

오스트레일리아의 개인정보에 대한 안전장치는 여전히 제한적으로 운영되고

---

61) Irish Data Protection Commissioner, Annual Report, 1998, p16

62) Decree No. 1616/96, Comment by Supreme Court of Argentina Comparative Law Research and Library Secretary

63) United Nations, 19th Annual Report of the Human Rights Committee, A/50/40, 3 October 1995.

있다. 연방정부나 6개 주정부 모두 프라이버시에 대한 명문화된 규정을 갖고 있지 않다. '인권헌장' 에 대한 논쟁은 활발하게 일어나고 있지만 실질적인 법안제출은 이루어지지 않고 있다.

오스트레일리아의 1988년 사생활권 보호법은 OECD 기준에 의거 11개 조항으로 구성되어있다. 여기에 1989년 소비자 신용정보 취급에 관한 규정이 추가되었으며, 2000년에 보수당 정권은 사적 부문에서의 사생활권 보호를 더욱 강화시켰다. 그러나 오스트레일리아의 사생활권 보호 조항은 일반적인 EU 규정에는 미치지 못하는 것으로 평가된다. 예를 들면 각 기관들은 자신들이 취합한 소비자 개인정보를 또다른 목적을 위해 이용하기 위해서는 당사자들의 동의를 얻어야만 하는데, 그렇지 않을 경우에 그 기관은 직접 통화를 통해서 지속적인 관계를 가질 의향이 있는지만 확인해도 무방하도록 되어있다.64)

또한 소비자 개인정보의 해외유출에 대한 제한도 제한적으로만 이루어지고 있어서, 기관은 개인정보가 보호될 수 있도록 '합리적' 인 절차만 밟도록 규정되어있지만 그 '합리성' 은 매우 자의적이고 편의적으로 해석될 여지를 남겨두고 있다.

오스트레일리아 정부는 그들의 사생활권 보호장치를 '가벼운 법적 장치(light touch legislative regime)'이라고 지칭하듯이 이는 사생활 보호의 최소한의 장치일 뿐이다. 이 법안은 고용인에 관한 정보 이용에 관하여는 규제의 상당부분이 면제되며, 미디어 업체는 자신들이 보유한 개인정보를 공공에게 커다란 제약없이 공개할 수도 있다. 또한 연간 매출 300만불 이하의 소기업은 또한 이 법의 규제에서 제외되기도 한다.65)

오스트리아

사회주의적 정치, 경제적 색채가 강한 오스트리아는 사생활권을 명시적으로 인정하지 않고 있다. 정보보호법의 몇몇 부분은 헌법의 보장을 받는다. 이 권리들은 유럽인권선언(European Convention of Human Rights)의 제한만을 받는다.

---

64) Parliament of the Commonwealth of Australia, House of Representative Standing Committee on Legal and Constitutional Affairs, Advisory Report on the privacy Amendment (Private Sector) Bill 2000 <

65) Eleventh Annual Report, Office of the Federal Privacy Commissioner, 1998-99

2000년 제정된 새로운 정보보호법(Datenschutzgesetz 2000- DSG 2000)은 유럽 규정을 오스트리아 법체계에 조화시킨 것으로 1999년 승인되어 2000년부터 시행되고 있으나, 새로운 법은 전문가들부터 불완전한 것으로 비판받고 있다.[66]

이 법안은 정보보호 위원회에 의해 운영되는데 위원회 보고서는 10만개의 개인정보 취급 기관들이 등록되어 있으며 매년 85건의 공식적인 항의와 1,200건의 비공식적인 요구와 민원이 접수되는 것으로 집계되고 있다. [67]

전화 도감청과 전자 감시는 형법으로 다스려지는데 전화 도청은 1년 이상의 징역형이 예상되는 범죄에 관한 수사일 경우에는 허용된다.

Auskunftspflichtgesetz 는 정보이용자유법으로서 연방정부 관리들로 하여금 소관부처에 대한 시민들의 문의에 책임을 지도록 규정하고 있으나 정부 문서에 대한 시민들의 접근을 허용하지는 않고, 해당 정보에 대한 시민들의 질의에 관리들이 답변하는 데 그치고 있다.

우크라이나

우크라이나 헌법은 프라이버시와 개인정보보호를 명문화하고 있다. 헌법 31조는 법률에 의하지 않고는 모든 개인의 서신, 전화, 전보등 모든 통신의 비밀을 보장하도록 명문화하고 있다.
현재 우크라이나는 정보보호법 신설을 준비하고 있다. 정보보호법 초안은 1999년 마련되었으며 이는 개괄적으로 유럽 인권 위원회 선언 108조와 독일 헤세주의 법안을 따르고 있다. 1970년의 정보 보호법은 개인의 재산권 보호에 관점을 두었으나 새로운 초안은 재산권 이외에 포괄적인 내용을 담고 있다.

1982년 제정된 수사운영법은 조직범죄와의 전쟁의 기본틀을 구성하고 있는데 여기에서 수사관들에게 광범위한 감시의 재량권을 부여하고 있다. 이 법안은 도청에 관한 명확한 절차를 규정하고 있지 않다. 도청에 관한 규정은

---

66) See Viktor Mayer-Schoenberger and Ernst Brandl, Datenschutzgesetz 2000, (Line Publishing Vienna, 1999).

67) Datenschutzgesetz - DSG, BGBl 1978/565 changed by 1981/314, 1982/228, 1986/370, 1987/605, 1988/233, 1989/609, 1993/91, 1994/79, 1994/632. <http://www.ad.or.at/office/recht/dsg.htm>.

명시되지 않은 비밀법에 의해서만 규제될 뿐인데, 이는 내무장관에 의해 결정된다.[68]

내무장관에게 제출되는 도청허가원에는 관리의 이름, 일시와 통신의 종류등을 명시하게 되어있지만 도청 건수와 사례에 관한 자료는 아직 공개되지 않고 있다. 또한 비밀법 11조에 따르면 의사, 신부, 변호사등은 자신의 고객에 대한 정보를 추궁당하지 않도록 되어있지만 실제로 법원은 의사, 신부, 변호사등으로부터 수집된 정보를 빈번히 이용하고 있는 실정이다.[69]

이스라엘

이스라엘 기본법(1992) 7항은 "모든 국민은 프라이버시 권리를 가지며, 본인으로부터 허가받지 않은 어떤 사람도 개인 구역에 들어갈 수 없으며, 개인의 신체에 대한 검색을 금지하고, 개인정보와 갱린의 기록에 대한 비밀 '을 보장한다.

사생활 보호법은 개인 신상정보의 자료은행에 저장하는 절차를 규제하고 있다. 공영역과 사영역을 막론하고 1만명 이상의 신상정보를 저장하는 기관은 정부에 신고하여야만 한다.[70] 자료수집과 저장은 그 목적이 분명해야 하고, 또한 당사자들의 접근이 보장되어야 한다.

그러나 이러한 규제에서 경찰과 보안당국에게는 광범위한 예외가 적용된다.[71]

통신의 침해는 1979년 제정된 비밀감시법(Secret Monitoring Law)에 의해 허용되어 왔으나 1985년 개정된 법안은 위반사항에 대하여 더욱 무거운 처벌을 명시하고 있다. 통신 침해시 경찰은 반드시 지역 부장판사로부터 허가를 취득해야하며, 한번에 3개월까지 연장될 수 있다. 또한 국가정보원은 수상이나 국방장관으로부터 서면 허가서를 받아 도감청이 허락된다. [72]

---

68) Directive of the Supreme Court of Ukraine, No.9 of November 1, 1996, 'On referring to the Constitution in administering justice'.

69) "Power company denies involvement in telephone tapping," BBC Summary of World Broadcasts June 02, 2000.

70) The Basic Law: Human Dignity and Freedom (5752 - 1992). Passed by the Knesset on the 21st Adar, 5754 (9th March, 1994). <http://www.israel-mfa.gov.il/gov/laws/dignity.html>.

71) The Secret Monitoring Law, 5739-1979, Laws of the State of Israel, vol. 33, pp. 141-146.

72) United Nations Human Rights Committee, Initial report of States parties due in 1993 : Israel. 09/04/98. CCPR/C/81/Add.13. (State Party Report), 9 April 1998.

인디아

1950년 제정된 인도헌법은 프라이버시에 관한 법률을 제정하지 않았으나, 1964년 인도 대법원은 헌법 21조에 제시된 '어느 누구도 생명과 개인적 자유를 법률에 의하지 않고는 박탈당하지 않는다' 는 조항이 묵시적으로 프라이버시 보호를 규정한 것으로 판시하였다.[73]

인도에는 개인정보 보호법이 별도로 제정되지 않고 있으며, 2000년, 인도정부는 정보기술법(Information Technology Act)를 통과시켰는데, 이법은 전자상거래의 포괄적인 규제환경의 조성을 위해 마련되었다. 1992년 인도 정부는 정부 정보에 대한 접근은 가장 기본적이고 필수적인 언론과 표현의 자유라고 규정하였다.[74]

중국

중국의 사생활권은 제한적으로 보호된다. 중국헌법 37조는 '중국인민의 시민권적 자유의 불가침' 을 명시하며, 40조는 '국가안전과 범죄 수사, 공공의 안녕을 위한 검찰조직의 필요를 제외하고는 개인 서신의 비밀과 자유' 를 보장하고 있다.

중국은 그러나 아직 정부의 사생활 침해를 방지하는 일반적인 개인 정보 보호법이 제정하지 않고 있다. 최근 점증하는 인터넷 사용에 따른 우려는 인터넷 사용에 대한 기술적, 법적 제한을 강화하게 하고 있다.[75]

통신비밀은 헌법과 법에 명시되어있으나, 현실적인 실효성은 거의 없다. 실제로 당국은 외국인. 외교관, 언론인과 반체제 인사들의 전화와 팩시밀리, 전자메일등을 광범위하게 도청하고 감시하고 있다. 1998년 중국을 방문했던 토니 블레어 영국 총리는 그의 호텔 침실에 대한 도청이 이루어진 것을 알

---

73) South Asia Human Rights Documentation Centre, Alternate Report and Commentary to the United Nations Human Rights Committee on India's Third Periodic Report under Article 40 of the International Covenant on Civil and Political Rights, July 1997.

74) United Nations, Human Rights Committee, Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Third periodic reports of States parties due in 1992 Addendum -India /1, 17 June 1996.

75) Gary Chapman, "China Represents Ethical Quagmire in High-Tech Age," Los Angeles Times, January 27, 1997.

고 분노하기도 했다.[76]

칠레

1999년 칠레는 “사생활 보호를 위한 법 ‘을 제정하여 라틴 아메리카 최초로 정보 보호법을 통과시킨 국가가 되었다. 그러나 정보보호를 관할하는 부서가 따로 설치되지 않고 정보보호법은 사안에 따라 개별 부서에서 처리되고 있으며 정보보호법의 실효성을 검증할 판례 역시 아직 나타나지 않고 있는 실정이며, 또다른 결함은 정보의 제3국 유출에 대한 제한이 명시되지 않고 있다.[77]

1990년 칠레는 민주화를 이루었고, 전미 인권 협약(the American Convention on Human Rights)에 가입했지만 정부 관리에 의한 사생활권 침해를 종식시키지는 못했다. ‘수사경찰(인터폴 및 칠레 군부 수사국과 밀접한 업무교환을 하는 민간 사복 경찰 조직)은 칠레의 모든 성인 남녀의 신상기록을 보유하고 있으며 시민들이 항상 소지해야 하는 신분증을 발급하고 있다. 군부통치 기간 중 작성된 개인 신상정보들은 여전히 파기되지 않고 있다. [78]

캐나다

캐나다 헌법과 인권헌장에 사생활권은 명시되어있지 않다. 그러나 인권헌장 8조는 불합리한 체포를 금지하는 것으로 해석되며 캐나다 법원은 사생활권에 대한 합리적인 기대를 인정해 왔으나 2000년 실리아 파인스톤(Shelia Finestone) 상원의원이 제안한 ‘사생활권 헌장(Charter of Pravacy Rights)'는 모든 캐나다인들에게 사생활권의 헌법적 보장을 부여할 것으로 기대된다.

이 법안의 특징은 물리적 사생활권 뿐만 아니라 심리적 사생활권까지 포함하고 있는 점이다.

그러나 캐나다 연방 ‘사생활권 위원회(Federal Privacy Commission)'의

---

76) W.J.F Jenner “China and Freedom” in Kelly & Reid, Asian Freedoms (Cambridge University Press, 1998).

77) Chile: A Country Report, 1994: U.S. Library of Congress.

78) United Nations, Human rights committee concludes consideration of Chile's fourth periodic report, March 25, 1999.

브루스 필립(Bruce Phillip)은 캐나다의 사생활 보호법은 여전히 비디오 감시체제, 약물과 DNA 테스트등 '생의학적 사생활권(biomedical privacy)', 신체적 사생활권등의 문제에 있어 한계와 개선의 여지가 남아있다고 평가한다. 79)

이러한 문제점에 대하여 유럽위원회는 2001년에 캐나다와 국가간 정보이동을 허용할 것인지 문제를 놓고 캐나다가 적절한 수준의 사생활과 정보보호 조치를 취하고 있는지 검토를 시작한다고 발표하였다.80)

타이완

1994년 타이완 헌법은 통신의 프라이버시를 보장한다.
컴퓨터에 의한 개인정보 보호법은 1995년 발효되었으며, 이 법안은 개인신분에 관한 정보는 정부나 사설기관 모두에 의해 이용되는 것을 금지하고 있다.
그러나 이 법률을 시행하는 통괄부처는 마련되지 않아 혼선을 빚고 있는 실정이다.81)

대만 의회는 1999년 통신보호와 감시법을 승인하여 도감청에 대한 더욱 엄격한 규정을 마련하였다. 그러나 도감청은 여전히 '국가안보'와 '사회질서'의 명분으로 광범위하게 허용된다. 대만 검찰부의 발표에 따르면 1996년 한해에만 약 1만5000건의 '정치적 사찰' 성격의 도청이 행해진 것으로 보고된다.

2000년 대만 법무부는 각 은행이 보유한 모든 개인의 금융정보를 재무부에 통고하라는 요청을 하였으나 재무부에 의해 거부되었다.

1997년 대만정부는 모든 개인의 건강보험, 운전면허, 세금정보등이 수록된 개인별 '스마트 카드' 발급을 계획하였으나 개인신상정보의 무제한적 노출에 대한 우려로 무효화되었다.

---

79) Privacy Commissioner, 1999-2000 annual report, May 2000. <http://www.privcom.gc.ca/english/02_04_08_e.htm>.

80) European Commission, Data protection: Commission adopts decisions recognising adequacy of regimes in US, Switzerland and Hungary, July 27, 2000. <http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm>.

81) Constitution of the Republic of China, Adopted by the National Assembly on December 25, 1946, promulgated by the National Government on January 1, 1947, and effective from December 25, 1947. <http://www.oop.gov.tw/roc/charter/echarter.htm>.

타이완

1994년 개정된 타이완 헌법은 통신의 프라이버시를 보장한다.
컴퓨터에 의한 개인정보 보호법은 1995년 발효되었으며, 이 법안은 개인신분에 관한 정보는 정부나 사설기관 모두에 의해 이용되는 것을 금지하고 있다. 그러나 이 법률을 시행하는 통괄부처는 마련되지 않아 혼선을 빚고 있는 실정이다.

대만 의회는 1999년 통신보호와 감시법을 승인하여 도감청에 대한 더욱 엄격한 규정을 마련하였다. 그러나 도감청은 여전히 '국가안보'와 '사회질서'의 명분으로 광범위하게 허용된다.[82] 대만 검찰부의 발표에 따르면 1996년 한해에만 약 1만5000건의 '정치적 사찰' 성격의 도청이 행해진 것으로 보고된다.[83]

2000년 대만 법무부는 각 은행이 보유한 모든 개인의 금융정보를 재무부에 통고하라는 요청을 하였으나 재무부에 의해 거부되었다.[84]

1997년 대만정부는 모든 개인의 건강보험, 운전면허, 세금정보등이 수록된 개인별 '스마트 카드' 발급을 계획하였으나 개인신상정보의 무제한적 노출에 대한 우려로 무효화되었다.

타일랜드

1997년 발효된 태국의 프라이버시 보호법은 다소 특이하게 개인의 사진의 유포까지를 법률적으로 제한하고 있다.
국립 정보기술위원회(NITC)는 1998년 발족되어 2000년 개인정보 보호법을 발효시켰다.
1997년 공공정보법이 채택되어 정부의 개인정보 접근에 관한 규정을 마련하였다. 공공 정보법에 따르면 정보를 다루는 관리는 개인으로부터 직접 정보를 취득해야하며, 국가의 정보업무에 합당한 정보만을 수집해야 한다. 만약 당사자가 아닌 제3자로부터 그 해당 개인의 정보를 수집하였을 경우에는 반

82) ′"Taiwan's Watergate,' says Chen after wiretap found," Taipei Times, January 26, 2000.
83) "Surveillance must not be abused," China News, November 7, 1999.
84) U.S. Department of State, Taiwan Country Report on Human Rights Practices for 1998, February 26, 2002.

드시 당사자에게 그 사실을 통지해야 한다.[85]

전화도청은 이미 1934년 전신전화법에 의해 범죄행위로 규정도이었으며, 감청은 국가안보 차원에서 제한적으로 허용된다. 그러나 불법 도감청은 현재 타일랜드에서 광범위하게 이루어지는 것으로 보고된다. 1997년 정부청사에서야당 사무총장에 대한 도청과 그 녹취록이 발견되기도 하였다.[86]

터키

1992년 터키 헌법은 '프라이버시와 사생활 보호법'을 포함시켰다. 터키 헌법 20조는 '사법조사와 검찰조사의 필요성이 인정되는 경우를 제외하고 모든 국민은 사생활과 가정생활의 프라이버시 권리를 주장할 수 있다'고 규정하고 있다. 헌법 22조는 모든 국민의 개인통신의 비밀의 권리도 보장하고 있다.

2000년 터키 법무부는 개인정보 보호법을 마련에 들어갔으나 아직 구체화되고 법안채택에 이르지는 못하고 있다. 터키정부는 전자상거래의 활성화를 위하여 개인정보 취합의 용이성을 확보하여야 함과 동시에 정보화 시대에 개인정보 보호의 필요성 증대라는 상반된 가치 속에서 고민하고 있다.[87]

터키 헌법에서 개인권의 보호는 사법체계 속에 포함되어있다. 개인은 자신의 사생활 침해에 대한 소송을 제기할 수 있으나 이는 형법조항에 해당되지 않으며 형법에 개인정보 보호에 관한 법률적 장치가 마련되어있지 않아 개인정보 보호에 커다란 취약점을 안고 있다.[88]

터키는 현재 개인정보 보호법 초안을 마련하고 채택을 준비 중인데, 이 초안은 대체적으로 유럽인권선언과 독일 헤세주의 정보보호법을 기초로 하고 있다. 본래 초안에는 개인정보보호를 위한 감시단(옴부즈맨)제도를 기안하였으나 터키 보안청과 법무부의 반대로 제외되었다. 전문가들은 터키 개인정보보호법이 통과되더라도 이는 유럽의회의 기준에는 미치지 못할 것으로 예상하고 있다.

---

85) Nakorn Serirak, Thailand's Information Law, March 2000.

86) "Inside Politics Infuriated by tap rap," FT Asia Intelligence Wire, July 3, 1997.

87) Asia Times, "No privacy on the phone lines," April 16, 1997, p 8.
"Turk policeman convicted in phone tapping scandal," Reuters, December 6, 1999.

88) See Republic of Turkey, Ministry of Foreign Affairs paper, "Human Rights in Turkey: V. Turkey's Place and Role in the International Context," at <http://www.mfa.gov.tr/GRUPF/hrtur.htm>.

터키는 유럽의회의 회원으로서 개인보호에 관한 유럽선언에 서명했으나 아직 의회의 비준을 받지 못했다.

페루

페루의 1993년 헌법은 개인정보 보호와 정보 이용의 자유를 포함한 포괄적인 사생활권 보장을 명시하고 있다. 1999년 의회에 의해 제청된 정보보호법은 스페인의 정보보호법과 이탈리아의 정보프라이버시 법에 기반을 두며, 또한 1988년 오스트레일리아의 프라이버시법, EU의 정보보호 규정등 모든 내용을 담고 있다. 또한 이 법안은 정보보호 위원회의 신설도 담고 있는 등 가장 야심찬 구상으로 이루어져 있다.[89]

그러나 현실적으로페루 보안당국의 불법적 도감청은 끊임없이 빈발하고 있다. 대통령의 측근이 책임지고 있는 정보국의 도감청은 정부의 장관, 판사등에까지 광범위하게 이루어지고 있다. 또한 육군 정보당국은 이스라엘의 고도화된 도감청 장비를 이용하고 있으며, 정보국은 마약단속을 위한 미국의 CIA와 긴밀한 관계를 유지하고 있는 것으로 보고된다. 정보국은 단지 반정부세력을 단속하기 위한 목적으로 전국적인 규모로 대대적인 도감청과 사생활 침해도 불사하고 있는 실정이다.[90]

폴란드

폴란드 헌법은 프라이버시와 개인정보 보호를 규정하고 있다. 헌법 47조는 '모든 국민의 사생활과 가정생활, 그리고 명예의 보호와 사생활의 결정권' 존중을 명문화 하고 있다. 헌법 51조는 별도의 법적 규정 없이 모든 국민은 개인정보 제공 요구를 거부할 수 있으며, 공권력은 그것이 민주적 법 집행에 불가피한 경우가 아니면 개인정보 수집과 접근을 할 수 없도록 규정하고 있다.

1997년 승인된 폴란드의 개인정보 보호법은 유럽의회의 개인정보 보호 규정에 의거한다. 이 법에 따르면 개인정보의 처리는 본인의 동의하에서만 이루어지도록 규정하고 있다. 또한 모든 개인은 사설정보업체나 정부에 의해 수

89) "Former Agent Accuses Peru Spy Chief," AP, March 17, 1998.

