가상공간(사이버)에서의 부패: 행정윤리적 접근*

Controlling Cyber Corruption: an Administrative Ethics

김 영 종 (Kim, Young Jong)**

ABSTRACT

This research focuses on the reality of new serious corruption phenomena called cyber corruption. Unlike previous research, which mainly focuses on the corruption phenomena in the visible social world in the process of social change, cyber corruption is new corruption phenomena, which have been created in the process of radical scientific and technological development by computerizing information in the 21st century. The paper discusses the conceptualization of cyber corruption, compared with computer crime in terms of comparative perspective. The author proposes that cyber corruption is a broad concept that extends the notion of ordinary computer crime. The characteristics of cyber corruption include anonymity, speciality, unlimitation of time and space, rapid propagation, unlimited damage of property, unfaced communication, and unfeeling of sin regarding the matter. As for the analysis of existing cyber corruption phenomena, major efforts have been made to identify general patterns and various typologies of the cyber space. The author suggests several ways to effectively measure and control cyber corruption phenomena, especially in terms of administrative ethics.

* 이 논문은 2001년도 숭실대학교 교내 학술연구비 지원에 의하여 이루어졌음.

** 숭실대학교 행정학과 교수 (行·博)

Ⅰ. 서론: 연구의 목적과 방법, 그리고 한계

부패는 건강한 사회를 파괴시키고 특히 인간의 삶의 질을 저하시키는 사회적 암(social cancer)이라고 하여도 과언이 아닐 것이다. 국제투명성 위원회(TI)는 해마다 각국의 부패지수(CPI)를 발표하고 있다. 이에 의하면 우리 나라의 부패정도의 등위는 95년에는 27위, 96년도 27위, 97년도 34위, 98년도 48위, 99년도 50위, 2000년 48위, 그리고 2001년 42위로 나타났다. 특히 부패지수는 지난 3년동안 4.0/10정도를 맴돌고 있다. 2001년도의 발표에 의하면 한국은 세계 91개국의 비교국 중에서 42위를 차지하였고 CPI는 4.2/10를 차지하였다.[1)]

한국정신문화연구원(99.3), 리서취 & 리서취(99.5), 한국갤럽(99.7), 현대리서취(99.11)가 실시한 부패에 관한 여론조사에서 응답자의 93%, 91%, 95%, 92%가 각각 부패의 심각성을 인정하고 있다. 한편 서울시가 1999년 12월에 1년간 일선구청을 통해 민원업무를 이용하였던 민원인 8,789에 상대로 조사하여 발표한 '반부패지수'에 의하면 민생분야(예: 건설, 위생, 세무 등)가 평균 74.8%에 이르고 있다. 이제 부패가 삶의 방식(modus operandi)이 되어버린 것 같다.[2)] 특히 놀라운 사실은 구조화된 부패현상은 실제공간에서만이 아니라 가상공간에서도 급속도로 확산되고 있는데 문제의 심각성이 있다.

부패는 국가사회의 기본적인 조직기능을 저하시키고, 정치행정의 비용을 증가시키며, 합리적인 의사결정을 방해하고, 궁극적으로 심각한 사회적 갈등을 일으키게 함으로서 국가사회의 발전을 가로막는 공적이다[3)]. 이 부패는 실제공간에서 인위적인 일탈행태로 일어나는 것이 일반적이었으나 정보화와 세계화에 따라서 이제는 실제공간이 아닌 가상공간에서 상상을 초월할 정도의 부패현상이 범람하고 있는 것이 현실이다. 사이버 공간은 바로 익명성에 의해 지배되는 문화 공간이기 때문에 행동의 탈억제(disinhibition)를 수반하여 자기통제(self-control)의 윤리적 기능을 벗어나 부패의 일탈 행동을 하게된다. 뿐만 아니라 사이버 공간자체가 개방성과 평등성이 보장되는 공간이고 정보의 공유가 용이하고 또한 이용자의 구성원들 사이에 수평적인 관계가 존재하기 때문에 상대방의 인격과 권리를 무시하는 비윤리적인 방법으로 쉽게 부패의 유혹에 몰입하게된다. 사이버부패야 말로 21세기에 들어와 일년이 지나가는 현 시점에서 앞으로 국가사회가 당면한 최대의 과제가 아닐 수 없다. 바로 그것은 국가사회의 문제이고 모든 공사조직이 당면한 절실한 해결 과제라고 할 수 있다. 그런데 사이버공간에는 2000년 현재 약 327억여명에 달하는 사용자가 인터넷을 이용하고 있다. 이 수치는 10년전인 1990년의 1억 8천 5백만명에 비해 176배 이상 증가한 것으로 사이버 공간을 사용하는 사람이 매년 큰 폭으로 늘어나고 있음을 알수 있다. 국내의 경우도 2000년 8월 현재 1,640만명이 인터넷을 이용하고 있다[4)]. 2001년 9월 30일 현재 컴퓨터 범죄의 유형별