90) "President Fujimori denies intelligence services behind phone-tapping," America Television, Lima, BBC Summary of World Broadcasts, July 19, 1997.
"Former U.N. chief charges Peru tapped his phone," Reuters, Aug 4, 1997.
The United Nations High Commissioner For Human Rights. Third periodic report of Peru: 21/03/95. CCPR/C/83/Add.1.

집, 저장된 자신의 정보를 확인할 권리가 있으며, 그러한 정보가 존재하는지, 존재한다면 누가 그 정보를 관리하고 있는지 문의할 권리가 있으며, 이러한 문의에 대하여 해당기관은 30일 내에 회신하도록 되어있다.

이 법은 폴란드 개인정보 심사국(Bureau of Inspector General for the Protection of Personal Data)에 의해 시행되며, 심사국은 정보 파일 수록과 정보에 대한 항의와 무작위적 추출방식에 의한 정보검색을 통하여 문제를 파악한다.

폴란드 정부는 범죄행위 예상자들의 '성적 취향' 과 DNA 지문, 종교와 정치성향, 건강 상태 등 민감한 정보를 경찰이 수집, 처리하도록 하려는 움직임이 있으나, 이러한 움직임은 야당에 의해 저지되었다. 그러나 전화회사의 개인교통정보와 기록 등에 대한 수집은 허용 쪽으로 가닥을 잡고 있다.[91]

폴란드에는 구체적이고 명시적인 정보 자유법(freedom of information)이 명시되어 있지 않다. 폴란드 언론인 연맹(Polish Journalists' Union)은 2001년 의회에 정보 자유법을 청원하였다.

폴란드는 아직 정보공개법을 시행하고 있지 않다.

포르투갈

포르투갈 헌법은 프라이버시와 통신비밀, 그리고 개인신상정보 보호를 광범위하게 규정하고 있다.

1997년 포르투갈 헌법 35조 수정조항은 모든 개인의 정보보호를 명문화 하여, '모든 시민은 본인이 관계된 모든 전자정보를 열람할 수 있는 권리를 가지며, 법에 따라 그 정보가 어떻게 이용되는지 통보받을 권리를 갖는다' 고 규정하고 있다. 또한 수정헌법 35조 2항은 개인정보의 범위를 규정과 그 정보들의 처리방법, 그리고 그 법적 보호장치를 명문화하고 있다.[92]

---

91) United Nations, Report of the Human Rights Committee, A/54/40, 21 October 1999.

92) Constitution of the Portuguese Republic, <http://www.parlamento.pt/leis/constituicao_ingles/IND_CRP_ING.htm>.

1998년 제정된 개인정보 보호법은 EU의 정보보호 규정을 과 포르투갈 법률 체계에 도입하여 완성되었다. 이 정보보호법은 개인정보의 수집과 사용, 그리고 유출을 통제하며, 비디오 촬영을 포함한 음성과 이미지의 수집 저장도 금지하고 있다.

이 법은 폴란드 국립 정보보호 위원회(National Data Protection Commission)에 의해 시행되며, 이 위원회는 의회에 소속된 독립적인 기구로서 정보의 수록과 통제를 담당하며, 또한 정보 시스템까지 일괄 관리한다.[93]

필리핀

1987년 필리핀 헌법 3조는 프라이버시권을 인정하였다. 3조wgkd은 '모은 국민은 자신의 서류, 가정, 개인을 어떠한 목적으로든 외부로부터의 이유없는 수색과 억류로부터 보호받을 권리'가 있음을 명시한다.

1998년 필리핀 대법원 판결은 1996년 라모스(Romos) 전 대통령에 의해 도입된 '국민 전자정보 검색 체계'를 위헌적 제도라고 판결하였다. 이 제도는 어느 누구도 전자 ID 발급을 거부할 수 없도록 하고 있다. 대법원 이 제도가 국민들의 프라이버시를 명백하게 위협할 위험성을 내포하는 것으로 판단하였다. 또한 프라이버시를 침해할 위험성이 있는 모든 법률은 엄격한 검증을 거쳐야한다고 했지만, 대법원은 또한 '프라이버시의 보호가 모든 법률을 거부할 수 있는 권리'는 아님을 명백히 하였다. [94]

조셉 에스트라다(Joseph Estrada) 전 대통령은 국민 신상정보 체계 도입에 다시 찬성하였다.

필리핀에는 일반적 개인정보 보호법이 마련되지 않았으나 개인정보는 민법상 보호 대상으로 규정되고 있다.

헝가리

---

93) "Bug Found in Portuguese State Prosecutor's Office," The Reuters European Business Report, April 27, 1994.

94) "Erap wants nat'l ID system (Only criminals disagree with it, says the President)," Businessworld, August 12, 1998.

헝가리 헌법 59조는 헝가리 모든 국민이 '명예를 지키고, 가정에서의 프라이버시와 통신, 그리고 개인신상정보를 보호받을 권리'가 있음을 명시한다. 1991년 헝가리 대법원은 여러 가지 용도로 전용될 수 있는 개인별 번호를 만드는 것은 헌법의 프라이버시 보호권을 침해하는 것이라고 판시하였다.[95]

1992년의 개인정보 보호법은 공적영역과 사적영역 모두에 있어서 개인신상정보를 수집, 이용하는 행위느 불법으로 규정하였는데 이는 정보자유법과 개인정보 보호법의 통합형태이며, 그 근본원칙은 정보의 자결권(self-determination)이다. 헝가리의 강화된 프라이버시 보호법은 유럽의회의 인권선언 규정에 비해 손색이 없다.[96]

개인에 대한 경찰의 사찰은 5년 이상의 징역형이 예상되는 범죄행위일 경우로 제한되며 국가 보안청에 의한 감시는 법무부의 특별 허가를 얻은 경우에 한하며, 그 기간도 90일 이내로 제한된다. 그러나 여전히 정적, 환경단체, 그리고 소수인종에 대한 비밀첩보 행위가 빈발하는 것으로 보고된다.[97]

헝가리 정부의 정보공개법은 아직 마련되지 않고 있다.

분석

이상 41개국을 대상으로 1)빈도분석(frequency analysis)과 내용분석(contents analysis) 2)구조적 분류분석(structural-category analysis)을 통하여 밝혀진 사실은 정보의 자유와 사생활 보호의 조화, 그리고 대응책은 대체적으로 개별국가가 처한 역사문화적 환경과 사회발전 단계, 그리고 정치경제 체제에 따라 선택됨을 알 수 있다.

이상 살펴본 세계적인 추세는 기본법과 헌법에 인권보호의 가장 중요한 가치로서 '사생활권' 보장을 많은 주요국가들이 명시적으로, 만약 명시적이

95) Constitutional Court Decision No. 15-AB of 13 April 1991.
96) 참조; See Hungarian Civil Liberties Union, Data Protection and Freedom of Information, 1997.

97) Hungary: government, far-right clash with opposition over surveillance case, BBC Monitoring Europe - Political, March 2, 2000.

아닐 경우는 '해석'에 의하여 묵시적으로 규정하고 있음을 알 수 있다. 이러한 추세는 '자유민주주의'의 전세계적인 확산과 함께 '개인 자유'의 가치가 더욱 부각되면서 모든 국가들이 '개인 자유'를 더욱 적극적으로 보호하고 있는 것으로 파악된다. 따라서 현재 사생활권과 개인정보 보호를 법제화 하지 않은 아시아, 아프리카의 대다수 국가들도 이러한 흐름에 조만간 동참할 것으로 보이며, 현재 그러한 움직임을 보이고 있다.

또한 1980년대 이후 정보화시대가 진행되고 정보통신 기술의 발달, 인터넷의 발달에 따라 '개인정보'의 보호문제가 프라이버시 보호의 중대한 과제로 떠올라, 세계각국이 '정보보호법'을 적극적으로 도입하고 있음을 보여준다. 국가역할의 축소에 따라 정보보호법 역시 과거와는 달리 단순히 개인신상에 대한 국가기관의 정보수집과 저장만이 아니라 사설정보업에 의한 개인신상정보 역시 엄격하게 규제하고 있음을 보여준다. 따라서 정보보호법의 채택과 그 범위는 개별 사회의 '자유'의 정도와 사회의 '정보화' 발전 수준에 따라 차등화 되고 있는 것으로 보여지는 바, 선진 정보화 사회일수록 '개인정보' 보호 요구가 확산되고 엄격한 보호장치가 마련되는 것을 알 수 있다.

또한 세계화시대의 전세계적인 민주주의의 확산에 따라 국가기관의 정보수집과 저장의 투명성, 그리고 정보민주화에 대한 요구에 부응 '정보공개법'이 폭넓게 시행되고, 공개정보의 범위도 각국에서 점차 확대 실시되고 있음을 알 수 있다.
우리사회는 자타가 공인하는 '정보화' 첨단국가이다. 정보화 산업은 현재 한국의 국가경쟁력을 견인하고 있으며, 미래경쟁력 역시 상당부분 정보화 산업이 담당하게 될 것이다.

정보화 사회는 필연적으로 개인정보와 사생활권의 침해를 야기하나, 상기 해외사례에서 적시되듯, 아시아 문화권은 사생활권과 개인정보의 보호에 다소 유연한 태도를 보이며, 현재 우리사회도 이에서 크게 벗어나지 못하고 있다. 따라서 한국사회는 정보화 시대의 개인정보 보호와 사생활권의 보호를 강화하기 위하여 OECD기준(OECD Guidline)과 같은 '국제체제(international regime)'에의 동참도 고려할 필요가 있다.[98]

---

98) 정보기술 환경이 변화함에 따라 가장 먼저 유럽국가들이 주도적으로 개인정보의 보호에 관한 구체조치를 입안하고 나섰다. 이미 70년대 초에 유럽국가들은 사생활보호에 관한 논의를 활발하게 진척시켜 73년에는 민간

위 사례연구에서 보듯 많은 국가들이 1)OECD 규정에 따름으로써 국내의 사생활권 보호에 획기적 전기를 마련하였으며, 2)세계화 시대 국가간 '정보의 유통'에서 실질적 효과를 보고 있다.

그러나 위 사례에서 보듯, 개인 정보와 사생활 보호에 관한 법적 제도적 장치가 완비된 국가에서도 사생활권 침해에 대한 우려는 지속되고 있다. 많은 국가에서 법적 보호장치는 급속하게 발달하는 정보기술을 따라가지 못하여 개인정보와 사생활 보호에 심각한 괴리현상을 보이고 있다. 또한 다른 국가들에서는 국가기관과 정보기관에 광범위한 법적책임의 면제가 이루어지고 있다.

세계 각국에서 통신감시가 광범위하게 이루어지고 있으며 몇몇 가장 민주적인 국가도 예외는 아니다. 미국 국무성 인권 백서는 약 90개국에서 정치적 반대세력에 대한 통신감청이 이루어지고 있다고 보고된다. 1996년 프랑스 정부는 민간부문에서 연간 약 10만건의 도청이 발견되었다고 발표하였다. 아일랜드에서는 영국이 북아일랜드에서 영국과 아일랜드 사이의 모든 통신을 감시한 것이 드러나 거센 항의가 일어나기도 하였다.

사생활권이 강력히 보호되는 국가의 경찰조차도 정치적 목적에 따라 기소되거나 혐의가 없는 일반시민에 대한 정보까지 광범위하게 수집하고 있는 실정이다. 최근 사생활 보호의 강력한 전통이 있는 스웨덴, 덴마크, 노르웨이

부문, 74년에는 공공부문의 전자정보 은행에 대한 개인의 사생활보호에 관한 결의("resolution")를 당시의 EC 이사회(Council of Europe)에서 채택하였고 이 내용이 1980년 OECD 가이드라인에 반영되었다. 1990년대 인터넷 시대에 들어 개인정보 보호의 필요성이 더 강해지자 유럽연합은 개인정보 보호에 관한 새로운 지침을 제정하여 3년 후인 1998년 10월부터 회원국의 이행입법 조치를 통해 발효되도록 하였다

.

정보시스템 발전에 따른 개인정보 유출에 대한 우려를 반영하여 1980년 OECD에서는 프라이버시 보호에 관한 가이드라인을 채택하였다. 이 가이드라인은 특정한 기술을 염두에 두지 않고 작성된 것이기 때문에 급속히 변화하는 환경에서도 적용될 수 있는 큰 원칙들을 제시하고 있다. 또한 이 가이드라인은 공공부문뿐만 아니라 민간부문에도 적용될 것을 염두에 두고 작성되었다.

1980년의 사생활보호에 관한 OECD 가이드라인의 주요한 원칙은 데이터를 수집할 때에 그 사용목적을 명기하고 이후 목적을 바꿀 때에는 매번 이를 명기할 것, 정보주체의 인지나 동의가 있을 것, 명기된 사용목적 이외에는 정보주체의 동의가 있거나 법원의 요구 없이 전용하지 말 것, 정보주체의 권리보장 등으로 이루어져 있다. 그 외에도 이 가이드라인은 개인정보가 합법적으로 국경을 넘어 유통되는 경우 이를 제한하지 말아야 함을 선언하고 있다.

같은 북유럽 국가들에서 경찰과 정보기관에 의한 정보수집에 대한 감찰이 이루어졌으며, 스위스에서는 경찰의 불법행위가 야기한 스캔들로 인하여 정보보호법이 제정되기도 하였다. 동유럽 국가들에서는 과거 비밀경찰에 의해 수집된 정보의 공개문제가 여전히 논란거리로 남아있다.

미국에서는 소비자 신용정보 보호법에도 불구하고 많은 기업들이 이 정보를 마케팅에 광범위하게 이용하고 있다. 또한 많은 국가에서는 소비자 개인 신용정보에 관한 부적절한 보안으로 인하여 수많은 소비자 개인정보가 유출되고 있는 실정이다.

시사점

그러나 위 사례연구를 통한 중요한 사실은 명목상의 사생활권 보호와 실질적인 보호에는 상당한 괴리가 있음을 알 수 있다. 사례연구에서 보듯, 비록 많은 주요국가들이 사생활권 보호를 명문화하고 있지만 '자유'의 가치를 전통적으로 중시하는 서구국가를 제외하고는 실질적인 보호가 제대로 이루어지지 않고 있음을 알 수 있다. 특히 최근 정치적 민주화를 이루었거나, 국가의 역사가 일천한 경우, 그리고 '자유'보다는 '사회통합'의 가치에 무게를 두는 '아시아적 가치'의 국가에서는 여전히 '사생활권 보장'과 '사회 합목적성' 사이의 갈등이 있음을 알 수 있다.

'문화권'에 따른 분석은 '개인의 자유' 인식이 발달한 서구사회일수록 개인정보에 대한 보호가 엄격하게 법적 보장을 받는 반면, '개인' 보다는 '사회'를 강조하는 아시아 국가들은 정보화 수준의 급속한 발달에도 불구하고 '개인정보' 보호에 대한 엄격성이 다소 떨어지는 것으로 나타난다.

상기 해외사례 연구는 우리나라의 사설정보지에 대한 제도적 대처방안 마련도 이러한 전세계적 흐름의 방향성에 맞추어 기본틀이 구성되어야 할 것으로 보이며, 한국사회의 일천한 '민주화'의 역사, 그리고 '사회통합적 가치'의 전통적 중시 현상등이 적절히 조화되어야 할 것이다..

V-2. 5개국 사례연구(case-studies)

V-2-1. 미국

민주주의의 전제로서 요구되는 사상의 자유시장을 형성하기 위하여는 정보화사회에 있어서의 국민 각자의 알 권리, 특히 정보에의 자유로운 접근의 권리가 보장되어야 하는 한편 공개로부터 보호되어야 할 영역 특히 개인 사생활의 보호가 지켜져야 한다.

이러한 논의는 20세기에 들어와서야 조직범죄에 대비하여 1928년 Olmsted 판결[99]에서 처음으로 그 법적성격을 판단한 뒤 1934년 연방통신법에서 전화통화의 도청을 금지하고, 1968년 범죄단속 및 가두안전종합법(Omnibus Crime Control and Safe Streets Act Title III)이 제정되었으며, 1986년에는 과학기술의 발달을 대비하기 위하여 보완된 전자통신프라이버시법(Electronic Communication Privacy Act : ECPA)를 제정하였으며, 1994년에는 정부의 권한을 강화시킨 통신보조집행법(Communication Assistance for Law Enforcement Act : CALEA)[100]을 제정하였다. 이러한 미국의 제 규정은 국가기관의 효과적인 법집행이라는 공공의 이익과 프라이버시라는 개인의 이익이 절충된 결과라 할 수 있다.[101] 그리고 최근 9·11테러 이후 공공의 이익을 한층 더 강조하고 있다.

대부분의 나라들이 민간 부문에 의한 개인의 프라이버시 침해를 규제할 법조항을 따로 두지 않고 있는데 반해 미국은 캐나다와 마찬가지로 민간 부문의 침해 사례를 규제할 법조항을 따로 명시하고 있다. 또한 미국의 프라이버시권 개념은 다른 나라에 비해 그 개념의 범위가 넓고 세세한 부분에서도 프라이버시권의 개념을 충실히 적용한다.

현재, 유럽이 입법조치를 통해 프라이버시 보호문제를 다루는데 비해 미국에서는 원칙적으로 자율규제(self-regulation)를 통해 이 문제를 다루려고 하고 있다. 미국의 경우도 FCC는 최근 전화회사들이 가입자들의 정보를 이용하여 다른 상품을 마케팅하기 위해서는 가입자의 동의를 얻어야 한다는 프라이버시 규정을 채택한 바 있다.

---

99) Olmsted v. United States, 277 U.S. 438,48, S.Ct. 564,72 L.Ed. 944 (1928).
100) 47 U.S.C. §1001-1010(1994&Supp.IV 1998).
101) 심희기, "과학적 수사방법과 그 한계-미국법과 한국법의 비교-," 1994, 형사정책연구원 연구보고서, 27면 참조.

자율규제 쪽을 선호하는 나라에서는 프라이버시 보호를 위한 기술적 해결책 등에 대한 연구와 상품화가 진행되고 있다. 프라이버시 보호를 위한 기술적 해결책으로는 "Anonymiser" 등과 같은 것을 들 수 있는데 그 원리는 정보를 수집하려는 정보관리자와 정보주체 사이에 신뢰할 수 있는 제3자를 개입시키는 것이다. 이때 이 제3자(Trusted Third Party)는 정보주체의 실제정보를 알고 있으나 정보를 수집하려는 관리자는 정보주체의 정보를 직접 얻는 것이 아니라 제3자가 공급하는 익명의 정보를 얻게 됨으로써 정보주체를 보호하는 역할을 하게 된다. 물론, 이 경우 신뢰할 수 있는 제3자의 책임문제가 새로이 대두된다.

1965년 미국연방대법원 판례를 통해 수정헌법 제 14조의 보호를 받을 권리로 인정되기 전까지 미국 역시 고전적 의미의 프라이버시권 개념만을 갖고 있었다. 그러나 지금은 공적 기관에 의한 침해뿐만 아니라 민간 부문에 의한 개인정보침해를 규제하는 규정을 두고 있다.

다음은 1970년대 미국 보건교육복지성의 보고서에 제시된 개인 정보 보호에 관한 5개의 기본 원칙이다.

ⅰ) 기록의 존재 자체를 비밀로 해서는 안된다.

ii) 어떤 개인정보가 어디에 쓰여지는지 본인이 알 방법이 있어야 한다.

iii) 본인의 승낙 없이 다른 곳에 개인 정보가 이용되는 것을 방지할 방법이 있어야 한다.

iv) 틀린 정보는 정정할 방법이 있어야 한다.

ⅴ) 관리자는 데이터의 신뢰성을 확보해야 하고 오용을 방지할 예방조치를 강구해야 한다.

이러한 기본 원칙은 미국의 법 적용에서 풍부한 판례를 통해 어느 정도 지켜지고 있다. 우리나라의 경우 이념적으로는 이런 원칙들이 의미를 가질지 모르지만, 관련 법조항에 뚜렷이 명시된 문항이 없고 실제 상황에서는 곧 잘 무시된다.

미국은 조사대상 해외사례 중 가장 '개인가치'의 존중과 자유의 폭이 넓은 사회이다. 따라서 정보의 생산과 유통의 자유가 폭넓게 허용되고 있으며 정보의 생산과 유통에 있어서도 '시장의 자유'와 '개인적 표현의 자유'는 넓은 폭으로 허용되어 사설정보(private intelligence)가 가장 활성화된 국가로 판단된다.

미국의 공영역에서의 정보생산은 사실상 상당부분 사영역과의 경계가 허물어진 상태(privatization)에서 이루어지고 있어, 정보생산과 유통의 투명성이 비교적 보장되는 사회이기도 하다. 또한 민간영역과 협력체제 속에서 경제적이고 효과적인 정보의 방대한 생산과, 정비된 '정보공개법'을 통한 생산된 정보의 '공공재'로서 사회에의 환원이 상당부분 이루어져 민간이 접근가능한 1차정보 풀(raw information pool)의 폭과 깊이가 깊고 넓게 형성되어 있다.

이러한 여건 하에서 양성화된 정보 브로커(information broker)와 독립정보연구소(independent information researcher)들이 비교적 불법, 탈법과 적법의 경계를 넘나들 위험성 없이 사설정보업 차원에서 정보고객들에 대한 '맞춤형' 정보업을 영위하고 있다.

이러한 미국적 제도운영은 사설정보업에 의한 사회적 혼란과 개인적 피해의 양산을 비교적 순조롭게 통제하는 시스템으로 자리잡고 있는 것으로 평가된다.

아래에서는 미국의 가장 대표적인 사설정보지인 '드러지 리포트(Drudge Report)'의 사례와 대표적 거대사설정보업체인 ChoicePoint사의 사례를 통하여 미국의 사설정보 현황과 그 시사점을 고찰해 본다.

사설정보지: 드러지 리포트(Drudge Report)

대표적 사설정보기관 중 하나인 Nelson이 발행하는 사설정보지 넬슨 리포트

(Nelson Report)의 경우 그 정보수집의 네트웍은 국가기관인 CIA와 견주어도 크게 차이가 없다는 정도의 평가를 받기도 하고, 미국의 대외정책 자체에까지 일정정도 영향을 주고 있다고 보고된다.[102)]

그러나 이러한 대형 사설정보기관과 그들이 발행하는 정보지(report, newsletter)에 의해 유통되고 소비되는 정보들 중 상당부분은 국가적 목표와 사회의 합목적성과 괴리현상을 보이고 있으나 정보통신의 자유라는 대전제와 사회적 합의, 그리고 미국적 전통 위에서 통제되기 어려운 것이 현실이다. 실제로 Nelson Report의 경우 미국의 대 한반도 정책과 이라크 전쟁과 같은 주요한 대외정책의 방향의 수정과 혼란까지 야기시키는 사례도 보고된다.

미국의 가장 대표적인 사설정보지는 국제정치와 경제문제를 주로 취급하는 넬슨 리포트(Nelson Report)와 미국 국내정치를 다루는 드러지 리포트(Drudge Report)를 꼽을 수 있다.
넬슨 리포트는 크리스 넬슨(Chris Nelson)이 편집을 담당하는 국제정치경제 정보 전문 웹사이트로 넬슨 리포트는 2005년 11월 미군이 이라크에서 포로들에 대한 고문을 자행하고 있다는 미확인 정보기사를 게재하여 물의를 빚기도 하였다.

드러지 리포트는 미국 헐리우드에 기반을 두고 인터넷을 통하여 e-메일을 통하여 리포트를 회원들에게 발송한다. 드러지는 한때 CBS방송국의 선물점을 운영할 당시 친분을 쌓았던 인사들을 통하여 정관계, 재계의 가십(gossip)을 수집, 그것이 신문방송에 보도되기 전에 폭로함으로써 관심을 끌게 되었으며, 1998년 공식적으로 e-메일리포트를 발행하게 되었다.

드러지 리포트가 미국사회 전체의 관심을 이끌어 낸 것은 1996년 미국 대통령 선거 당시 잭 켐프가 공화당 밥 도울의 러닝메이트로 결정되었다는 소식을 주류언론의 발표이전에 보도하면서부터이다. 또한 결정적으로 1998년 클린턴 대통령과 모니카 르윈스키의 추문을 보도하면서 미국사회를 뒤흔들었다. 그러나 르윈스키 추문은 이미 주류언론들에 의해서도 이미 전모가 어느

---

102) Broad, William J. Study 랴운 pu7blic science is pillar of industry (New York Times, Tuesday, May, 1997)

정도 파악되어있던 상태였으나 주류언론들은 그 추문 보도의 사회적 파장과 그 '필요성'의 고민과, 정부측의 비보도 요청에 협조하는 '신사협정'으로 보도를 자제하였을 뿐이었다.

드러지 리포트의 경우, 미국정부에 의해 그 존재조차 파악되지 않았던 상태에서 비보도 협조요청 대상에서도 제외되었고, 주류언론과는 달리 '사회적 합목적성'에 대한 고려도 기대하기 어려운 사설정보지였을 뿐이었기에 가능한 보도였다.

드러지 리포트는 통상 리포트의 대부분을 다른 언론매체들의 보도내용을 편집하여 구성하면서 때로 편집인 드러지 본인의 칼럼을 게재하는데 여기에서 드러지 특유의 폭로성 기사를 내보낸다.

드러지 리포트는 일일 방문객 수가 800만-1,000만 명에 달하며, 드러지는 이 리포트의 발행으로 상당한 경제적 이윤창출을 하고 있는 것으로 알려지고 있다. 드러지 리포트는 년간 약 100만불의 수익을 창출하고 있는 것으로 보고된다.[103] 그 제작비용이 거의 소요되지 않는 점을 감안한다면 대단한 수익을 창출하고 있는 모델로 관심을 끌고, 이러한 성공이 이와 유사한 수많은 사설정보지의 출현을 이끌어내기도 했다.

드러지 리포트와 같은 사설정보지에 대한 미국사회의 비판점은 리포트의 거의 모든 정치정보 기사들이 드러지 리포트에 소속된 기자들이 작성하지 않고 다른 기자들에 의해 작성되기 때문에 그 신뢰도가 떨어지며, 또한 그 정보에 대한 책임소재가 불분명하다는 데에 있다. 1998년 폴 프리드만(Paul Friedman)판사는 드러지 리포트에 관한 '무고 소송'에 대한 판결에서 '드러지 리포트는 보고서, 저널, 혹은 정보기관으로 볼 수 없다'고 판시하여 그 귀책사유를 인정하지 않았다. 이 판결을 드러지 리포트가 사실관계 확인에 있어서는 면책됨을 의미하였으나, 그 신뢰성에 대해서는 '불가' 판정을 받은 것과 다름없다.[104]

---

103) Benson, Michael, State Web sites offer firms competition (*Wall Street Journal*, May 14, 2004)

104) Brownin, Edgar, Unreliable spying eyes in American political drama, (*New York Times*, June 18, 2003)

이점은 드러지 리포트의 발행인 매튜 드러지(Mattew Drudge)도 일정부분 인정하여 리포트의 정확성을 '80%' 라고 한정하고 있다. 가장 대표적인 사례는 1997년 8월 드러지 리포트가 신임 백악관 보좌관 내정자 시드니 블루멘탈(Sydney Blumenthal)에 관하여 그가 그의 아내를 구타하였다고 보도하고, 그 다음날 이를 드러지는 이를 오보라고 정정하였으나블루멘탈로부터 3,000만불에 달하는 명예훼손 고소를 당한 사건이었다. 비록 그 보도의 '고의성' 이 인정되지 않아 양자간에 합의로 소송은 일단락 되었으나, 사설정보지의 한계와 그 사회적 파장을 보여주는 대표적 사례로 기록된다.

또한 2004년 대통령 선거 당시 공화당 케리후보가 자신의 러닝메이트로 존 에드워즈를 지명하기 일주일 전 드러지 리포트는 케리후보가 힐러리 클린턴을 러닝메이트로 지명할 것이라고 백악관 내부정보자를 인용하여 보도하였다.[105] 그리고 케리후보가 에드워즈 상원의원을 지명하자 아무런 설명없이 이미 보도되었던 '힐러리 부통령 지명' 에 관한 모든 기사를 내렸는데, 이는 드러지 리포트가 상용하는 오보 처리 방식이기도 하다. 드러지 리포트는 웹사이트 매체이기 때문에 이러한 부정확성을 처리하는 방식이 가능하기도 하다.

그러나 이러한 사설정보지의 확인되지 않은 소문과 정보원(정보원)에 의한 기사로 포장된 정보의 유통은 많은 경우 미국 정치계, 사회에 적지않은 혼란을 야기시키고, 거론된 당사자들의 사생활과 활동에 타격을 입히기도 하지만 그 책임소재가 불명확한 채로 남아있다.

공영역(public sector)과 사영역(private sector)의 통합:

사설정보업 ChoicePoint의 사례

미국은 또한 통상적인 영역분류(sector)에 있어서 영역별 통합이 가장 두드러진 사회이기도 하다. 다시 말하면 제1섹터(정치, 정부)와 제2섹터(경제, 민간), 그리고 제3섹터(시민사회)가 명확한 분류가 어려울 정도로 유기적으로 작동하고 있다.

---

105) Browning Edgar, *Ibid*

이러한 현상은 이미 1960대 군산복합체(military-industrial complex)의 모습이 보여주듯 미국사회의 대표적 현상 중 하나라 하겠다. 정보의 생산과 유통에 있어서도 이러한 현상은 두드러져 미국의 또 다른 대표적 거대 사설정보회사인 ChoicePoint의 경우 그 주고객은 민간뿐만 아니라 오히려 정부기관들 조차 ChoicePoint를 통하여 수집된 민간부문의 정보를 이용하고 있다.

미국의 사설정보 시장의 특징은 거대기업화하고 공적기관과 유착관계를 형성하고 있는 경우가 많아 사설정보기관들이 생산하는 정보의 신뢰성이 상당수준에 달하고 있으며, 그에 따라 정보의 가격도 일반인들이 접근하기 어려울 정도로 고가로 책정되는 경우가 많은 것으로 집계된다.

미국에서 가장 활발하게 활동하는 사설정보업 형태는 공개된 공공정보를 취합하여 특정목적의 고객들에게 판매하는 정보 브로커(information broker)의 활동이다. 이러한 사설정보의 사회적 배경은 미국의 정보공개법이 활성화되어 실질적으로 국가비밀로 분류되어 비공개되는 정보(classified information)가 상당부분 제한적으로 운영되기 때문에 대부분의 정보는 일반에게 대량으로 공개되기 때문이다.

이러한 현상을 반영하여 미국의 공개된 정보를 처리하는 전자정보출판(electronic publishing industry)는 연간 약 130억불에 달할 정도로 방대한 시장을 형성하고 있다. 따라서 특정목적의 정보수집을 원하는 일반개인이나 기관, 조직조차도 자력으로 이러한 방대한 정보를 취합하기 어려워 정보 브로커(개인과 회사)들이 그 수집과 가공을 대행해 주고 있다. 미국 CIA 요원들의 통상적인 업무 중 상당부분은 이렇듯 공개된 과학, 경제, 군사, 그리고 정치정보들을 인터넷 접속을 통하여 파악하는 업무라고 하며, 실제적으로 CIA 요원들조차 사설정보력에 의존하고 있다.[106)]

미국의 사설정보기관의 또다른 특징 역시 이러한 방대한 공개된 정보(unclassified public information)의 특성에 의하여, 정부기관들 조차 공개

106) Wesley Cohen, Richard Nelson, and John Walsh. Approachability conditions and why firms patent and why they do not in the American manufacturing sector(*Technical Report,* National Bureau of Economic Research, 2001)

된 정보의 수집과 가공을 사설정보기관에 위탁한다. 예를 들면 미국의 재무성은 BDM Federal Inc.라는 특정 정보 브로커(information broker)의 성격을 지닌 대규모 사설정보회사에 재무성의 업무추진과 기획을 위해 공개된 정보의 수집과 분석을 의뢰하고 있다.

이미 다양한 사설정보기관들이 워싱턴에 본부를 두고 미국과 외국의 정부기구를 고객으로 활발한 활동을 전개하고 있다.

ChoicePoint는 미국시민 거의 모두의 개인신상정보를 파악하고 있는 종합정보회사이다. 그들이 파악하고 있는 시민들의 신상정보는 각 개인의 주택과 자동차, 범죄기록을 포함한 거의 모든 정보에 달하며, 이는 미국정부의 정보의 양보다 많고 그 깊이가 심도있는 것으로 보고된다.

ChoicePoint는 정부기관과 민간부문을 합쳐 약 5만개의 고객을 거느리고, 그 주식 시가총액이 41억불에 달하는 거대정보기업이다.[107]

이러한 거대정보기업의 성장배경에는 미국정보업무의 민간화정책(privatization policy)이 작용하고 있다. ChoicePoint를 비롯한 다른 사설정보업체들은 점차 미국의 국가방위와 경찰업무에까지 깊숙이 간여하게 되었는데, 그 주된 이유는 정부관리라면 사생활과 정보법의 저촉 때문에 실행할 수 없는 정보수집과 그 사용을 자유로이 행할 수 있기 때문이었다.

ChoicePoint는 이에 만족하지 않고 2001년 가을에는 미 법무성과의 계약을 갱신하고 그 용역계약 범위도 종전보다 더욱 확장했다. 이후로 ChoicePoint와 그의 경쟁사인 LexisNexis는 CIA에게 새로운 문서정보에 따른 공공정보의 온라인 제공 계약을 체결하였다

이에 대하여 시민단체들과 법률가들은 현행법은 사기업과 정부기관이 범죄자나 무고한 시민을 감시하는 막강한 권한을 남용할 가능성을 원천적으로 봉쇄하지 못하는 상태에서 이러한 형태의 협력은 위험하다고 주장하고 있다.

미국의 전자 개인정보 센터의 크리스 후프네이글(Chris Hufnagel)은

---

107) Benson, Michael, *ibid*

ChoicePoint가 시민들을 분류하는 사회가 되었다고 개탄한다.

사설정보업계는 전통적으로 정부의 규제에 대하여 그들의 자율과 자정능력을 강조하였다.

지난 10년간 미국의 사설정보업은 컴퓨터 기능의 개선과 전자정보통신 기술의 발달로 괄목할 만한 성장을 이룩하였다.[108]

이러한 과정을 통하여 그들 사설정보산업체들은 시민들의 일상생활의 수많은 결정에 대하여 점차 강력한 영향력을 행사하게 되는 것이다.

ChoicePoint 이외에 거대 사설정보업체인 LexisNexis와 Seisint Inc. 역시 정부에 정보를 제공하는 용역사업을 수행하고 있다. LexisNexis의 경우 미국국토방위청의 대 테러 시스템 용역을 확보하기 위하여 Seisint에 7억7천500만불을 지불할 정도의 거대기업으로 성장하고 있다.[109]

또 다른 대규모 정보 브로커(information broke)기업인 FIND/SVP의 경우 100여명의 정보수집, 분석 전문가를 고용하고 3000개의 온라인 출판물, 12000개의 주제별 파일, 그리고 전세계적으로 17개의 정보전문기업들과 연계하여 정부주문에 맞춘 정보수집과 분석을 대행해주고 있다.

2001년 CIA는 i2 Inc.라는 사설정보업체의 한 소프트웨어 프로그램을 구입하는 데 200만불을 지불하였는데, 그 프로그램은 이라크 사담 후세인의 행방추적을 위한 것이었다. i2Inc.의 대표 존 레이스(John Reis)는 미국 사법당국이 범인추적 방식에서 종전의 범행후 체포에 주력하던 방식에서 범행전에 예상가능한 범죄를 미리 포착하고 미연에 방지하는 방식으로 전환하면서 이 회사의 예상범죄 추적 프로그램을 구입하고 있다고 밝히고 있다.[110]

---

108) Randalll Davis, Mitchell Kapr, and Pamela Samuelson. A manifesto concerning the legal protection of computer program (*Columbia Law Review*, 94, 1998)

109) Joseph Kattan and Carl Shapiro, Privacy, self-regulation and antitrust (*Technical Report*, UC Berkeley, 2002)

110) Joseph Kattan and Carl Shapiro, *ibid*

이는 상당한 정도의 미국시민 개개인의 신상정보를 기반으로 이루어질 수밖에 없기 때문에 사설정보수집기관을 통하여 미국시민 개인신상정보가 대량으로 방대하게 이미 수집되었음을 의미하기도 한다.

이들의 주된 업무는 방대한 양의 공개된 정보를 실제 목적을 위해 사용가능하도록 간략하게 정리해 주는 것이다. 경찰과, 변호사, 사설탐정, 기자 그리고 많은 이러한 상업정보업체(commercial information services)의 주 고객이 되고 있다. 그러나 이들 상업정보업체들은 국가안정보장회의에 의해 통제되는 은밀한 최첨단 기술의 영역에서는 아직도 배제되고 있다.[111)]

정부는 아직도 최첨단의 도감청 기술을 독점하고 있지만 정부관리들은 공공 기록과 신원확인을 위해 상업정보업체에 용역을 의뢰하고 있다.

미국에서 가장 대표적인 상업정보업체인 ChoicePoint는 사업영역의 확장을 위하여 지난 2003년 국토방위 프로그램 제작을 위하여 여러명의 전직 고위관리들을 고용하기도 하였다.

이러한 협력관계를 긍정적으로 평가하는 관리들도 있으나 FBI 부국장 Pasquale D;Amuro와 FBI 뉴욕 지부장은 ChoicePoint와 같은 업체에 대해서 충분하고 적절한 감시 통제가 필수적임을 강조하고 있다. 그들은 "정부기관의 민간정보 수집은 엄격한 통제가 이루어지고 있지만 사설정보업체에 대해서는 그러한 통제가 전혀 이루어지지 못하고 있으며, 이는 미국시민들에게 잠재적인 위협요소가 될 것"이라고 경고한다.[112)]

미국 사례가 보여주는 특징은 시장의 논리와 개인적 자유가치의 실현이라는 대전제 위에서 사설정보의 영역이 극도로 확대되고 있으나, 이는 위의 사례들이 보여주듯 오히려 사회의 합목적성을 저해하는 요인으로 작용하기도 하고, 경우에 따라서는 개인적 권리인 사생활권을 침해하기도 하는 이율배반적 양상을 보이기도 한다.

---

111) Joseph Kattan and Carl Shapiro, Privacy, self-regulation and antitrust.
112) Joseph and Shapiro, 2002.

그러나 우리사회에서 현재 제기되는 것과 같은 사설정보에 대한 커다란 문제제기가 되지 않는 이유는 우선 미국의 자유주의적 전통에서 비롯되는 측면이 강하고, 한편으로는 미국의 다양한 시스템이 소위 '견제와 균형(Checks and Balance)'의 원칙 위에서 형성되어(삼권분립, 양원제, 연방정부 형태 등), 권한과 권력이 집중되지 않고 비교적 분산되어 정보의 독점과 이에 따른 왜곡의 심화 현상이 일어나지 않기 때문인 것으로 파악된다.

우리사회의 미국식 모델의 적합성 여부는 이러한 사회구조적, 그리고 역사문화적 관점에서 신중하게 연구되고 고려되어야 한다.

V-2-2, 영국

영국은 미국보다 더욱 급속도로 제1섹터와 제2섹터간의 융합과 영역붕괴가 발생하고 있는 사회이며, 따라서 사설정보회사와 그 활동영역이 확장되는 사회이다. 영국의 장기적인 정부조직 혁신안은 장기적으로 노동부, 교육부의 임무를 민간에 이양하고, 심지어는 경찰 업무의 상당부분도 민간 용역에 의존하고, '시민경찰' 제도의 도입까지 고려하며, 국방의 역할 일부분의 민간이양도 고려하고 있다.

상기 '세계 추세(global trend)'에서 지적된 바와 같이 전세계적으로 개인정보 보호가 약화되는 상황에서 영국은 서구 선진국가 가운데에서도 가장 개인 사생활권 보호에 소극적이고 개인정보에 대한 국가차원의 감시가 폭넓게 허용되는 국가라는 특징을 갖는다.

영국에서는 1985년 제정된 통신도청법(The Interception of Communication Act)을, 독일에서는 기본법 제10조와 형소법 그리고 편지 우편 및 통신비밀의 제한에 관한 법률(Gesetz zur Beschr□nkung des Brief'-, Post-, und Fernmeldegeheimnisses)을, 프랑스 등의 유럽국가에서는 효과적인 법집행이라는 공공적 법익이 프라이버시라는 사적인 이익보다 더 중시되어온 경향이 있다.[113]

---

113) Human Rights Bill, CM 3782, October 1997.
<http://www.official-documents.co.uk/document/hoffice/rights/rights.htm>.

이러한 특징은 ‘개인적 자유’와 ‘사생활권 보호’에 민감한 미국에 비하여 유럽의 역사문화적 특성 중 하나인 ‘평등지향성’과 ‘사회통합’의 가치의 중시가 정보기술의 발달로 인한 사회통합의 저해로 나타났을 때, 그 접점으로서 사생활권의 일정부분의 양도를 선택한 것으로 보인다. 또한 이러한 역사문화적 특성에 기반을 두고 있어 사생활권의 일정부분의 제약은 일반시민으로부터도 커다란 저항 없이 사회적 합의로서 받아들여지는 특성을 보이는 바, 이러한 측면은 싱가포르의 경우와 크게 다르지 않은 현상으로 파악된다.

영국은 이러한 추세에 맞추어 세계에서 가장 많은 사설정보(private intelligence), 사설경호(private security), 사설탐정(private investigator)들의 활동이 활발한 사회로 보고되고 있으며, 사설정보의 경우 역시 상당한 정도의 자유가 허용되어 허가제나 등록제가 아닌 신고제로서 비교적 자유롭다.[114]

2004년 6월 데이비드 블런킷(David Blunkett) 내무장관은 국가정보법을 개정하여 국가의 약 1,000개 기관이 개인의 e-mail과 전화통화 내역을 조회할 수 있는 권한을 허용하는 강도 높은 법안을 제출, 시민사회의 거센 항의에 직면하여 3주후에 법안제출을 철회하기도 하였다. “프라이버시 인터내셔널(Privacy International) ‘의 사이먼 데이비스(Simon Davies) 국장 블런킷 내무장관은 그러나 국가의 정보통제에 대한 그의 의지를 굽히지 않고 있으며, 여전히 영국사회에서 팽팽한 찬반논란을 불러일으키고 있는 실정이다.[115]

영국에서의 사생활권 보호의 훼손은 최근의 새로운 현상이 아니라 이미 90년대 말부터 지속되어왔다. ‘범죄와 공중질서 법’이 이미 1999년 통과되어 집회결사의 자유, 사생활권, 거주이전의 자유, 묵비권 행사의 자유와 표현의 자유에 상당부분 제약을 가했으며, 정부 기관의 개인 감시와 불법 ‘탐정’ 행위는 ‘유럽인권선언(European Convention on Human Rights)'을

---

114) Statute “On Information” adopted by Parliament on October 2, 1992 (No.2657-XII).

115) Study of the Availability and Use of Personal Information in Public Registers. Final Report to the Office of the Data Protection Registrar J.E. Davies and C. Oppenheim, Loughborough University, September 1999.

일정한도 내에서 벗어나고 있다.[116]

이러한 영국의 사생활권 보호의 훼손은 싱가포르와 이스라엘 수준에 이르러 유럽국가 중에서는 매우 특이한 사례로 파악된다.

Private intelligence (사설 정보업)	Control Risks Group Pinkerton Consulting & Investigations Kenyon Investigation Services Legal Search Ltd MC Eden & Associates Peregrine International Risk Analysis Ruthven & Co Dating Detectives Jell Ltd
Private investigatio (사설 탐정업)	AM Investigations Anglo European Private Detectives Ltd Argyll Investigations Bastille Security Services LRI Research Ltd Nationwide Investigations Group No Hiding Place Ltd. Peter Reay Security Consultants & Special Investigations Limited Cooperate Investigation Service, Ltd. Finlays Bureau of Investigation Ltd Grenadier Investigation Services Hides Detective Agency International Legal Network Ltd International Security Network Ltd John F. Hope & Co.
Private intelligence +investigation	SIASS

116) Draft report on the uses and misuses of Personal Data in employer/employee relationships, by Robin Chater - Director of the Personnel Policy Research Unit, commissioned by the Data Protection Commissioner, January 1999. A Draft code of practice and management checklist by Robin E J Chater, Director: PPRU , commissioned by the Office of the Data Protection Commissioner, February 25th

(사설정보 + 사설탐정)	IIG Associates International Intelligence Ltd
Information Processing (경제정보처리업)	Jell Ltd. Kroll,Inc.-Northern European Practice A&B Associates Access Investigations ADM International Mega Company Services Plc Moore & Associates SIP Services International Fintecs Investigation
Private investigation + information processing (사설정보 + 정보처리)	International Intelligence Ltd Pegasus Investigations Peter Smith Richard Day & Wilson Surveillance Services D.A.C. Group Ltd. Global Intelligence Services Hobson Associates Investigations and Special Tax Services (I.S.T.S) Investigative Solutions JJ Associates TAS Legal Services Tracetech Vogon International Ltd

도표 3: 영국의 사설정보업 현황

그러나 최근 2002년 발효된 정보통제법(Enactment of Private Information Regulation)이 보여주듯, 영국사회는 무제한적인 '사적영역' 의 확대와 그에 따른 공영역의 위축이 야기하는 사회적 합목적성의 훼손에 따른 반성으로 사설정보의 규제를 강화하고 있으며, 그 설립절차와 조건, 그리고 평가를 강화하고 있다.

영국의 사설정보수집기관은 비공식적으로 약 700여개 업체가 활동하는 것으로 보고되고 있으며, 미국의 경우와 마찬가지로 정치정보 보다는 경제정보와 경제인에 대한 정보수집이 주로 유통되고 있으며, 사설탐정(private

investigator)의 활성화로 사설탐정이 개인적으로 유통하는 정보가 많은 부분을 차지하는 것이 특징이다.[117]

가장 대표적인 거대 사설정보기관은 A&B Associates, Access Investigations, ADM International, Global Intelligence Services, IIG Associates 등이 영국을 근거지로 활동하고 있다. 이들의 특징은 사설정보와 사설탐정을 겸하여 영업하고 있으며, 경제정보의 수집과 처리는 미국의 경제정보회사들과 연계하고 있으며, 특히 영국경제가 유럽과 연동되면서 더욱 활성화 되고 있다. 사설탐정(private investigation) 활동은 경제정보의 확인 및 보완 차원에서 이루어지고 있다.

영국에서 이러한 사설정보업과 사설탐정업의 융합형태는 최근의 두드러진 현상으로, 영국의 개인정보보호가 강화됨에 따라 개인정보에 대한 접근성의 저하로 인하여 '신체적 접근(physical access)'를 특징으로 하는 사설탐정 활동이 강화되는 것으로 분석된다.

영국의 사설정보업 중에서 사설탐정의 비율이 유난히 높은 특징을 보이며, 영국정부도 사설탐정의 범람과 개인의 사생활 침해를 우려하여 사설탐정업의 허가는 기존의 정책대로 유지하되, 사설탐정업체와 개인에 대한 면허 'licence' 발급에 필요한 교육의 강화와 재교육, 그리고 윤리 교육을 강화하고 있다. 2003년 영국 내무성은 기존의 면허 갱신에 13시간의 소양, 윤리 교육을 매년 단위로 바꾸어 강화하고 있다.[118]

영국의 사설탐정의 또다른 문제점으로 제기되는 점은 상당수의 사설탐정들이 전직 경찰들로 충원되어 경찰내부의 정보 유출과 경찰조직과 사설탐정의 유착관계에 따른 문제점이 노정되고 있다.

---

117) Regulation of Investigatory Powers Act 2000. <http://www.homeoffice.gov.uk/ripa/ripact.htm>. See the FIPR Regulation of Investigatory Powers Information Centre

118) National Criminal Intelligence Center, 13 May 1999, Available at <http://www.cyber-rights.org/interception/>.

한국에서도 개인정보 보호가 강화될수록 사설탐정(private investigator)에 대한 욕구가 점차 높아질 것을 예측할 수 있다.

정부차원에서 사설정보의 통제를 위한 특별한 조치는 취하지 않고 있지만, 사설탐정에 대한 허가증(permission) 발급 요건은 점차 강화하고 있는 추세이다.

또한 무차별적인 검증되지 못한 정보의 생산과 유통에 따른 사회가치의 훼손과 개인의 사생활권 침해를 방지하기 위하여 개인적 자유의 가치의 일정부분 유보하고 '인터넷 실명제'까지 고려하고 있다.

영국의 사례는 미국과 같은 역사문화적 가치체계를 가진 사회에서 미국보다 앞서 '사회의 공동선' 추구의 가치를 회복하는 사례로 주목할만하다. 이는 미국 사례연구에서 지적된 바와 같이 미국에서 발견되는 언론자유와 사회적 합목적성의 가치충돌에 따른 국익에 반한 무분별한 국가정보 유출의 문제점을 개선하는 하나의 방식으로 풀이될 수도 있으며, 나아가 한국적 모델 정립에 있어 미국식 모델의 보완점으로도 시사하는 바가 크다.

V-2-3. 프랑스

프랑스는 전통적으로 미국과 영국에 비하여 '개인적 자유'와 '사회적 필요성'의 가치선택에 있어 사회적 가치에 다소 무게중심을 두는 사회이다. 사생활권 보호에 있어서도 역시 1958 프랑스 헌법은 명시적으로 포함하지 않았으며, 1994년 개정헌법 역시 사생활권 보호문제를 명시하지 않고 있다.

국립 정보와 자유 위원회(The Commission Nationale de L'informatique et des Libert□s (CNIL))는 독립된 기구로서 국민정보 보호법(Data Protection Act)을 관리하고 있는데 지난 1999년 보고에 따르면 지난 5년간 개인정보 유출에 따른 민원이 2배로 증가할 정도로 사생활 보호에 관한 문제가 증가하고 있다.[119] 이에 따라 프랑스 정부는 유럽의회로부

119) The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well

터의 사생활보호권 침해에 대한 경고를 지속적으로 받고 있는 실정이다.

여기에는 정부기관에 의한 개인사생활 정보유출과 사설정보기관에 의한 사생활침해가 공통적으로 포함되어 있으며, 공식적으로 등록된 약 400여개의 각종 사설정보기관에 의한 피해가 보고되고 있지만 그 정도는 미국과 영국에 비하여 낮은 것으로 평가된다. 사설정보기관의 개체수도 미국과 영국에 비하여 상대적으로 적은 것으로 보고되고 있으며, 사회적 피해와 그 심각성도 상대적으로 낮은 것으로 평가된다.

프랑스 법의 골간을 구성하는 1958년 프랑스 헌법은 개인의 사생활권을 명시적으로 표시하지 않고 있으며, 199년 대법원은 프랑스 헌법에 사생활권이 묵시적으로 표현되어 있다고 판시하였다.

1987년 발효된 정보보호법은 사기업과 정부에 의해 수집된 개인정보의 보호를 목적으로 하고 있다. 개인정보를 열람하기 위해서는 반드시 등록절차를 밟게 명문화되었다. 정부가 개인정보를 수집하기 위해서는 반드시 그 당사자에게 정보수집의 목적을 설명해야하며, 만약 이 절차를 생략했을 경우 개인은 정보제공을 거부할 수 있다.

1998년 프랑스가 유럽연합에 가입한 이후 이 법률조항은 유럽정보보호법에 일치시키키 위하여 변경이 요구되어 1999년 국립정보보호기구를 신설하였으나 현재까지 유럽의회가 요구하는 수준의 강력한 사생활보호법을 제정하지 않고 있다.

유럽연합 인권재판소(European Court of Human Rights)는 프랑스가 수차례 유럽인권헌장을 위반하였다고 판결하였다. 1990년 유럽연합의 판결은 프랑스의 1991년 사생활보장법을 이끌어내게 되었다. 가장 최근에 유럽연합은 프랑스정부의 내국인을 상대로 한 도청행위에 대하여 25,000프랑의 벌금을 부과하기도 하였다. 프랑스에서는 테러의심 집단에 대한 장기간의 도청사건이 지속적으로 발생하였으며, 이러한 도청행위가 미테랑 대통령의 집무실에서 직접 행해진 것으로 조사되기도 하였다.[120)]

---

and Flourishing in Paris, 68 Tul. L. Rev. 1219 (May 1994).

CNCIS에 따르면 1996년 한해에만 프랑스 정보기관에 의해 고용된 사설정보기관과 개인에 의한 도청건수가 10만 건을 상회하는 것으로 보고되었으며, 이에 따라 1997년 도감청 장비의 판매제한이 실시되었다.

프랑스의 정보자유법은 2000년 발효되었다. 이 법안에 따르면 인터넷상에 정보와 게시물을 올리기 원하는 모든 개인은 실명과 자신의 주소를 웹호스트나 웹사이트에 입력과정을 거쳐야하게 되었다. 이 규칙을 위반하는 개인이나 인터넷 제공자는 무거운 벌금과 징역형에까지 처할 수 있다.

프랑스는 강력한 '인터넷 실명제'를 이미 실시하고 있으며, 그 과정을 통하여 개인의 정보가 인터넷에 노출될 위험성도 인정하고, 그 기술적 방지책도 여전히 확고히 개발되지 못한 상태이지만 국민들과 인터넷 사용자들의 커다란 반발을 사지 않고 사회적 합의가 어느 정도 이루어진 것으로 평가된다. [121]

또한 사생활보호법이 유럽의회의 그것에 미치지 못하고 있지만 그에 대한 문제제기와 저항도 크게 사회문제화되지 않고 있는 실정이다. 사생활권에 대한 프랑스사회의 '실용적' 분위기는 크게 개인적 자유와 사회적 통합의 가치충돌에 있어 일정부분 사회통합과 질서를 강조하고 '작은정부'보다는 '큰정부'라는 정부의 역할을 강조하는 프랑스의 역사문화적 전통에서 찾을 수 있다.

V-2-4. 일본

일본의 경우 그동안 통신제한을 위한 입법이 없었으나 1999년 범죄수사를 위한 통신방수(傍受)에 관한 법률을 공포하여 합법적 통신감청을 할 수 있도록 하였다.[122]

---

120) A full history of the developments since the law was first introduced on May, 1999 is available at www.iris.sgdg.org/actions/loi-comm/index.html

121) Code of Post and Telecommunications, L. 41.

122)The Act for the Protection of Computer Processed Personal Data held by Administrative Organs, Act No. 95, 16 December 1988 (Kampoo, 16 December 1988).

일본은 우리와 유사한 역사문화적 토양과 정치경제적 구조를 가진 국가이나 우리보다 앞서서 다양한 가치의 분화를 이루었고 사적영역의 확대를 경험한 사회로 '사설정보' 에 대한 대응책에 있어서 참고할만한 경험을 제공한다.

일본 역시 우리와 마찬가지로 프랜시스 후쿠야마가 제기한 사회적 자본으로서의 사회적 신뢰 구축이 미흡한 사회로 평가되며, 따라서 '사설정보' 의 생산과 소비가 활발한 사회이다. 덴츠연구소(電通研究所)의 통계에 따르면 사설경호나 사설탐정기관은 미국과 영국에 비해 현저히 떨어지나 사설정보회사와 정보지 개체수는 오히려 영국과 미국을 능가하는 것으로 조사된다.[123)]

그러나 세계최대의 출판국가라는 그 특성상 사설정보의 생산과 유통은 인터넷을 통한 경우보다는 출판 경로를 통하여 유통되는 비율이 현저히 높다는 것이 특징이다. 한국사회는 비록 부정확한 추정자료이기는 하나 약 300-400종의 사설정보지가 유통되는 것으로 파악되는 반면, 일본의 경우는 5000종 이상의 사설정보지가 범람하고 있는 것으로 보고된다.[124)]

서구사회와 차별화되는 현상은 서구사회의 사설정보업은 대부분이 경제정보에 모아지고 있으나, 일본은 서구사회보다 오히려 더 고도화된 경제구조를 가지고 있음에도 불구하고 한국사회의 사설정보지 시장과 마찬가지로 여전히 '정치정보' 의 유통이 많다는 점이다. 이는 일본이 한국사회와 마찬가지로 '정치의 영역' 이 여전히 사회의 중심축으로 작용하고 있으며, 정경유착 현상이 계속되고 있다는 방증이기도 하다.

또한 일본 사설정보업의 특징은 서구사회와는 달리 사설정보의 생산이 많은 경우 '서설탐정(private investigators, detectives)의 활동과 연계되어 이루어지는 점이다. 이는 일본에 아직도 강하게 남아있는 ' 인간중심 '의 사회망 구축이라는 사회적 특성과도 밀접하게 관련되어 있으며, 따라서 자료와

123) 덴츠연구소, 일본 신용조사업의 현황, 전망 장기예측 보고 (2001)

124) Nigel Waters, 'Reviewing the adequacy of privacy protection in the Asia Pacific Region, IIR Conference Information Privacy - Data Protection, 15 June 1998, Sydney; see also Ministry of International Trade and Industry (MITI) 'Japan's views on the protection of personal data' (April 2003).

1차정보(raw information)에 대한 분석과 추적을 통한 정보생산을 하는 서구사회와는 차별화된 모습으로 한국의 유형과 유사한 특징을 보인다.

이러한 사설탐정(혹은 정보맨)에 의한 직접적인 물리적 접근(physical access)에 의한 1차정보 수집은 필연적으로 도감청, 도촬등의 정보수집 장비의 발달과 수요를 증대시키는 현상을 보이는 바, 이 역시 우리사회의 모습과 유사성을 보인다. 그리고 일본사회에서 야기되는 사설정보업의 많은 문제는 이러한 정보수집 대상자에 대한 물리적 접근 과정에서 불법, 탈법 행위가 발생한다는 데 있다.

일본의 경우가 우리에게 시사하는 바는 현재 우리사회에도 무허가 사설탐정업이 점증하고 있는 것으로 보고되는 바, 사설정보업에 대한 거시적 차원에서의 근본적 정비책이 마련되지 않는다면, 일본형의 사설탐정에 의한 정보수집과 그에 따른 '범죄행위'의 만연이라는 부정적인 방향으로 전개될 우려가 높다는 점이다.

일본의 사설탐정은 미국과 영국과 같이 정부의 허가증(license)와 등록에 따르기 보다는 무자격, 무허가인 경우가 많아, 정확한 통계는 어려우나 2004년도 기준으로 지방자치단체에 신고된 사설탐정의 수는 약 3,000명으로 집계되고 있으나, 무허가 사설탐정의 수는 이의 약4-5배에 달할 것으로 추계된다.[125]

공식적 사설탐정의 수는 미국과 영국에 비해 적으나, 미등록된 무허가 사설탐정을 포함시킬 경우 그 수는 미국과 영국을 상회한다. 또한 전국에 산재한 약 50-60개소의 유.무허가 사설탐정학원의 공식 수강생도 3,000명에 달하고 있으나, 그 교육 커리큘럼은 영국과 미국의 규범화된 프로그램과 윤리규정의 강화보다는 실질적 '기술'과 '현장교육'에 집중되고 있다.[126]

실제로 많은 사설탐정 양성소에서는 미국과 영국에서는 사설탐정 교육 커리

125)"Japan Ministries To Compile Credit Data Protection Bill," Nikkei, July 4, 1999.
126) "Japan, U.S. bodies ink deal on data-privacy certification," The Yomiui Shimbun, May 19, 2000.

큘럼에서는 다루지않고 사설경비(private security) 양성소에서 다루는 각종 호신술을 포함시키고 있으며, '변장술' 까지 포함시키고 있다. 이는 기본적으로 일본의 사설탐정이 법과 탈법의 경계를 넘나드는 상황을 설명해 준다.

이들 대규모의 사설탐정들은 정규적인 사설정보업체에 연계되기보다는 일본의 '신용조사업' 에 연계되어 각종 기업과 경제단체의 '인물' 중심으로 정보를 수집하며, 그 정보는 신용조사업소들이 비공식적으로 유통시키는 사설정보지와 각종 소문의 인터넷 사이트 내용구성에 이용된다.

서구적 개념의 사설정보(private intelligence)와 정보 브로커(information brokerage)는 미국과 영국에 비해 미발달한 상황이며, 한국에 비해서도 덜 활성화되어있다. 그 원인은 1998년 채택되어, 2001년부터 시행되기 시작하였으나 아직 그 내용상 미비점이 많으며, 또한 전통적인 일본관료사회의 소극적 적용으로 아직 실효를 거두지 못하는 일본정부의 '정보공개법' 의 한계에 있는 것으로 판단된다. 또한 고도정보화 사회로 진입하였으나 아직 정보의 생산을 정부가 독점하는 상황에서 공공재로 민간에 공개되는 1차정보풀 (raw information pool)의 절대적 부족으로 전문적인 정보 브로커(information broker)나 독립정보연구소(independent information researcher)들의 합법적 활동 여건조성이 미비한 데에서 찾을 수도 있다.

그러나 한국사회와의 차별성은 그러한 사설정보회사가 독립적인 회사의 형태보다는 기업과 연구소의 부속기관으로 활동하는 경우가 많아 비교적 사회적 책임과 공신력을 확보하고 있으며 따라서 수집되고, 생산되고 소비되는 사설정보 역시 우리사회에 비하여 신뢰도를 확보하고 있으며, 그 사회적 폐해도 커다란 사회문제화 되지는 않는 실정이다.

이러한 정비는 일본의 경우 기본적으로 1945년 이래 사적 영역의 정보이용과 유통은 시장의 자유 검증에 맡기는 것을 원칙으로 했으나 1988년 사설기관의 전화도감청에 의한 정보생산, 1997년 역시 사설정보기관에 의한 개인의 재무금융 현황파악, 그리고 2000년 사설기관에 의한 개인의 혈액형 표본조사와 그 정보유통등의 사회문제가 발생하고 그에 따른 '사생활 보호법' 이 제정되고 강화되어 현재의 상태에 이르고 있다.[127)]

그러나 이러한 사설정보에 대한 제도적 규제 강화는 표면적으로는 효과를 발휘하는 것으로 평가되기도 하지만 다른 한편으로는 점차 사설정보기관이 거대기업군에 소속되면서 정보이용의 가격상승과 그에 따라 정보격차를 심화시키는 부작용을 야기하는 것으로 나타나고 있다.

따라서 일본 역시 미국과 유사한 본원적 해결책으로서 공적정보 제공의 확대를 통하여 사설정보 생산과 그에 따른 사회적 비용 감축의 방법을 채택하고 있으며, 그 시발점을 '정보공개법'의 보완과 실행에서 찾고 있다는 점은 유의할만한 대목이다.

V-2-5. 싱가포르

싱가포르(Republic of Singapore)

싱가포르에는 포괄적인 개인정보 보호법이나 사생활권 보호법이 존재하지 않는다.[128] 싱가포르 정보는 사회통제 목적을 위한 잠재적 위험집단과 정치적 반대자들에 대한 통제와 감시에 매우 적극적이다. 단적으로 1986년 당시 리콴유 총리는 그의 사생활권에 대한 견해를 다음과 같이 밝히고 있다.

"나는 종종 시민들의 사생활을 침해한다고 비난받는다. 그러나 내가 그러지 아니한다면, 그리고 그러지 아니했다면 우리는 현재 존재하지도 못했을 것이다. 또한 나는 한치의 망설임 없이 우리는 앞으로 존재할 수도 없다고 말할 수 있으며, 경제적 번영도 이룰 수 없었을 것이라고 말할 수 있다. 무엇이 옳은 것인지는 우리가 결정하는 것이며, 국민들이 어떻게 생각하는지는 신경쓰지 않는다. 그것은 또다른 문제일 뿐이다" [129]

1998년 싱가포르 인터넷 자문국(National Internaet Advisory Board)은 개인정보 보호를 위한 산업계의 자율규제 방안을 발표하였다. 그러나 싱가포르

---

127)MITI, Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector, March 4, 1997. <http://www.jipdec.or.jp/security/privacy/guideline-e.html >. For a detailed analysis of the guidelinest, see MITI Handbook Concerning Protection of Personal Data, February 1998. <http://www.jipdec.or.jp/security/privacy/handbook-e.html>.

128) Constitution of the Republic of Singapore, 16 September 1963.

129) Lee Kwan Yew's speech at National Day Rally, 1996, Straights Times, 20 April 1987, Cited in The Political Economy of Social Control in Singapore

경찰은 여전히 광범위한 범위 내에서 모든 컴퓨터를 검색할 권한을 부여받고 있으며 법원의 영장 없이도 매우 공격적으로 개인정보를 수집할 수 있다.

실제로 1999년 싱가포르 내무성은 가입자에게 통고하지도 않은 상태에서 20만명의 SingNet 가입자의 인터넷 사용내역을 검색하기도 하였다. 싱가포르 정보통신국은 이것이 불법이 아니라고 발표하였다. 130)

싱가포르의 사설정보업(private intelligence industry)의 특징은 국제교역거점 지역(international trade post)이라는 지역적 특성을 반영하여, 상업 정보에 대한 사설정보업이 활발하며, 영국과 미국의 정보산업체도 진출하고 있다. 그러나 영국, 미국등과 같은 서구 사회와는 달리 대규모 정보산업이 발달하지는 못하고 있다. 이러한 특징은 싱가포르의 경제가 화교에 의해 장악되어 있고, 화교사회는 특정내부집단간의 정보교환에 의존하기 때문에 국내 정보산업의 상업화에 한계가 존재한다.

싱가포르는 상기 사례들과는 커다란 차별성을 보이는 특이한 경우로 평가된다.싱가포르의 정보이용법은 기본적으로 사회적 이익을 우선으로 하고 그 대신 정보의 공익성과 접근성 제고에 맞추어져 있다.

싱가포르는 기본적으로 영국의 법체계를 따라 헌법이 규정되었지만 특이점은 사생활권에 대한 어떠한 명시적 조항도 담고 있지 않으나 여타 국가에 비해 사설정보 생산과 유통에 따른 사생활의 피해는 상대적으로 적은 것으로 보고된다.

싱가포르의 다양한 사설정보 산업 중에서 국내시장을 목표로 한 정보처리 산업은 비교적 취약한 편인데, 이는 싱가포르의 개인정보를 비교적 수월하게 각 민간부문에서 수집할 수 있기 때문인 것으로 파악되고 있다. 131)

그 대신 싱가포르의 지역 특성상 싱가포르에는 2004년 현재 Private Investigators Mall, USA Records Search, Discreet Data Research,

---

130) The Straits Times, May 12, 1999.

131) "Singapore To Get 'Speakers' Corner'," Asian Wall Street Journal, April 25, 2000.

Bakground Check Gateway, Creative Research Inc. Advanced Surveillance Group, Fast Track Cyber Master, Investigative Resources International 등 거대 다국적 정보산업체를 비롯한 약 170여개의 사설정보, 사설탐정, 정보처리 업체들이 활동하고 있다.[132]

개인의 사생활권 보장과 개인정보 보호, 그리고 공공의 이익 사이에서 공동체의 이익에 비중을 두는 싱가포르의 정책기조에 기반하여 사설정보업은 허가제가 아닌 신고제로 간편화되어 있으며, 사설정보업체들의 활동에 제약은 다른 국가들에 비하여 매우 제한적이 편이다.

2005년 현재 등록된 사설 정보지(intelligence report)는 국내 정보지 20여개가 있으나 등록되지 않은 정보지까지 감안하면 70여개가 넘는 것으로 보고되고 있다. 그러나 등록과 미등록과는 실질적으로 법적 제한에서는 거의 차이가 없다. 등록된 사설정보지의 경우에도 그 내용에 대한 실질적인 제재조치는 '정부'와 '국가 기밀' 혹은 정부에 불리한 정보를 게재하지 않고, 개인의 신상에 대한 정보일 경우에는 그 정보의 '진위'와 '정보원'에 대한 제재는 이루어지지 않고 있으며, '피해구제'에 관한 법적, 제도적 장치도 마련되어있지 않다.[133]

따라서 많은 다국적 거대 정보업체들이 싱가포르를 global networking의 head office 지역으로 활용하여 전세계적으로 가장 많은 거대 정보업체들이 활발하게 활동하고 있다.

그러나 사설정보업이 국내 산업이나, 싱가포르 내의 사생활권과 개인정보를 침해하는 사례보다는 그 성격상 전세계적인 문제로 희석되고 있는 실정이다.

이러한 싱가포르의 특징은 무엇보다도 정보의 공정성과 접근성의 평등에서 기인하는 것으로 평가되며, 한국사회의 한 대안적 모델로서 연구할 가치가 있다.

---

132) The Straits Times, September 27, 2004.

133) 참조; Christophen Tremewan, The Political Economy of Social Control in Singapore (St. Martin's Press, 1994), christopher Bergersen, "Information Industry and Political Economy of Singapore and Malaysia" in Information Society.

V-3, 사례연구의 분석결과

5개국 사례 심층분석(in-depth study)에 따르면 현재 전세계적으로 오히려 선진국들을 중심으로 점증하는 terror의 위협으로부터의 국가의 재산과 생명을 보호한다는 취지하에 개인적 사생활권이 상당부분 제한되고 개인정보 보호가 약화되고 있는 추세를 알 수 있다.

5개국 사례에서 보듯, 개인 정보와 사생활 보호에 관한 법적 제도적 장치가 완비된 국가에서도 사생활권 침해에 대한 우려는 지속되고 있다. 선진 국가에서 법적 보호장치는 급속하게 발달하는 정보기술을 따라가지 못하여 개인정보와 사생활 보호에 심각한 괴리현상을 보이고 있다. 또한 다른 국가들에서는 국가기관과 정보기관에 광범위한 법적책임의 면제가 이루어지고 있다.

세계 각국에서 통신감시가 광범위하게 이루어지고 있으며 몇몇 가장 민주적인 국가도 예외는 아니다. 미국 국무성 인권 백서는 약 90개국에서 정치적 반대세력에 대한 통신감청이 이루어지고 있다고 보고된다. 1996년 프랑스 정부는 민간부문에서 연간 약 10만건의 도청이 발견되었다고 발표하였다. 아일랜드에서는 영국이 북아일랜드에서 영국과 아일랜드 사이의 모든 통신을 감시한 것이 드러나 거센 항의가 일어나기도 하였다.

사생활권이 강력히 보호되는 국가의 경찰조차도 정치적 목적에 따라 기소되거나 혐의가 없는 일반시민에 대한 정보까지 광범위하게 수집하고 있는 실정이다. 최근 사생활 보호의 강력한 전통이 있는 스웨덴, 덴마크, 노르웨이 같은 북유럽 국가들에서 경찰과 정보기관에 의한 정보수집에 대한 감찰이 이루어졌으며, 스위스에서는 경찰의 불법행위가 야기한 스캔들로 인하여 정보보호법이 제정되기도 하였다. 동유럽 국가들에서는 과거 비밀경찰에 의해 수집된 정보의 공개문제가 여전히 논란거리로 남아있다.

미국에서는 소비자 신용정보 보호법에도 불구하고 많은 기업들이 이 정보를 마케팅에 광범위하게 이용하고 있다. 또한 많은 국가에서는 소비자 개인 신용정보에 관한 부적절한 보안으로 인하여 수많은 소비자 개인정보가 유출되고 있는 실정이다.

많은 정부들이 발전된 정보기술과 통신기술을 바탕으로 개인 정보의 감시와

통제를 허용하는 법적, 제도적 장치를 강화하고 있으며 정보화 시대에 개인 정보 보호는 점차 약화되는 추세이다.

특히 IT산업이 발달한 사회일수록 인터넷 정보의 유통에 의한 개인적 사생활 권의 침해 방지와 완화를 위하여 사용자의 책임을 강화하고 통제하는 방향으로 법적, 제도적 장치를 마련하고 있으나 그 실효성는 기대에 미치지 못하는 것으로 평가된다.

사설정보업에 대한 규제와 통제는 기본적으로 최소화하는 가운데, 공적정보의 생산과 제공의 양과 질을 늘이고 높여서 사설정보의 수요를 줄이는 방향으로 나아가고 있음을 알 수 있다. 이는 우리사회에서 인터넷 시대에 사설정보의 폐해을 줄이는 대응책을 마련하는 데 의미있는 논의의 시발점이 될 것이다.

이 결과가 보여주듯 한 사회가 선택할 수 있는 사회공동체에 합목적적인 정보의 유통과 사생활과 인권보호의 접점은 단일한 기준에 의해 설정되고 실현되는 것이 아니라 개별 사회의 구조(정치, 경제, 문화)에 최적화되어야 함을 알 수 있다. 이러한 기본적 방향성 위에서 한국사회의 선택과 법적, 제도적 장치도 마련되고 수정, 보완되어야 한다.

이상 41개국에 대한 cross-country analysis와 5개국에 대한 사례연구를 통하여 우리는 잠정적으로 다음과 같은 유의미한 시사점을 발견할 수 있다.

1) 무분별한 사생활권 보호와 사회적 비용 감소를 위한 제도적 장치 마련은 개별 사회의 역사문화적, 사회경제적 조건에 부합하여야 한다.

2) 정보 보호법과 사생활 보호법만으로 '사설정보'에의 욕구와 수요를 통제하고 사생활권의 보호해 주지는 못한다.

3) 사회적 신뢰도(social trust)의 제고만이 사설정보에 대한 욕구와 수요를 근원적으로 감소시킬 수 있다.

4) 사회적 투명성과 정보독점, 그리고 공적 정보에 대한 신뢰가 확보되지 못한 상태에서의 개인정보 보호의 강화는 오히려 사설정보에 대한 욕구를 증대시킬 수도 있다.

5) 정보화 시대에 정보의 자유와 사회적 합목적성의 조화를 이루기 위한 노력은 현재 세계적으로 점차 사회적 합목적성을 강화하는 방향으로 전개되고 있다.

6)정보의 생산과 유통은 그 특성상 단순히 시장논리에 일임하기에는 부적절한 특징이 있다.

7)정보화 시대의 정보생산은 차츰 국가의 배타적 영역에서 민간부문과의 협조체제로 이전하고 있다.

이와같은 외국 사례연구로부터 도출된 시사점을 바탕으로 한국사회가 정보화시대에 정보의 자유로운 생산과 유통을 통한 국가발전을 이루고, 동시에 정보화 시대에 우려되는 정보격차로 인한 사회갈등과 사생활권 침해의 위험을 최소화하고, 무분별한 사설정보기관의 난립과 이에 따른 사회혼란을 방지하기 위한 정책적 고려사항과 그러한 정책적 고려가 이루어져야 할 방향과 기본틀 (foundational framework)을 아래에 살펴본다.

Ⅵ. 정책과제

Ⅵ-1. 정책의 방향

사설정보지들이 무책임하고, 왜곡된 정보를 생산하거나 가공하여 유통하여 개인적, 사회적 피해를 야기하였을 경우 그 책임 소재를 명백히 하기 위하여 사설정보지의 '주체'를 명확히 하여야 한다. 이러한 제도적 장치는 영국과 일본에서 이미 실시되어 일정정도 효과를 나타내고 있는 것으로 평가된다.

왜곡된 정보의 유통에 따른 피해구제는 현실적으로 금전적이나 법적으로 명백히 이루어지기 어려운 경우가 많은 특성을 감안하면, 사설정보업체에 대한 '평가제'를 도입하여 문제를 야기한 업체나 주체는 사설정보시장에서 영

구히 추방하는 것도 고려되어야 한다.

외국의 사례를 우리사회와 비교해 보면, 우리사회의 사설정보의 유통이 야기하는 사회적 해악의 문제는 그에 관한 법적, 제도적 장치가 크게 부족하여서라기 보다는 그러한 법과 제도적 장치의 준수와 집행에 있어서의 미비점이 큰 것으로 판단된다.

한국사회는 전통적으로 씨족, 부족단위의 '농경 공동체'를 영위하여 왔으며 농경공동체의 문화적 특징은 사적영역과 공적영역의 구분이 분명치 않고, 따라서 '법'에 대한 인식도 발달하지 못한다.[134] 이러한 특징적 문화유형은 우리사회에서 개인의 사생활권을 침해하고도 큰 도덕적 책임감과 죄의식을 느끼지 못하게 하며, 사생활에 대한 법적 보호에 대해서도 둔감한 경향을 보인다.[135]

현재 문제가 되는 사설정보지의 확산과 그 폐해도 이러한 인식체계 위에서 확대되고 있는 측면이 존재한다. 따라서 사적영역과 공적영역을 명확히 구분할 수밖에 없고, 그래야만 정상적으로 작동할 수 있는 지식정보화 사회에서 개인의 사생활 보호를 위해 마련된 제도적, 법적 장치들의 집행은 엄정해야만 한다.

정보의 독과점 현상과 그에 따른 사설정보지의 난립과 폐해는 정보의 수집과 생산, 가공 과정에 있어 영역의 파괴와 유착관계에서 비롯된다. 흔히 법조계의 '전관예우'라는 관행이 사회문제로 대두되듯이 해외의 거대 사설정보기관의 종사자들은 대부분 '공영역' 출신자들로 충원되어, 그러한 개인적 커넥션을 활용하여 정보접근성을 확보하고, 정보를 독점하고 왜곡 유통시키기도 한다.

사회적 합목적성에 부합되지 않는 사설정보의 대량생산과 소비를 예방하기 위하여 특정 공직분야의 종사자들은 일정기간 사설정보기관에 종사하는 것을 금지하는 제도적 장치 마련이 요구된다.

---

134) 조긍호, 한국인의 의식구조 (해냄, 2002)
135) 오세철, 한국인의 사회심리 (박영사, 1997)
한백연구재단, 한국인의 원형에 관한 델파이 연구 (1998)

상기 사례 연구들이 보여주듯 권력의 분산과 상호견제 시스템은 정보의 독점현상을 완화해 주고, 독점화된 정보(monopolized information)가 왜곡되었을 경우 야기하는 사회적 비용과 폐해의 위험성을 감소시켜 주며, 또한 단수가 아닌 복수의 '정보 중심' 은 사회 구성원들의 정보접근성을 향상시켜 무분별하고 무책임한 사설정보에 대한 욕구를 근원적으로 감소시키는 기제로 작용할 수 있다.

많은 논란이 존재하지만 현재 진행되는 참여정부의 당정분리, 지방분권화등 권력의 분산과 시스템에 의한 정부의 운영이라는 커다란 방향성은 이러한 관점에서 건강한 정보화 시대를 구현하기 위한 하나의 조건 충족이 될 수도 있다.

사회 공공재(public goods)로 공개 제공되는 양질의 정보의 영역을 현재보다 대폭 확충시킬 필요가 있다. 제공된 정보를 이용, 가공하여 기회와 재화를 창출하는 것은 개인적 능력에 따라 차별화 될 수밖에 없으므로 정보 이용에 따른 결과의 평등을 보장할 수는 없지만 최소한 '기회의 균등' 의 원칙 위에서 정보의 접근성의 평등을 확대하여야 한다.

정보기회와 접근성의 평등의 원칙은 John Rawls의 minimax와 maximin의 기준 설정이 사회통합과 digital, information divide의 완화를 위해서 바람직하다. 다시 말하면 정보접근성이 취약한 계층에 국가적 차원에서 기회의 확충에 주안점을 두고, 상대적으로 정보접근성이 앞선 계층에 대해서는 특별한 지원을 최소화 하는 방안이다.[136]

상기 사례연구를 기반으로 하는 정책대안은 구체적 정책프로그램(action program)의 제시보다는 법적, 제도적 정책 마련을 위한 방향성 정립의 틀(framework)의 정립에 맞춘다.

사설정보지의 범람과 폐해에 대한 정책적 접근은 전통적인 사회과학적 연구방법인 '진단에 따른 처방' 의 방식에 의거, 문제의 원인을 파악, 제거하고 목적달성을 위한 새로운 '요소 투입' 의 방식을 채택할 때에만 현실에 입

136) Rawls, John, A Theory of Justice, (Harvard University Press, 1972)

각한 실효성 있는 대책 수립이 가능하다.

이러한 정책기조의 틀 속에서 선택되어야 할 방향성은 아래와 같이 설정되는 것이 바람직하다.

1) 비공개정보의 최소화와 공개정보의 확대를 통한 국가정보의 공공성 제고
2) 공개되는 국가정보 질, 정확성, 신뢰도의 제고를 위한 정보생산, 유통 시스템의 구축
3) 국가정보 생산 능력 제고를 위한 산학정 협력체제 구축
4) 비공개 정보 유출에 대한 엄격한 법적 통제 강화

Ⅵ-2. 공공재(public good)로서의 정보의 확대
대국민 정보서비스 강화

사설정보지의 양산과 그에 따른 사회적 폐해는 근본적인 원인(遠因: distant cause)은 정보의 수요와 공급의 균형 붕괴에서 찾을 수 있다. 위에서 지적한 바와 같이 지식정보화 사회의 다양한 새로운 가치의 출현에 따른 다양한 정보의 생산은 모든 사람들의 정보필요성과 정보욕구를 자극한다.

더욱이 세계화의 흐름이 가속화되면서 외부로부터의 새로운 가치와 정보가 무제한적으로 생산되어 여과없이 무차별적으로 내부사회에 유통됨으로써, 정보욕구와 그 수집과 분석, 해석 능력은 더욱 절실한 문제가 된다.

이와 같은 시대적 환경 속에서 국민들이 필요로 하는 정보의 수집과 배포는 '국가의 일' 중에 가장 긴요한 임무로 자리를 잡게 되었다. 과거 'hard power'를 중심으로 한 ' high politics' 시절, 국가의 핵심적 업무가 '국방' 이었다면, 세계화와 정보화로 상징되는 'soft power'의 ' low politics' 혹은 소위 '세계경제전쟁' 시대인 오늘날은 국가의 핵심적 업무가 국가경제의 중추를 담당하는 기업활동을 도와 기업들이 '세계경제전쟁' 에서 승리하도록 하는 것이다. 그것이 곧 국가의 대국민 서비스의 제1의적 목록이 되었다.[137]

다음과 같은 해외사례들이 이러한 국가 역할의 변천을 극명하게 보여준다.

미국의 경우 국가정보기관이 사기업을 위한 해외정보활동의 정당성 문제를 놓고 오랜 기간 치열한 논쟁이 지속되었으나 1970년대 이후 CIA가 미국기업 활동을 보조하기 위한 해외정보 업무를 본격적으로 개시하였다. 이는 점차 치열해지는 세계경제전쟁 속에서 미국의 사기업들의 성공이 곧 미국의 국익으로 연결된다는 인식과, 유럽과 일본경제의 거센 도전에 직면하였던 미국의 선택이었다. 일본기업의 성공에 대한 분석에서 미국은 일본정부의 기업에 대한 적극적인 해외정보 제공이 주요 원인 중 하나라는 사실을 발견하였다.[138]

MITI(Ministry of International Trade and Industry)와 JETRO(Japan External Trade Organization)으로 대표되는 일본정보부의 주된 임무는 기본적으로 경제정보 수집과 분석으로 정평이 높다. 이러한 경제정보들은 대부분 이들에 의해 수집되고 분석, 처리되고 있다. 일본정부 정보당국과 민간기업 사이에는 매우 심도깊은 교류가 일상화 되어있다.[139]

이는 정부의 정보업무가 '정부' 자체를 위한 것이 아니라 사기업으로 대표되는 민간의 필요에 의해 이루어지는 대표적인 사례라고 할 것이며, 이러한 정부의 정보업무 역량을 민간을 위한 서비스 차원에서 파악한 것이 일본경제성장의 원동력 중 하나라는 것은 아무도 부인 할 수 없다.

따라서 국민들이 사설정보의 필요성을 절실하게 느끼지 않을 정도로 국가가 공공의 재화로서 신뢰할 수 있는 충분한 양의 정보를 수집, 생산하여 유통시켜야 한다. 이는 기본적인 정부의 의무이기도 하다.

현재 진행중인 정보공개법도 이러한 방향에서 이해할 수 있으며, 사설정보의 폐해를 최소화하기 위한 중요한 조치로 파악된다. 그리고 정보공개법은 단순

---

137) 참조; Robert Gilpin, *Political Economy of Internation Relations*, Robert Keohane, *Neorealism*

138) U.S. Japan Joint Statement on Electronic Commerce, May 15, 1998.

139)Government of the United Kingdom, Code of Practice on Access to Government Information, April 4 1994, revised in January 2001,

히 정부운영의 투명성 차원이 아니라 일반국민들과 민간에게 신뢰할 수 있는 다양한 분야의 1차정보(raw information)의 제공확대의 차원에서 진행되어야 한다.

경제적 재화로서 정보의 특징은 정보의 생산은 그 생산비용은 매우 높으나 그 복사는 매우 저렴하다는 데 있으며, 또한 디지털 시대에 정보 복제 비용은 더욱 저렴하다. 따라서 초기 정보생산비를 누가 부담할 것인지, 그리고 어떠한 정보를 국가가 생산할 것인지가 가장 주요한 문제가 된다. 여기에서 정부의 주도적이고 책임있는 역할이 요구된다.

사례연구 역시 정부가 사회에 양질의 충분한 information pool을 제공해 준 사회에서는 비교적 사설정보지의 폐해가 감소되고, 반대의 경우에 그 사회적 비용은 증대하는 것을 보여준다.

정보란 일반적으로 '공공재(public good)'라고 불리지만, 현상황에서 엄격하게 말하자면 이는 정확치 않은 표현이다. 공공재란 1) 한사람이 이 재화를 사용함으로써 다른 사람이 그 재화를 사용함에 제한을 받아서는 아니되며; 2)아무도 이 재화의 사용으로부터 배제되어서는 안된다. 정보저장과 복사기술이 획기적으로 발달한 정보화 시대에 쉽게 복사할 수 있는 정보의 성격은 첫째 조건을 충족시키지만, 정보는 그 속성상 공공재로서의 두 번째 조건을 충족시키기 어렵다. 예를 들어 위성방송은 위성수신기를 설치하지 못한 사람들에게는 접근할 수 없다. 인터넷 정보도 마찬가지이다.

따라서 정부정보가 진정한 의미에서 '공공재'의 역할을 수행하기 위하여는 두 번째 충족조건인 '정보 접근 용이성'을 제고시켜야 하며, 시민들에게 '무상'으로 제공되는 다량의 양질의 정보가 존재하여야 한다.

특정정보의 창출을 공적 영역이 담당하여야 할지 사적영역에서 담당하여야 할지의 문제와 정보의 공공성 확보와 제고방안은 다음의 3가지 관점에서 파악되어야 한다.

1. 정부의 정보 생산은 어떠한 경우이든 국민들의 세금에 의존한다는 점을

명확히 하여야한다. 또한 국민의 세금에 의해 생산된 정보는 공공재(public goods)로서 납세자인 국민들에게 공평하게 그 혜택이 돌아가야 하는 것이 대원칙으로서 준수되어야 한다.

정부활동의 자금은 사기업에 부과되는 세금에 의해서 충당되므로 세금에 의해 조성되는 자금은 사기업에 의해 소비되는 자금보다 더 비용이 크다. 왜냐하면 세금에 의해 조성되는 자금은 다른 사경제 활동을 위축시킬 수 있기 때문이다. 정부활동의 예상되는 혜택은 그 예상비용보다 커야하는 것은 물론이다.

2. 사영역에 의한 정보생산은 권력의 독점을 야기할 수도 있다. 사설정보업체에 의한 정보생산이 경제적이기 위해서는 그 업체가 이미 어느 정도의 시장 독점력을 확보하고 있어야 한다는 논리적 모순도 여기에서 발생한다. 이러한 고려는 정부에 의한 정보생산과 통제가 사설업체에 의한 그것보다 훨씬 바람직하다는 쪽에 무게를 두게 된다.

3. 정부에 의한 정보생산이 사설업체보다 그 생산비용이 훨씬 저렴한 경우가 있다. 이러한 대표적 경우는 정부가 정부활동을 스스로 보고하는 정보의 생산이다. 혹은 사회적으로 가치 있는 정보가 정부의 법집행과정에서 발생하는 부산물일 경우도 이에 해당된다.

이러한 관점에서 과학기술분야는 정부가 그 정보생산을 담당하여야 할 가장 바람직한 분야이다. 또한 국가경제통계, 법률 기록, 판결등 역시 공공성이 강하고 또한 그 공정성이 요구되는 분야로서 정부가 생산을 담당하는 것이 바람직하다.

반대로 정부의 정보생산이 바람직하지 못한 분야는 정부가 사설업체에 비해서 그 정보의 생산에 있어 뚜렷한 비용우위를 점하지 못하는 경우, 정부가 사설업체와 그 정보의 생산을 두고 경쟁을 벌이는 것은 바람직하지 못하다. 만약 어느 사설업체가 특정한 정보생산에 대한 의지가 있다면 그 분야에 정부가 반드시 나서야 할 근거는 사실상 희박하다. 정보생산에 대한 정부의 기본정책은 자신이 직접 사설업체의 역할을 대신하기 보다는 사적영역을 통하

여 정보의 질을 향상시키기 위한 감독의 역할이 바람직하다.

만약 방대하고, 양질의 신뢰성을 담보한 정보들이 공적인 기관에서 생산되어, 역시 투명하고 공적인 경로를 통하여 보급되어 유통된다면 information brokerage나 independent information researcher 형태의 바람직한 사설정보업과 사설정보지 유통이 가능한 여건이 조성될 수 있다.

사실상 방대한 정보가 공공재로서 시장에 공개되었을 때, 특정목적을 위한 정보의 필요를 느끼는 개인이나 단체도 어떤 정보가 필요한지, 그리고 어디에서 그 정보들을 수집할 수 있을지, 또한 그 정보들을 어떻게 분석하여 결론을 도출할지에 대해서는 능력을 갖추지 못한 경우가 대부분이다. information broker나 independent information researcher의 역할은 현재 우리사회에 문제를 야기하는 1차 정보생산(raw information)에 있는 것이 아니라 이미 공개된 공신력있는 정보를 분석하여 특정목적의 고객에게 전달하는 것이다.

따라서 이들의 활동은 비공개정보(classified information) 유출의 통로가 될 위험성도 낮고, 또한 소문과 유언비어를 확대재생산하여 사회적 혼란을 야기할 위험 역시 낮다고 할 수 있다.

information broker와 information researcher들의 정보시장에서의 성패여부는 기본적으로 공개된 정보의 수집과 처리능력, 그리고 본인의 종합적 분석력에 의해 결정된다.

현대사회에서 점차 많은 정보작업이 공개적인 영역에서 이루어지고 있다. 현대 국제정치와 정치발전, 그리고 기술진보는 정보원천의 양과 질에 있어 그 공개성이 점차 확대되고 있다. 현재 정보는 전화, 팩스, 인터넷, 라디오, 그리고 TV등을 통하여 즉각적으로 접근 가능하게 되어가고 있다. 사회주의의 몰락과 함께 동서세계의 접촉 역시 획기적으로 증대하게 되었으며, 전세계 거의 모든 국민들이 이념과 국경에 구애받지 않고 지구의 거의 대부분 지역을 자유로이 왕래할 수 있게 되었다.

미국의 경우 CIA는 소비에트 해체이후, 냉전구조 해체와 함께 본격적으로 개시된 세계화 시대를 맞이하면서 공개된 정보가 4년간 약 10배에 이르는 것으로 보고된다. 사설정보업체들이 민간과 정부의 정보요구에 대응하는 방식에 있어 경제 정보에 관한 한 약 95%가 공개된 정보에 의해 수집되고 가공, 유통되고 있는 것이 현실이다.[140]

이것이 미국의 사설정보업체들이 신뢰성을 확보하고 무책임하고 오도된 정보 생산의 위험성을 줄이고, 개인의 사생활을 크게 위협하지 않고도 정보업을 영위할 수 있는 중요한 기반이기도 하다. 또한 이것이 정보화, 세계화 시대 '세계경제전쟁' 속에서 미국의 국가경쟁력의 중요한 원천이기도 하다.

현재 운영되는 정보공개법에서의 공개정보의 범위를 더욱 확대하여 정부에 의해 생산된 공신력 있는 정보를 가능한 한 다량으로 공공재로서 사회에 공개, 환원하고 이러한 바탕 위에서 '정보분석사'의 성격을 지닌 양질의 information broker들이 시장에서 자유롭게 경쟁할 수 있도록 시장의 투명성을 관리해 준다면 사회적 혼란을 야기하고, 사생활을 침해하는 사설정보지 문제의 상당부분을 발전적으로 해결할 수 있을 것이다.

이는 기본적으로 '음성화'된 사설정보업을 '양성화'하기 위한 선결과제이기도 하며, 음성화된 사설정보업을 법규제와 처벌 일변도로 단속한다는 것은 그 소요비용에 대비한 예상 효과는 매우 낮다. 오히려 양성화시켜 예상되는 사회적 혼란과 폐해를 줄일 수 있는 거시적 접근(macro-approach)가 고려되어야 할 시점이며, 이를 위한 구체적 접근은 정부의 정보공개법의 정비와 확대실시가 요구된다.

신뢰할 수 있는, 양질의 다양한 공공정보들이 제한적으로 유통될 때 상업적 목적의 정보수집은 많은 경우 사설정보업체에 의존하게 된다. 따라서 사회구성원들이 신뢰할 수 있는 양질의 정보를 생산하기 위한 산학정의 협력이 요구된다

---

140) Right to Financial Privacy Act, PL 95-630.

VI-3. 산.학.정 (産.學.政) 공동체제

전통적으로 국가의 핵심적 영역으로 존재하였던 국가의 정보생산과 분석종합의 작업에 민간을 참여시킨다는 것은 쉽게 사회적 공감대를 형성하기 어려울지도 모르지만 미래사회학자 앨빈 토플러(Alvin Toffler)가 그의 저서 권력이동(Power shift)에서 지적한 바와 같이 '정보의 민간화는 점증하는 세계적 추세' 임은 아무도 부인하기 어렵다.[141]

우리는 모든 것을 알아야만 하는 시대로 진입하고 있다. 그러나 현실적으로 국가정보력이 그 모든 영역을 관장한다는 것은 미국과 일본도 한계를 절감하듯이 한국 역시 뚜렷한 한계를 가질 수밖에 없다.

세계화 시대는 흔히 말하는 '산동반도의 나비의 날개짓이 플로리다해안에 해일을 불러일으킨다' 는 '나비효과(butterfly effect)'이 현실화 되는 시대로 이해된다. 실제로 전 미국 국무부 차관보이자 저명한 국제정치학자인 조셉 나이(Joseph Nye)는 냉전붕괴 이후 미국이 아프리카 동부 소말리아와 같은 변방국가에 대한 관심을 줄여나갔으나, 곧 소말리아의 예기치 못한 사태가 미국외교 전체를 혼돈으로 몰아넣은 경험을 통하여 세계화 시대의 전방위적 정보의 수집과 분석의 중요성을 강조한다.[142]

한국 역시 냉전의 종식과 더불어 미국일변도의 정보의존에서 탈피하여 전방위적 정보수집과 분석을 축적해야할 시점에 이르고 있으며, 이는 국가차원에서만 담당할 수 있는 단계를 지나고 있다. 이제 국가정보는 모든 종류의 예상가능한 '위협' 과 '기회' 를 파악하기 위하여 전지구적, 전영역에 걸쳐 이루어져야 한다. 그러나 미국이나 다른 여타 우리와 유사한 환경에 놓인 어떤 국가도 그러한 능력을 보유하지는 못하고 있는 실정이다.

전 미국 국무부 차관보였던 로버트 키밋(Robert Kimmit)은 '국가정보력은 모든 주제에 있어 보다 두텁고, 훨씬 더 광범위하고, 훨씬 깊이있게 이루어져야 한다고 말한다.[143] 그리고 이러한 능력은 현재 한국정부를 포함하여

---

141) Alvin Toffler, *Power Shift*
142) Joseph Nye, 'The Decline of America's Soft Power' in *Foreign Affairs* May/June 2004
143) Foreign Intelligence Surveillance Act of 1978, 50 USC 1801.

대부분의 국가정보능력만으로는 불가능한 상황에 도달하고 있는 것이 현실이다.

이러한 '필요정보'의 폭발적 증가와 그 수집과 가공, 생산능력의 '한계'라는 불균형 상태는 비단 안보분야 뿐만 아니라 경제, 정치, 문화, 과학등 전방위에 걸쳐 발생하고 있다.

정보수요의 폭발적 증가와 그에 미치지 못하는 국가의 독점적 정보생산 능력의 한계에 대한 돌파구로서 오늘날 정부와 산업계, 그리고 학계의 정보공유와 협조적 관계 속에서의 생산은 뚜렷한 시대적 흐름으로 자리 잡고 있다.

1994년 클린턴 전 미국 대통령은 대통령령 23호(presidential decision directives 23)를 발동하여 미국기업들이 국가정보와 국방부의 안보관련분야에 긴밀하게 협력할 수 있는 길을 열었다.[144)]

정보기술의 발달은 정보수집 능력은 과거에 비해 현저히 향상되었으나, 불확실성(uncertainty)의 증대로 말미암아 우리가 무엇을 원하고 있으며, 우리에게 무엇이 필요한지를 파악하는 데 오히려 어려움을 겪고 있다. 다시 말하면 방법론(methodology)는 발달하였으나 존재론(ontology)은 오히려 약화되고 있는 것이 현실이다.

한국현대사는 한국전쟁 이후 안보정보에 있어서는 북한의 정세에 대해 거의 전적으로 미국의 정보에 단일의존성을 보여 왔고, 경제정보 역시 미국시장 중심으로 구성되어 왔으나, 세계화 시대를 맞이하면서 안보정보는 중국과 북방까지 확장되고 있으며, 경제 정보 역시 미국중심으로는 그 한계를 노정할 수밖에 없다.

산학정 공동 정보협력은 그러나 언론인, 종교인, 그리고 단순 자료처리 학자들은 엄격하게 배제시키는 원칙을 고수하는 가운데, 최근 정보업무는 산업계와 학술기관을 폭넓게 활용하고 있다. 또한 각국 정보기관들은 전직 정보업

144)Testimony of Robert Corn-Revere, before the Subcommittee on the Constitution of the Committee on the Judiciary, United States House of Representatives, The Fourth Amendment and the Internet, April 6, 2000.

무 종사자들 역시 그들의 전문영역에 필요성이 발생할 경우 한시적으로 재고용하는 프로그램의 운영을 통하여 정보수집과 생산의 효율성을 제고하고 있다.

현재 미국의 산학정 협력체제를 통하여 미국의 정보업무능력은 현저히 증가한 것으로 평가되고 있다. 그러나 여전히 민간업체와 학술기관들이 미국의 정보업무능력 제고에 기여할 수 있는 가능성은 여전히 무궁무진하다. 특히 민간부문의 효율성과 창의성이 미국정보능력 향상에 기여한 바는 막대하다.[145]

많은 외부인사들의 정보집단에의 참여는 정보업무의 유연성과 신뢰성을 제고시켜 줄 것이며, 정부와 시민사회의 관계개선과 상호신뢰 구축에도 일조를 할 수 있을 것이다.

폭발적으로 증대된 공개정보와 함께 사회에서 정보의 분배를 숙지하는 외부인사들은 정보집단이 제대로 된 연구방향을 설정하고 공공에게 접근가능한 정보를 보다 효율적으로 관리할 수 있는 능력을 배양하게 될 것이다.

이를 통하여 한국의 정보집단(information community)의 정보생산, 가공능력을 획기적으로 제고시킬 수 있으며, 이곳에서 수집, 가공되거나 분석 생산된 다양하고 양질의 신뢰할 수 잇는 정보들이 상기한 개선된 '정보공개법' 을 통하여 민간에 제공된다면 사설정보에 대한 수요와 그 폐해를 획기적으로 개선할 수 있을 것으로 기대된다.

이를 위하여는 학술기관과 사기업이 정보집단(information community)에 참여할 경우 준수하여 할 규범화된 법률제정이 필요하다. 정보업무의 사안마다 다른 기준이 적용된다면 이는 정보생산 업무 비용의 증가로 이어지게 될 것이다.
사설정보기관과 국가정보기관의 정보생산과정에서의 공동참여가 이상적이다.

사영역과 공영역이 공동참여하는 정보기관은 무책임하고, 사회적책임을 방기하고 오로지 사적, 경제적 이익만을 추구하는 사설정보기관 정보의 '세

145)Testimony of Robert Corn-Revere, before the Subcommittee on the Constitution of the Committee on the Judiciary, United States House of Representatives,

척’ 과정을 거칠 수 있게 할 것이다.

또한 정보의 질의 향상을 위하여 학술기관과 사설연구기관의 참여를 용이하게 한다. 이러한 공동정보기관은 ‘회원제’를 통하여 기업, 조직, 그리고 일반개인들에게 정보의 공유대를 확대시킴으로써 정보의 왜곡된 유통과 정보격차(information-divided)를 완화시켜주며, 왜곡되거나 신뢰성이 낮은 사설정보에의 유혹과 그 수요를 원천적으로 봉쇄하게 할 것이다. 그리고 민간사업자들에게 경제적으로 효율적인 정보를 제공함으로써 기업경쟁력을 제고시킬 수 있을 것이다.

산학정의 협력은 어느 경우이든, 가장 중요한 부분은 이러한 형태의 정보생산이 양질의, 신뢰도 높은, 다량의 정보를 국민들에게 공공재로서 제공되어 사회의 정보격차(information divided)를 완화하고, 사설정보의 폐해를 완화해 줄 수 있는 방향에서 실시되어야 하며, 또한 이러한 방식이 한국사회의 문화와 충돌하지 않는 범위 내에서 실현되어야 한다는 점이다.

서구사회에 비하여 한국사회는 아직 민간과 정부 영역의 ‘융합’이 자유롭지 못하고 명확한 선을 긋고 있는 실정이다. 세계화와 국가 영역의 축소라는 전세계적인 추세 속에서 한국사회의 민간부문과 정부부문의 일부 융합 현상이 발생하고 있으므로 머지않은 장래에 이러한 시도는 실현될 수 있을 것으로 보인다.

위의 사례연구가 보여주듯이, 사생활권 보호와 정보업무의 민간화 문제는 사생활권 보호가 강화되면 될수록 정부가 수집할 수 있는 가본정보 수집 능력은 제한적으로 운영될 수밖에 없으며, 그 정보의 분석과 가공, 생산을 통한 공공재로서의 정보생산능력도 저하되게 된다.

산학정 협력 정보공동체 구축의 비용과 효과 분석

국가정보에 외부인사의 접근을 허용할 경우 국가기밀 유지의 어려움이 뒤따른다. 또한 외부전문가들은 ‘국가목적성’에 대한 인식이 내부인사와는 차이가 발생할 수밖에 없어, 정보의 경제적 유용성과 국가목적 사이에서 쉽게 타협점을 찾는 경향이 발생할 수 있다.

외부학자들이 정보생산에 밀접하게 관련될 경우 정보업무의 효율성이 떨어질 수 있다. 특히 군사분야에서 지나치게 이상적이거나 논리적으로 접근하는 것이 외부학자들의 기본적 속성이기 때문이다.

미국의 대외정부업무을 담당하였던 조셉 나이 전 국무부 차관은 학자들의 속성을 자신이 친구로부터 받은 한 편지를 통해 소개한다. "나는 30-40 페이지에 달하는 수많은 주석이 달린 페이퍼를 받았는데, 학자들은 그것들이 얼마나 쓸데없는 것인지 알지 못한다." 일반적으로 학자들은 시간에 구애를 받지 않는 반면, 정보업무 담당자들은 정보가 필요한 제 시간에 정보생산을 마쳐야만 한다.[146]

민간전문가를 정보업무에 참여시키는 것은 그 비용절감 효과를 기대할 수 있다. 민간정보회사들은 정부와 계약을 성사시키기 위한 경쟁적 입찰과정을 통하여 비용을 최소화하기 위한 온갖 노력을 할 수밖에 없다.

민간부문과의 협력은 또한 내부에서 쉽게 고용하기 힘든 외부의 전문가의 협력을 이끌어 내는 장점이 있다. 특히나 관료주의적 타성에 물들지 않은 새로운 시각과 접근법, 그리고 창의성을 이들로부터 수급받을 수 있다.
많은 외부의 전문학자들이 정보의 생산과 분석에 참여함으로써, 사회의 이해와 동의를 용이하게 하며, 정보업무에 대한 중립적인 평가를 얻을 수 있다. 많은 민간과 학술기관의 전문가들은 정보업무에 대한 협력을 자신들이 국가를 위한 봉사의 기회로 인식, 적극적으로 참여하는 경향이 있다.

또한 정부는 정보생산에 공동참여한 학술기관과 기업에게 그 비용을 지불하는 방식이 아니라 연구에 공동참여함으로써 기업목적성 연구와 학술적 연구 자체에서 성과물에 대한 성취를 유도할 수 있어야, 정보의 '공공성'을 담보할 수 있다.

국가정보에 대한 민간부문의 첩보행위에 대한 의혹과 우려는 존재하지만, 대학교수들이 정부정보를 취급하고 분석, 종합하는 것은 학자들이 정부가 어떻게 운영되고 있는지 이해하고 큰 틀 속에서 협조하는 데 있어서 매우 긴요한 기회를 제공하기도 한다.

---

146) Testimony of Joseph Nye, Hearing of the Commission on the Roles and Capabilities of the United States Intelligence Community (jan. 19, 1996, Washington, Dirsen Senate Office Building)

만약 학자들이 자문역으로 참여한다면, 그들은 비밀정보에 접근하게 된다. 학자들은 그 정보를 그들의 강의와 저술에 사용할 수는 없겠지만 자신의 전문분야에 있어서 새로운 지적자극과 통찰력을 제공받게 되기도 한다.

이보다 더욱 중요한 것은 산업계와 학술계가 국가정보생산에 공동참여 한다면, 정부는 국민의 세금으로 이루어지는 정보생산을 정부만의 목적을 위하거나, 혹은 특정집단만을 위하여 실행할 여지가 줄어들게 되고, 사회에 환원될 '공공재' 적 성격의 정보에 보다 주력하게 될 것이다. 이는 정보업무의 투명성과 공공성을 획기적으로 증대시킬 수 있다.

동서냉전의 해체와 세계화시대에 과거 국가의 정보업무에 할애되었던 정부예산은 급격하게 축소되고 있는 것이 현실이며 우리사회도 남북간의 긴장완화와 민간부분의 역할이 강화되면서 국가안보와 경제정보에 대한 국가정보원 중심의 정보업무에 대한 예산이 증대되지 못하고 경제와 활동영역의 확장에 비해서는 오히려 퇴조하고 있는 추세이다.

방대한 예산의 지원이 담보되지 않는 한 국가차원의 정보수집과 생산, 분석은 정보필요성의 확대에 발맞추기 어려운 것이 현실이다. 따라서 이미 미국과 일본의 예에서 보듯이 정보의 생산과 수집, 분석은 국가와 민간, 그리고 학문기관에서 공조하여 이루어지는 것이 현실적인 대안이 될 수 있다.

막대한 예산 투입이 요구되는 국가정보의 독점이, 예산상의 뒷받침이 이루어지지 못할 때에는 그 양과 질의 급격한 저하를 야기할 수밖에 없다. 이미 우리나라에 있어서 일부대기업의 해외정보망은 그들이 집중하는 특정분야에 있어 오히려 국가정보망 수준에 접근했거나, 오히려 능가하는 경우도 있으며, 국내연구기관은 물론 해외의 다양한 연구기관에 종사하는 학자들 역시 다양한 국제학술회의와 전공 유관분야의 해외 정부관리, 전문가들과의 교류를 통하여 정부정보기관이 쉽게 수집하고 분석하기 어려운 정보에 대한 접근성과 그 정보의 해석과 분석에 있어 국가기관의 정보력을 보완할 수 있는 입지를 구축하고 있다.

이들 자원을 국가정보력으로 종합하여 활용하는 시스템 구축이 시급하고 현실적이다.

산학정 협동체제를 통하여 공공성을 강화하여 생산된 정보는 정보공개법을 확대하여 국가기밀이 아닌 일반정보는 가능한 한 공개정보(unclassified information)으로 해제하여 공공재(public good)로서 환원시켜야 그 의미를 완성할 수 있다. 아무리 공공의 목적에 부합되는 정보라 해도 일반에 공개되지 않는다면 무의미하다.

VI-4. 정부 정보공개의 확대

정보공개법이란 공공 목적상 필요성이 인정될 경우 국민이면 누구나 국가기관이 보유하고 있는 정보를 열람할 수 있게 하는 것이며, 행정기관의 게시의무를 명시한 것이며 국민의 「알 권리」를 보호하는 제도이다.

즉 공공기관이 직무상 작성 또는 취득하여 관리하고 있는 정보를 수요자인 국민의 청구에 의하여 열람 · 사본 · 복제 등의 형태로 청구인에게 공개하거나 공공기관이 자발적으로 또는 법령 등의 규정에 의하여 의무적으로 보유하고 있는 정보를 배포 또는 공 표 등의 형태로 제공하는 제도를 말한다. 그리고 여기서 전자를 '청보공개' 라 한다면, 후자는 '정보제공' 이라 할 수 있다.

이러한 정보공개법 제도는 선진국에서는 이미 시행하고 있는 제도로 미국의 경우 1966년에 정보공개법이 입안되었고 1974년에는 워터게이트 사건으로 보다 확장된 정보공개법 개정안이 입법되었다.[147] 우리나라의 경우 전통적으로 정보접근, 유포, 인쇄 등에 대한 국가기관의 강력한 통제로 제도의 정착이 어려웠으나, 1998년에 비로소 정보공개법이 제정되고, 공개정보를 더욱 확대하려는 움직임이 계속되고 있다.

일본의 사설정보업체의 범람은 기본적으로 한국사회와 마찬가지로 일본국민들 역시 정부의 투명성과 공정성에 대한 신뢰도가 낮기 때문에 정부에 의한 개인정보의 수집에 부정적인 태도를 보이는 것으로 나타난다,

이러한 사회는 정부의 개인정보의 수집과 처리에 있어 엄격한 통제장치를 요구하여 미국의 경우처럼 그러한 엄격하게 요구되는 제한을 피해 능동적으

147) Administrative Office of the US Courts, 1999 Wiretap Report.
<http://www.epic.org/privacy/wiretap/stats/1999-report/default.html>.

로 민간부문에 정보수집의 권한 상당부분을 이양하여 정보생산을 하는 '편법'을 동원하게 되기도 한다. 이는 정부의 공적 정보생산력의 저하로 나타나고, 다시 사설정보업의 성행으로 이어진다.

따라서 사설정보 범람에 따르는 사회적 비용과 개인의 사생활 침해를 근원적으로 방지하기 위해서는 '단속'과 규제라는 부정적 접근(negative system)이 아니라 긍정적 접근(positive system)이 바람직하다.

'긍정적 접근'의 요체는 일반시민들이 최소한 정부에 의한 개인적 신상정보 파악에 대해서는 그 필요성을 인식하고, 그 정보수집의 공공의 안녕과 사회통합의 본래 목적 이외에 전용되지 않는다는 신뢰가 선결과제이다. 신뢰구축이라는 선결과제가 선행되어야만 정부의 개인정보 수집과 저장에 대하여 협조관계를 구축할 수 있다.

또한 수집된 국가가 수집한 정보를 정보공개법을 통하여 사회에 공공재로서 환원하여 기본적 정보욕구를 해소시켜 줌으로써, 사설정보에 대한 수요와 그 의존을 낮출 수 있다.

최근 정보사회에로의 급속한 진입으로 인하여 우리사회는 많은 변화를 겪고 있다. 이와 함께 시민들의 민주정치에 대한 참여의식의 향상과 정보사회에 있어서 정보의 중요성에 대한 인식은 최근 들어 두드러지게 나타나고 있다. 특히 정치, 경제 사회분야 전반에 걸쳐서 만연하고 있는 부조리는 정부 행정의 투명성에 대한 시민들의 욕구를 증대시켜 놓았다. 그 결과 정부 공공기관이 생산하여 보유하고 있는 정보에 대한 공개의 필요성이 제기되어 왔다. 한편, 90년대 들어 새롭게 대두되고 있는 세계적인 흐름은 방송과 통신의 급격한 융합현상이다. 이러한 새로운 국제적 조류는 각국의 언론환경을 근본적으로 바꾸어 놓고 있다. 다매체 다채널시대의 방송은 시민들의 정보욕구를 부채질할 뿐만 아니라 시민들 삶의 양식조차 서서히 변화시키고 있다.

따라서 사설정보 범람을 치유하기 위한 방안으로서의 정보공개법의 정비와 확대실시는 두가지 관점에서 매우 긴요하다.

첫째, 국민의 알 권리와 정보공개법, 그리고 사설정보시장은 상호 밀접한 관계에 있다. 정부 공공기관이 보유하고 있는 정보의 공개는 국민의 알 권리를 충족시키는데 필수 불가결한 요소이다.

정부의 정보공개는 민주사회의 시민들을 계몽하고 그들로 하여금 국가운영에 관한 올바른 의견을 형성하도록 하고 나아가 이를 바탕으로 민주정치과정에 참여할 수 있도록 하는 밑거름이 되며 국정과 사회적 투명성을 제고하여 정보화 시대의 필수적인 요소인 사회적 자본(social capital)으로서의 사회적 신뢰(social trust)를 확보하는 필수적인 조치이다.

사례연구에서도 지적된 바와 같이, 정부와 사회에 대한 신뢰도가 낮은 사회일수록 '사설정보'의 파급력이 통제되지 못한다. 따라서 사설정보 성장의 기본 토양인 정부와 사회에 대한 불신을 제거하기 위한 사회적 투명성 제고의 차원에서 정보 공개법은 접근되어야 한다.

정보공개제도는 크게 두가지로 나눌 수 있다. 하나는 적극적으로 모든 정보에 대한 공개를 원칙으로 하고 국가기밀과 같은 비공개 정보를 예외조항으로 처리하는 제도이다(positive system). 이러한 제도를 채택하고 있는 대표적인 나라는 미국이다. 다른 하나는 소극적인 정책으로서 모든 정보에 대한 비공개를 원칙으로 하고 공개 가능한 정보를 선별적으로 허용하는 공개제도이다(negative system). 일본이 심의하고 있는 정보공개제도가 그 대표적인 보기라고 할 수 있다.

.

세계에서 가장 먼저 국민의 알 권리와 정보공개에 관한 법을 입법화한 나라는 스웨덴이다. 그리고 이러한 정보공개에의 권리를 헌법에 명시한 드물게 보는 나라가 스웨덴이다. 일찍이 1766년에 정보공개법을 마련하여 정부 행정의 투명성을 높이고 정부에 대한 국민의 신뢰를 향상시킴으로서 '정보'를 둘러싼 사회 각 세력간의 충돌과 갈등을 최소화하는 가운데 모범적인 민주복지국가 건설에 성공한 사례로 꼽힌다.[148]

148) International Helsinki Federation for Human Rights, Human Rights in the OSCE Region: the Balkans, the Caucasus, Europe, Central Asia and North America, Report 2000.

세계에서 가장 모범적인 정보공개법을 마련한 나라는 미국이다. 미국은 1966년에 정보공개법을 마련하여 정부부처 기관들이 보유하고 있는 정보를 외국인을 포함한 모든 사람들이 공개 청구할 수 있도록 규정하고 있다. 뿐만 아니라 1996년 10월의 법개정을 통하여 정보사회를 대비한 가장 선진적인 정보공개법을 확립하고 있다.[149] 미국은 정부 공공기관이 소위 '전자정보관(electronic reading room)'을 의무적으로 마련하도록 규정하고 있다. 이러한 전자정보관에 1996년 11월 1일 이후에 생산하는 공개 가능한 정보를 비치하여 시민들이 언제든지 열람할 수 있도록 의무화하고 있다.[150] 이러한 조치는 사회적인 정보기반(information infrastructure)을 바탕으로 정보사회를 앞당기는데 이바지할 것으로 보인다.

이와 같은 정보공개법이 미국이 정보의 자유를 훼손하지 않으면서도 사설정보업에 의한 사회경제적 피해를 최소화시킬 수 있는 기반을 제공한 것으로 평가된다.

우리나라는 1998년 12월 31일 국정사상 처음으로 정보공개법을 제정하였다. '공공기관의 정보공개에 관한 법률'은 청주시가 1992년 처음으로 이 땅에 정보공개조례를 마련한 이래 4년만에 중앙 정부 차원에서 결실을 맺은 것이다. 이 법은 선진국의 정보공개제도를 참고로 하여 그간 지적되어 왔던 정보공개법 관련 문제점들을 많이 극복하고 있다.

여러 가지 장점에도 불구하고 이 정보공개법은 몇가지 문제점 또한 안고 있다. 우선, 행정비밀의 분류는 보안업무규정과 그 시행세칙에 의거하여 I급 비밀, II급 비밀, III급 비밀 및 대외비의 4종류 되어 있다. 이 행정문서의 분류에 있어서 문제가 되는 것은 그 판정기준이 모호하다는 것이다. 따라서 일단 비밀로 분류해놓고 보자는 행정편의주의 행태가 발생되면 많은 행정문서가 대외비로 분류될 가능성이 높다.

아울러 정부 공문서의 공개 필요성에 대한 공무원들의 인식을 높일 필요가

---

149) Compilation of State and Federal Privacy Laws (1997 ed.), by Robert Ellis Smith and Privacy Journal..<

150)Drivers Privacy Protection Act, PL 103-322, 1994. <http://www.epic.org/privacy/laws/drivers_privacy_bill.html>.

있다. 정보공개는 정부행정의 투명성을 높여 정부에 대한 국민의 신뢰를 높이고 민주국가 발전에 이바지한다는 인식을 시켜줄 필요가 있다.

우리나라 정보공개법은 또한 정보사회에 대비하고 앞당기는데 미흡한 점이 있다. 정보공개법은 컴퓨터 통신을 통하여 정보청구를 할 수 있는 길을 열어 놓은 것은 좋은 일이다 (공공기관의 정보공개에 관한 법률 시행령 제4조). 그러나 공개방법(공공기관의 정보공개에 관한 법률 시행령 제14조)을 포함하여 컴퓨터나 인터넷을 통한 정보공개청구를 뒷받침할 만한 구체적인 조치가 미흡하다.

따라서 우리나라 정보공개법의 문제점을 극복하고 정보사회에 걸맞은 정보공개법을 마련하기 위해서는 몇가지 개선방안을 실천해야 할 것이다. 우선 행정비밀 분류체계를 구체화하고 행정편의주의에 따른 행정문서 분류행위를 탈피하도록 노력해야 한다. 정부 공문서의 공개 필요성에 대한 공무원들의 인식전환을 위하여 민주사회에 있어서 정보공개의 필요성을 교육할 필요가 있다. 아울러 국가 정보기반을 바탕으로 한 정보공개제도의 활성화를 위하여 컴퓨터 통신이나 인터넷을 통한 정보공개청구 및 정보제공이 신속히 이루어질 수 있도록 조치해야 할 것이다. 이렇게 될 때 정보사회는 앞당겨질 수 있다.

현재의 정보공개법을 공공정보의 확대 공급을 통한 사설정보 수요감소의 결과를 도출하기 위해서는 다음과 같은 보완이 이루어져야 할 것으로 판단된다.

첫째, 정보사회를 앞당기고 이에 대비하기 위해서는 우리사회의 정보기반 구축과 정보화 진척 정도에 따라 정보공개법을 개정할 필요가 있다. 이를테면, 미국과 같은 '전자정보관(electronic reading room)'의 설립을 고려할 필요성이 있다. 이는 시민들이 정보접근권(right of access)을 행사하여 손쉽고 빠르게 언제 어디에서나 정부 공공기관의 정보를 이용할 수 있도록 함으로써, 사적영역에서의 정보 브로커(information broker)들이 공개되고, 검증된 정보를 통하여 개인과 집단이 필요로하는 1차정보의 풀(raw information pool)을 풍부하게 해줄 것이다. 이러한 정보의 유통구조가 구축된다면 검증되지 못한 사설정보의 범람과 그에 따른 사회적 파장도 축소시키는 것이 가

능하다.

둘째, 정보공개심의회 위원선출방법에 대하여 재검토가 필요하다. '공공기관의 정보공개에 관한 법률' 제12조 제4항은 '심의회의 위원장 및 위원은 공공기관의 장이 소속 공무원 또는 임 · 직원 중에서 지명하되, 필요한 경우에는 공무원이나 임 · 직원이었던 자 또는 외부 전문가를 위촉할 수 있다'라고 규정하고 있다. 행정비밀주의와 편의주의, 관료주의에 익숙해온 정부 공공기관의 전통적인 특성을 생각한다면, 심의회의 독립성과 심의의 중립성은 무엇보다도 중요하다고 하겠다. '공개정보' 와 '비공개정보' 를 분류하고 선정결정하는 주체는 정부만이 아니라 그 정보를 필요로 하는 소비자인 '민간' 과 '시민' 들이 되어야하며, 이들의 위원회 참여는 정보공개의 실효성 확보를 위하여 필수적인 조치이다.

셋째, 정보공개심의위원의 임기는 한시적으로 하는 것이 보다 바람직할 것이다. 현행 정보공개법 시행령에 따르면, 정보공개심의회 위원의 임기는 그 직위에 재직하는 기간으로 한다. 다만 공무원이나 임 · 직원이었던 자 또는 외부 전문가인 위원의 임기는 2년으로 한다(공공기관의 정보공개에 관한 법률 제12조 제5항). 이 규정은 공무원이 재직기간 중 습득한 지식과 경험을 바탕으로 정보공개심의를 할 수 있다는 점에서 긍정적일 수 있다. 그러나 다른 한편으로는 재직 기간 내내 심의위원으로 활동한다는 것은 정보공개심의에 있어서 타성과 관행에 젖어 급변하는 정보사회에 있어서의 정보공개심의에 알맞지 않을 수도 있다. 또한 민간부문의 다양한 정보수요를 대변할 수 있는 다분야, 다직종, 다계층의 '시민' 참여 기회의 확충을 위해서 순환방식(rotation system)의 도입이 바람직하다.

VI-5. 민영화와 외부제작(privatization and outsourcing)

정보에 대한 국가차원의 관리와 통제는 필수불가결한 부분이 있지만 정보의 외주 제작이 더욱 효율적일 수 있다. 더욱이, 정부는 다양한 정보의 생산을 다양한 정보제작 업체에 발주함으로써 업체들이 제작, 생산한 정보를 비교검증하여 보다 신뢰성있는 정보를 선택하여 유통할 수 있다.

VI-6. 자율규제에 의한 프라이버시 보호

1. 정보화 사회에서의 개인의 주요 권리

정보화 사회의 발달로 정보민주주의 혹은 전자민주주의의 구현을 통해 참여민주주의에 대한 긍정적 기대를 가질 수 있게 되었다. 그러나 다른 한편에서는 정보의 무분별한 유포로 인한 부작용이나 개인의 정보가 보호되지 못하게 되는 해악이 사회적 문제로 제기되고 있으며, 이 문제가 현재 개인의 프라이버시권에서 중요한 이슈가 되었다.

프라이버시권에 대한 개념은 오래전부터 있었지만 정보화 사회로 진입한 현대에서는 '개인 정보에 대한 통제권'이라는 보다 적극적인 개념으로 바뀌고 있다. 이 권리의 개념은 미국에서부터 발전해 온 것이다. 즉 정보화 사회 진전에 따라 사생활 보호에 대한 권리가 소극적으로 "사생활의 평온을 침해받지 아니하고 사생활의 비밀을 함부로 공개당하지 아니할 권리"에서 나아가 적극적으로 "자신에 관한 정보를 관리, 통제할 수 있는 권리"를 포함하는 의미로 이해되고 있다[1]. 이는 프라이버시를 침해받지 않을 자유권적 성격뿐만 아니라, 기록된 개인정보가 부정확할 때 당하는 부당함을 사전에 막기 위해 자신의 정보를 확인하고 정정할 수 있는 청구권적 성격도 갖게 된다는 의미이다[2].

이처럼 개인의 프라이버시권 개념이 적극적으로 바뀌는 경향은 커뮤니케이션 기술의 발달로 쌍방적 의사소통이 가능해졌기 때문이다. 이제 더 이상 정보수용자들은 정부에게만 정보 관리·가공을 맡길 필요가 없다. 수용자들 스스로가 통신상에서 다른 이들과 서로간의 정보를 나눔으로써 정보 자체를 보다 확장시킬 수 있게 된 것이다. 또 다른 이유는 정보를 공유하고 확장하는 과정에서 개인신상정보 유출 경로가 무한정 확장되고 있다는 점이다. 개인들이 다양한 정보를 적극적으로 수집, 활용하고 생산할 수 있게 된 반면, 자신들의 고유한 신상정보를 어떤 용도로, 언제 어떻게 공개되는지도 모른채, 그리고 어떻게 남용될지도 모른채 내주는 경우가 많아졌다. 이러한 정보유출로 겪는 개인적 피해는 사회 문제로 대두 되고 있으며, 개인 스스로가 자신의 개인 정보를 관리하고 통제하면서 자신의 권리를 적극적으로 주장해야 한다.

한국의 경우, 개인정보보호법은 국가 기관에 의한 침해 사례에 국한되어 있다. 그러나 개인 정보 보호를 둘러싼 문제는 국가 기관에 국한되는 것뿐만 아니라 민간 기업에 의한 침해도 중요하게 다루어져야 한다. 왜냐하면 정보 수집에 필요한 기술이 발달함에 따라 국가 기관 이외에 학교, 병원, 은행, 흥신소 등의 사적 기관들도 개인 정보를 구축하게 되었고, 개인들은 여권, 신용카드 신청, 조세 감면 등 여러 인허가 신청시 자신들의 개인 정보를 등록할 수밖에 없기 때문이다. 이처럼 개인 정보가 유출될 수 있는 경로는 점점 많아지고 있다. 그러나 백서에서는 특히 개인 정보가 유출될 수 있는 경로 중 PC 통신을 통한 유출 사례에 집중하고자 한다. 또한 고전적 의미의 프라이버시권을 모두 다루기보다는 현대 사생활권의 주요 문제인 '개인정보 보호'에 초점을 두고자 한다.

2. 한국의 개인정보보호 수준

1) 한국의 사생활의 비밀과 자유

정부는 1987년 헌법 제 17조에서 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다"라는 명문의 규정을 둠으로서 '개인의 사생활 보호'에 대한 권리를 헌법 이념화했다. 그리고 사생활의 비밀과 자유를 보장하려는 헌법이념의 구체화법으로서 〈공공기관의 개인정보 보호에 관한 법률〉과 〈신용정보의 이용과 보호에 관한 법률〉 등이 제정되어 있다. 그 이전에는 사생활 보호 문제의 경우, 형법상 명예훼손이나 민법상 불법행위 책임 문제로만 이해되어 왔다.

미국의 경우는 정보화사회 진전에 발맞춰 1965년에 비로소 미국연방대법원 판례를 통해 수정헌법 제 14조의 보호를 받을 권리로 인정되었다. 우리나라는 거의 20년 뒤인 87년 헌법에 명문화가 이루어졌지만 아직 그에 대한 구체적 법제화가 미비한 상황이며, 이에 정보화로 인한 개인들의 피해에 대처할 방안이 거의 없는 실정이다.

개인정보보호에 관한 법률은 기본권으로서의 사생활보호에 해당하는 것으로 집회·결사의 자유와 같은 집단적 성격의 기본권과 구별되는 개념이다. 넓은 의미의 사생활보호에 관한 기본권은 주거의 자유(제16조), 사생활의 비밀과 자유(제17조), 통신의 자유(제18조)이며, 이 중 사생활의 비밀과 자유는 가

장 최근에 헌법적 가치를 갖는 기본권이다. 주거의 자유가 고전적인 기본권의 개념이라면, 오늘날과 같은 정보사회에서의 사생활 보호권은 일반적으로 사생활의 비밀과 자유를 지칭한다.

사실 사생활권에 대한 개념과 범위는 어느 나라도 정확하게 정의하거나 한계지우지 못하고 있다. 무엇보다 '사생활'의 범위를 정하지 못하고 있기 때문이다. 또한 현재와 같은 정보화 사회에서는 정보를 수집, 보유, 이용하는 것이 일반적으로 일상화되고 필수불가결하게 됨에 따라 정보공개권 혹은 알권리의 개념과 상충되는 경우도 수시로 발생하기 때문이다.

그러므로 법 내용을 갖고 정확한 범위를 따져 보는 것은 무의미하다. 법제화된 내용이 실제 생활에서 개인의 사생활을 얼마나 효율적으로 보호하고 있는지는 직접적인 사례를 통해 살펴볼 수 밖에 없다. 그러나 우리나라의 경우는 충분한 판례가 축적되어 있지 않아서 법을 적용하는데 큰 애로점이 있다. 더구나 해당 문제를 해결할 수 있는 실정법이 미비한 실정이다. 이미 PC통신 등 뉴미디어에서 프라이버시권 침해에 대한 여러 문제가 제기됨에도 불구하고 적절한 법조항이 마련되어 있지 않은 상태이고, 일반 이용자들이 그나마 권리를 주장할 수 있는 것은 헌법에 명시된 '이념' 조항일 뿐이며, 해당 서비스 업체의 이용약관에 기댈 수밖에 없다.

이렇게 법적 정의가 불문명해서 문제가 되는 또 다른 경우가 있다. 대부분의 법은 여러 복합적인 상황에서 적절하게 적용되기 위한 제한 조건들을 달고 있다. 우리나라의 '사생활의 비밀과 자유' 역시 헌법 제 37조 제 2항에 따라 국가안전보장·질서유지·공공복리를 위해 필요한 경우에 한해 법률로 제한할 수 있다. '사생활의 비밀과 자유'라는 헌법 이념이 구체화된 '개인정보보호법' 역시 그러한 조건에서 제한될 수 있다. 그러나 적용 기준이 특정 권력에 의해 자의적으로 해석될 여지가 많다면 충분히 문제가 제기될 수 있다. 미국의 경우, 법문항의 대상 범위가 보다 포괄적이면서 구체적으로 명시하고 있기도 하지만 무엇보다 풍부한 판례가 법 적용의 객관성을 뒷받침해준다.

반면 우리나라는 법 집행자들에게 'PC통신'이라는 커뮤니케이션 형태가 생소하다는 점, 법 문항 자체에 많은 제한점이 있다는 점, 역사적으로 '개인의 권리를 보호한다'는 개념이 희박하다는 점 등에서 여러 가지 문제들이 생겨난다. 비록 어떠한 경우에라도 사생활의 비밀과 자유의 본질적 내용은 제한

할 수 없다고 하지만 현실 문제를 '상징적 이념'만으로 해결할 수 없다. 특히 개인 권리의 주요 제한 이유인 '국가안전보장·질서유지·공공의 복리를 위한다'는 개념이 특정 기관에 의해 자의로 해석되는 여지가 많은 현실이라면 더더구나 정부 기관 혹은 특정 기관에 맡길 수만은 없다.

2. 프라이버시권의 의미 확대:소극적 개념에서 적극적 개념으로

이러한 법규정의 모호함이 사설정보업체에 의한 '무책임' 한 개인정보 접근을 용이하게 하고, 또 그에 대한 제재나 피해구제를 어렵게 한다. 따라서 정보화시대에 개인 사생활보호권을 강화하여 사설정보업의 폐해를 방지하기 위하여는 무엇보다도 '사생활' 과 '사생활 침해' 의 법개념을 명확히 하고, 그 구체적 처벌조항을 명료하게 하고 엄격한 집행이 이루어져야 하는 것이 선결과제이다.

현재, 외국의 사례를 살펴보면 유럽이 입법조치를 통해 프라이버시 보호문제를 다루는데 비해 미국에서는 원칙적으로 자율규제(self-regulation)를 통해 이 문제를 다루려고 하고 있다. 그러나 '자율규제' 방식은 바람직하기는 하지만 현실적으로 민간부문에 적용하는 데 어려움이 많아 미국의 경우도 FCC는 최근 전화회사들이 가입자들의 정보를 이용하여 다른 상품을 마케팅하기 위해서는 가입자의 동의를 얻어야 한다는 프라이버시 규정을 채택한 바 있다.

위에서 살펴본 바와 같이 현재 지식정보화 시대의 정보기술 발전 진행에 발맞추어 전세계적인 추세는 '입법' 을 통한 사생활 보호의 방향으로 나아가고 있다.

자율규제 쪽을 선호하는 나라에서는 프라이버시 보호를 위한 기술적 해결책 등에 대한 연구와 상품화가 진행되고 있다. 프라이버시 보호를 위한 기술적 해결책으로는 "Anonymiser" 등과 같은 것을 들 수 있는데 그 원리는 정보를 수집하려는 정보관리자와 정보주체 사이에 신뢰할 수 있는 제3자를 개입시키는 것이다. 이때 이 제3자(Trusted Third Party)는 정보주체의 실제정보를 알고 있으나 정보를 수집하려는 관리자는 정보주체의 정보를 직접 얻는 것이 아니라 제3자가 공급하는 익명의 정보를 얻게 됨으로써 정보주체를 보

호하는 역할을 하게 된다. 물론, 이 경우 신뢰할 수 있는 제3자의 책임문제가 새로이 대두된다.

우선적으로 해결해야 할 문제는 법률을 통해 명시적으로 프라이버시와 개인정보의 보호를 규정하고 있는 나라와 자율규제를 택하는 나라간의 개인정보의 흐름을 보장하는 방안을 강구하는 것이다.

VI-7. 사생활권과 공공성의 조화

외국사례에서 살펴본 바와 같이, 지식정보사회로 진입하면서 전통적인 사생활권 지상주의적 시각은 각국에서 현실여건의 변화로 상당부분 공공성과 조합점을 찾는 방향으로 조정되고 있다.

2001년 한백연구재단과 일본의 덴츠연구소가 한,중,일 3국 학자들을 대상으로 실시한 '사회신뢰도' 설문조사에서도 이러한 경향은 확인된다. 조사대상 167명중 50% 이상이 사생활권과 공공성 조화의 필요성에 공감하고 있는 반면, 70년대 이전 서구적 가치관인 사생활권 지상주의자는 가장 낮은 25%에 불과한 것으로 나타난다.[151]

이 결과는 위에서 살펴 본 유럽중심의 OECD 트렌드 조사와 큰 차이를 보이지 않는다.

사생활권 근본주의자 (약 25%).

이 그룹은 사생활 침해에 매우 민감하며, 사생활 정보 유출이 가능한 어떠한 정부의 프로그램에도 적극적인 반대의사를 밝히며, 정부에서 요구하는 어떠한 개인정보도 거부해야 한다고 믿으며 사생활 보호에 대한 정부의 강력한 법적, 제도적 장치를 요구한다. 이들 응답자는 사회와 정부에 대한 '신뢰' 설문에 극도의 불신감을 나타낸다.

실용적 사생활보호론자 (약 55%).

151) 한백연구재단, 덴츠연구소, 한중일 3국 사회의식 조사 보고 (2001, 미출판)

이 그룹은 사생활권의 보호와 사회적 목적 양쪽의 균형점을 추구한다. 따라서 정부에서 요구하는 사생활 정보가 사회적 목적달성과 사회전체를 위하여 필수불가결하다면 정부 프로그램에 협조할 의사를 가지고 있으나, 또한 사생활 침해가 최소화될 수 있는 제도적 장치 마련이 병행되어야 하고, 그 목적을 위하여 정부가 취할 수 있는 최선의 노력을 해야한다고 믿는다. 이 그룹은 사회와 정부에 대한 불신도가 중간에서 다소 높은 수준을 나타내는 응답자에 집중된다.

사생활권 보호 무관심층 (약 20%). 이 그룹은 사생활 논쟁 자체에 관심이 없다. 기본적으로 사생활 정보 보호를 위한 조치에 찬성을 하지만 기업이나 정부에 개인적 정보를 제공하는 데 역시 커다란 심리적 부담감을 느끼지도 않아서 굳이 사생활권 보호를 위한 정부의 별도기구 설치의 필요성에도 공감하지 않는다. 이 계층은 기본적으로 사회불신 정도가 낮은 특성을 보인다.[152]

'한백-덴츠' 조사결과는 정부와 사회에 대한 불신도가 높을수록 사생활보호 조치에 민감한 반응을 보이고, 신뢰도가 높을수록 무관심하다는 점이다. 이 조사결과는 따라서 정보생산과 유통의 투명성을 통한 정부와 사회신뢰도 구축이 사생활권과 공공성 사이의 정책적 접점을 찾는데 매우 중요한 고려사항임을 보여준다.

즉, 시민들의 정부에 대한 신뢰를 확보하면 그 사회는 시민적 저항에 직면하지 않고 한결 수월하게 사회공공성을 강조하는 정책을 펼칠 수 있고, 정책 구현에 운신의 폭을 넓힐 수 있다는 점이다. 반면, 정부가 시민들의 신뢰획득에 실패한다면 사생활권에 민감해진 시민들을 상대로 공공성을 호소할 명분과 근거를 상실하여, 사회합목적적 정책 전개에 어려움을 겪을 수밖에 없다. 결국 정부가 시민들의 신뢰를 상실하면 사회공공성도 위기에 처하는 악순환에 빠져들게 된다는 점이다.

정보통신 기술의 발달은 개인적 사생활을 침해하리라는 우려는 장기간 지

152) 참조, Big Brother Inside Campaign. <http://www.bigbrotherinside.org>.

속되어왔다 현재 진행되고 있는 도감청과 도촬, 신상정보의 유출과 저장등은 조지 오웰의 1984년의 우려의 일부분이다.

그러나 정보기술의 발달이 개인적 사생활을 침해하리라는 두려움을 '단기적' 전망이라고 한다면 '장기적'인 관점에서 본다면 오히려 그 반대의 현상이 발생한 가능성이 높다. 사생활을 침해할 수 있는 정보기술의 발달은 개인정보의 자율성을 조절할 수 있는 보다 강력한 수단이 될 수도 있기 때문이다.

현재 정보화 혁명의 과정에서 이러한 혁명이 진행되고 있다. 이러한 통제력을 확보함으로써 개인들은 그들의 정보를 원하는 측과의 협상력을 강화시킬 수 있다.

과거의 대응책은 규제일변도로 이루어져 왔다. 전화나 방송이 정부에 의해 통제되는 상황에서 그로인한 사생활권의 침해가 발생했을 때, 정부에 규제를 요구하는 것은 당연한 반응이었다. 이러한 방식은 사생활권의 보호라는 이슈를 권리와 정부, 혹은 정부 통제하 기관의 관계로 제한하였다.

그러나 그러한 시각은 권리를 결과로 인식하는 정체적 관점이다. 권리란 사회의 대부분의 분야에서 복잡다단하게 발생하는 사회적 교환의 시작일 뿐이다.

사생활권이란 교환적 가치이며, 여기에서 많은 이해당사자들이 충돌하는 것이다.

그러나 사생활권이란 신성불가침의 권리로서 무조건적으로 보호되고 어떠한 사회적 가치보다 우선되어야 한다는 시각은 지나치게 단순할 수도 있다. 사생활권을 바라보는 다른 시각들도 존재한다.

부정적 사생활: 사생활이란 바람직하지 못한 개인적 행위들을 감추려는 측면도 있다. 이는 부분적으로 사실이기도 하나, 이러한 견해는 개인적 자유를 위축시킨다. 권위주의적이거나 낙후한 사회에서는 사회구성원들을 통치자의

지배하에 두기 위하여 사생활권을 인정하지 않는 경우도 있다. 따라서 사생활권이란 문명화되고 자유화된 사회의 시금석이기도 하다.

사생활권의 경제비용: 사생활권은 정보수집 비용을 증대시킨다. 만약 잠재적 고용자나 구매자가 자신이 상대해야 할 대상에 대한 정보가 차단되어 있어 그 정보수집에 더 많은 비용을 지불해야 한다. 또한 거짓이 용이하게 되며 정보처리 비용이 증대하게 되기도 한다.

사생활은 엘리트 전유물: 이 견해는 사생활권 보호와 그 침해의 우려는 사회조직을 폭넓고 깊게 파악하는 제한된 소수의 엘리트계층에서만 제기되는 것으로 이해하기도 한다.

그러나 한 조사보고서에 따르면 미국의 경우 전화번호부에 자신의 이름을 기재하는 것에 대해서조차도 맨해튼 주민의 34%, 그리고 미국전체 주민의 24%가 반대하는 것으로 나타나는 바와 같이 자신의 개인신상 정보가 공중에 노출되는 것을 조심스러워하는 현상은 일반시민들 사이에서도 이미 광범위하게 형성된 정보화 시대의 모습이다.[153]

VI-8. '국민의 알 권리' 와 '국가의 감출 권리'

정보공개법의 시행과 더불어 비공개 정보(classified information)을 범위를 행정편의주의적이 아닌 대국민 봉사의 차원에서 엄격히 제한하여 최소화시키고 공개정보(unclassified information)를 확대하여, 국가의 안위와 사회혼란을 야기시킬 충분한 개연성이 있는 경우에만 비공개 정보로 전환, 많은 국가정보를 일반시민에게 공공재(public good)로서 환원하여야 한다.

공개정보의 확대 적용의 당위성은;

1) 교육수준의 일반적 향상으로 과거와는 달리 일반국민들이 공개된 정보에 대하여 보다 성숙한 '해석' 을 하고 '수용' 을 할 준비가 되어있다. 예를 들어 과거 민감한 안보정보의 무조건적인 국가독점은 오히려 안보불감증이나 안보과민증과 같은 비생산적인 안보혼란을 야기하기도 했다. 또한 현재 북한 핵위기에 대한 정확한 정보부재 역시 정부의 대북정책을 수행함에 있

153) Federal Communications Commission, In the Matter of the Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, November 5, 2003.

어서 국민적 합의 도출을 어렵게 하는 경향을 보이고 있다.

2)지식정보화 시대의 현상으로 이미 최고의 기밀을 제외한 많은 정보들이 정보기술의 발달로 광범위하게 공개되고 확산되고 있다. 비공식적 경로를 통한 민감한 정보들의 유통은 오히려 공식적인 정부의 '공개' 보다 불필요한 사회적 혼란을 야기할 우려가 있다.

그러나 공개정보의 확대는 다른 조건의 충족을 전제로 해야만 그 제도적 장치마련의 본래 취지를 살릴 수 있고, 의미부여가 가능하다.

모든 정보의 공개를 원칙으로 하고 비밀정보는 예외적으로 분류관리하는 미국식 정보공개법(positive system)을 따를 경우, 신중하게 제한적으로 선정된 '미공개 정보(국가기밀)' 의 엄격한 유지가 필수적이다. 비밀정보조차 제대로 기밀유지가 안된다면 사실상 정보공개법은 무의미하게 되고, 오히려 극도의 혼란만 야기하게 될 것이다.

비공개 국가정보의 유출은 명백한 위법행위이지만 실제로 법적 제재와 처벌을 받은 경우는 극히 예외적이다. 이는 비단 우리사회뿐만 아니라 미국을 비롯한 전세계적인 현상이기도 하다. 1급국가기밀 유출의 경우 극단적으로는 외환과 전쟁까지 야기할 수 있으며, 그 외에 2급 기밀의 경우도 심각한 내부혼란과 사회가 감당키 어렵고 회복불가능한 결정적 타격을 입는 경우도 있다. 따라서 이러한 인식하에 관행적으로 언론자유의 보호막 속에서 유명무실하게 운영되어왔던 국가정보보호법을 엄격하게 적용, 실해해야 한다.

그럼으로써 사설정보업체들의 무책임하고 무분별한 국가기밀정보 유출시도 유혹을 원천적으로 봉쇄할 수 있으며, 그에 따른 사회적 비용과 혼란을 최소화할 수 있다.

국가기밀정보 유출의 책임자는 크게 보아 정보당국자와 그를 통해 유출된 정보의 유통을 담당한 언론사(인)으로 구분된다. 정보당국자가 정보를 유출을 하였을 경우, 그 당사자에 대한 징계와 처벌은 비교적 엄격하게 집행되어 왔으나, 언론인에 대한 처벌은 성공적으로 집행되지 못한 데에 정보유출 만

연과 관행화의 근본적 원인이 있다.

이는 첫째, 정보유출에 책임있는 정부관리나 국회의원들을 상대로 강력한 제재를 지속적으로 전개하지 못한 정치적 의지의 부족, 둘째 , 정부 내에서 예상정책의 방향에 반대하는 세력이 불법적 정보유출을 통하여 그 정책에 영향을 끼치려는 의도에서 비롯되는 것으로 연구되고 있다.

이밖에 또 다른 주요원인은 민주사회에서 언론의 자유와 '국민의 알 권리'에 대한 신성불가침성이 상업주의 언론의 선정성(sensationalism)에 편승하여 무분별한 정보유출이 끊이지 않고 발생하였다.

지난 언론의 역사는 국가기밀 정보의 유출 통제가 성공하지 못했으며 모두에게 실망스러웠던 것으로 평가된다. 정보유출의 주된 경로인 언론을 '국민의 알 권리'라는 이유로 법적으로 강력히 제재할 수 없다면 결국 국가는 국가기밀 유출에 대해서 무기력할 수밖에 없게 된다.

- 비공개 기밀의 불법적 유출행위는 엄격하게 불법행위로 간주하여 처벌해야 한다는 원칙이 정치, 경제적 고려를 떠나 고수되어야 한다.
- 첩보 정보'와 '국가안전과 안보 정보'의 개념규정을 명확히 하여, 일반 첩보정보도 그것이 국가안전과 직접적으로 관련될 경우 그 첩보의 수집방법과 활동, 운영 역시 국가기밀정보로 분류해야한다.
- 고급기밀정보와 그 기밀이 민감할수록 재판과정과 처벌과정에서 그 엄격성이 강조되어야 한다.

유출된 비공개 정보를 보도한 언론인에게도 법적 책임이 추궁되어야 한다. 정보유출의 첫 번째 책임은 정부관리가 져야하지만 그 정보를 보도한 언론인에게도 법적 책임을 묻는데 대하여는 논란의 여지가 있는 것이 사실이다.

그러나 비공개 정보 기밀 유지의 효율성을 위하여 언론인, 저자, 출판사, 미디어, 그리고 웹 사이트 운영자에게도 일정부분 책임 추궁과 법적 제재가 따라야만 한다. 특히 단순히 기자에게 책임을 묻는 것으로는 실효성이 떨어지

고 해당언론사 대표에게 법적 책임을 부과하여야 그 실효성을 담보할 수 있다.

정보유출 방지를 위한 언론인에 대한 법적책임 추궁은 필수적이다. 정보의 공개와 비공개를 결정하는 정보관리는 국민에 의해 선출되었거나, 선출된 인물에 의해 지명된 자이기 때문에 그 선택의 정당성이 보장된다. 그러나 언론인은 국민에 의한 대표성을 확보하지는 못한다. 언론이 자의적으로 정보의 공개와 비공개를 판단한다는 것은 이러한 민주적 절차에 위배된다.

비공개 정보의 유출 행위에 대한 법적 책임 추궁은 그 실체가 분명한 언론사일 경우는 비교적 대상이 확실하나, 무분별하게 난립한 실체조차 파악되지 않는 군소사설정보지를 통한 정보유출일 경우는 더욱 어려워진다. 또한 '정규' 언론의 경우 사회윤리적 규범(social ethical code)에 대한 인식과 언론의 '공공성' 에 대한 최소한의 책임과 사명감을 기대할 수 있으나, 난립하는 영세 무허가 군소 사설정보지에 이러한 사회윤리와 공공성을 기대하기는 어렵다.[154]

따라서 사설정보업체의 양성화를 통한 정확한 실태파악과 엄정한 등록제, 그리고 법적 구성요건의 강화와 엄격한 실천이 선행되어야 하며, 비공개로 분류된 국가정보의 유출 행위에 대해서는 엄정한 법적 제재가 시행되어야 한다.

먼저 정보유출에 대한 법적제재의 실효적 적용과 집행은 정치적 의지를 요구한다. 정부내의 정보 유출자들과 언론인들은 그것이 간첩행위에 준한다는 사실을 명확히 인식해야한다.

그들의 의도가 간첩행위는 아니라고 할지라도 그 결과는 동일하기 때문이다. 만약에 정부관리나 언론인이 외국(혹은 적대국)에 그러한 정보를 전달했다면 이는 명백한 간첩행위로서 법적제재를 받게 되는 것과 마찬가지로, 언론을 통하여 출판물에 의한 유출행위도 동일한 범죄행위로 엄격하게 통제되어야

154) Hooshang Amirahmara야, 'Toward a Dynamic Theory of the State and CIvil Society in *The Development Process' in Global Transformation Toward a Sustainable Civil Society* (Hanul Academy, 2002)

한다.

기존에 엄연히 규정화되어 있는 법제도를 실행에 옮기지 않고 사문화시키는 것은 책임의 방기이며 엄격한 의미에서의 직무유기라고 할 수 있다. 이러한 법적용의 무관심과 방기는 국가정보능력에 심대한 타격을 가져올 수도 있다. 국가 기밀정보의 유출은 국가의 예민한 정부 수집능력에 심대하고 돌이킬 수 없는 피해를 야기하게 된다.

독특하고 민감하고, 때로는 예민한 정보수집 경로가 유출, 공개된다는 것은 미디어와 정보유출자가 사적인 이익을 위해 국가의 안위와 이익에 정면으로 도전하는 것과 다름없다.

간혹 국회에서 정치인들이 민감한 비공개 안보정보를 공개적으로 공개하여 사회문제가 발생하나, 대부분의 경우 정치적 타협으로 법적인 제재에 이르지 못하는 것도 이에 해당된다 하겠다.

따라서 정보유출 행위에 대한 엄격한 법의 적용과 집행이 사회구성원들의 공감대를 형성하기 위해서는 비공개 정보(classified)로 분류된 정보의 '비공개' 이유가 특정집단이나 개인을 위해서가 아니라 국민전체를 위한 것이라는 '신뢰'의 구축이 우선되어야 할 것이다. 그래야만 그 정보의 유출이 특정집단이나 특정인에게만 해로운 것이 아니라 국민 모두에게 타격을 가한다는 사회적 공분이 가능하고, 또한 법적 제재의 공감대를 형성할 수 있게 될 것이다.

유출된 정보의 '공동선 목적'이 신뢰받지 못한다면 '국민의 알 권리'인 '언론의 자유'와 '국가의 감출 권리'인 국가정보보호법의 가치충돌에서 '국가의 감출 권리'는 쉽게 무관심해지고 공격당하게 될 것이다.

미국 사례연구에서 살펴본 바와 같이 전통적으로 건국이후 언론의 자유와 표현의 자유를 국가적 가치의 핵심으로 강조하는 미국도 이러한 인식의 바탕위에서 비공개 기밀 국가 정보 유출에 대한 언론의 법적책임을 강조하는

추세이다. 지난 2005년 11월 발생한 소위 리크 게이트(Leakgate)가 정보화 시대의 환경에 따른 미국의 정책방향 선회의 신호로 여겨진다.

사태의 발단은 CNN 토크쇼 '크로스파이어(CROSSFIRE)'의 진행자이자 칼럼니스트인 로버트 노박(Robert Novak)이 지난 2003년 7월 14일 '두 명의 고위 행정부 관리'의 말을 인용해 CIA 여성 비밀요원 발레리 플레임의 신분을 폭로했다[155]. 비밀요원의 신분을 폭로한 것은 국가안보는 물론 당사자의 생명까지 위협하는 명백한 범죄행위이다. 지난 82년에 제정된 정보원 신원 보호법 위반으로 최고 10년형에다 5만달러의 벌금형에 처해질 수 있다.

리크 게이트(Leakgate;정보유출 파문)로 불리는 이 사건에 특별검사가 임명돼 수사에 착수했으며, 취재원 공개를 거부했던 뉴욕타임즈(The New York Times)의 여기자 쥬디스 밀러(Judith Miller)는 결국 이례적으로 구속되었다. 미국법정은 쥬디스 기자에게 법정모독죄를 적용했다.[156] 취재원을 밝히라는 법원의 요구를 거부했기 때문이지만, 이는 국가기밀 유출에 대해서는 언론의 자유권리까지도 일부분 제한하고 엄격한 법적 제재를 가하겠다는 의미로서, 결국 미국정부가 국가의 기밀정보에 대한 통제를 엄격하게 강화시킨다는 정책변화의 신호로 해석된다.

또한 거대언론의 유력기자의 구속이라는 초유의 사태를 야기한 Leakgate에 대한 미국시민들의 반응은 대체적으로 정부의 조치에 공감하는 편으로 보도된다. 이는 미국정부의 포지티브 정보공개법에서도 미국정부가 '기밀'로 보호하려는 정보는 공동체의 안위를 위해 보호되어야 할 정당한 이유가 있다고 믿기 때문으로 분석된다.

Leakgate의 사례는 국가기밀 정보 유출에 대한 엄격한 법적 제재가 사회적 공감대를 얻기 위해서는 먼저 정부의 투명한 정보관리와 과감한 정보공개 정책이 선행되어야 함을 보여준다.

---

155) Joseph Wilson, FBI interviews CIA Operative reprot, October 7, 2003, 'Without Justice There is Just US!'

156) New York Times, Sep. 29, 2005, 'Judith Miller Out of Jail, Will Testify Friday'

POLICE SCIENCE INSTITUTE