---

1) 자세한 것은 국제투명성위원회(Transparency Internmational: TI)의 자료를 참고할것 www.transparency.org

2) Simcha B. Werner, "New Direction in the Study of Administrative Corruption" in *Public Administration Review (1983)*, pp.146-154.

3) 김영종, 부패학(4판증보판) (서울: 숭실대출판부, 2001), pp.335-347.

발생현황을 보면 지난 '1997년-'2001년 기간중 전자문서관련죄는 106명, 전산업무방해는 81명, 전자기록비밀침해는 27명, 컴퓨터사용사기는 933명, 전자기록손괴는 21명, 정보통신망법 위반은 2,058명, 개인정보보호법 위반은 108명, 그리고 특별법위반은 33명, 총계 3,671명이나 되는 범죄자가 발생하였다. 특히 그중에서 457명이 구속 수사되었다. 한마디로 컴퓨터 범죄가 급속하게 확산되고 있는 것을 유의하여야한다.[5] 따라서 이 연구의 목적과 필요성은 다음과 같이 요약 정리 할 수 있다.

이 연구의 목적은 첫째, 사이버 공간에서의 부패 개념을 정립하고 둘째, 사이버공간에서의 행정윤리의 패러다임(paradigm)을 제시한다. 셋째, 사이버부패의 통제와 예방의 전략을 행정윤리적인 접근을 통하여 모색한다. 이 연구는 사이버부패의 선행연구가 전무한 시점에서 탐색적인 연구(exploratory research) 이므로 연구자의 주장에는 상이한 의견이 있을 수 있음을 인정하나 또 다른 기회에 시론 적인 연구를 보완할 수 있음을 밝힌다.

이 연구에서의 용어문제 있어서는 가상공간을 사이버(cyber) 라고 하고 '가상공간에서의 부패' 를 간단하게 '사이버부패' 라고 혼용하여 사용하기로 한다.

Ⅱ. 가상공간(사이버)에서의 부패에 관한 이론적인 개념정립

1. 실제공간에서의 부패이론

지난해 한국의 지하경제 규모는 59조원으로 국내총생산(GDP)의 11.3%에 이르는 것으로 추정됐다. LG경제연구원은 지난 30년간 지하 경제 규모를 따져 본 결과 이 같이 나타났다고 밝히고, 이같은 지하 경제 비중은 GDP의 10%이하인 스위스 미국보다 높고 일본 영국 캐나다 등과 비슷하며 13%선인 홍콩 싱가포르에 비해 낮다고 밝혔다.[6] 높은 지하경제 의존율은 부패의 감염도를 말한다고 할 수 있다.

부패에 대한 일반적인 개념적 정의를 보면 다음과 같은 여러 다양한 학설을 통하여 차이점을 알 수 있다. 다음의 <표 1>에 의하면 사회부패의 실체는 다양한 개념정의에 의하여 논의된다. 예컨대 윤리 도덕설은 윤리적 규범을 위반한 경우를 부패라고 하며, 공익설은 공익 위반을 부패라고 한다. 그리고 권력설은 권력의 남용을 부패라고 한다. 따라서 우리는 문제의 초점이 부패라는 개념적 정의가 보는 시각에 따라 다르나 <표 1>에서 제시하듯이 부패에 대한 통전적인 접근인 통합설(integrated approach) 에 의한 부패의 개념으로 보는 것이 바람직하다. 즉 부패는 공직자들이 국민의 기대가능성(expectation)을 일탈하여 불법적이거나 비윤리적으로 공직을 남용하여 사익을 추구하는 일체의 일탈행위(deviant behavior)를

---

4) http://icic.sppo.go.kr/

5) 자세한 것은 아래의 자료를 참고할것
http://www.icic.sppo.go.kr/statistics/table01.htm

6) www.jlogis.com

말한다.[7] 여기에서 공직자의 범위는 사실상 확대되는 추세이며 공조직 에서만 아니라 사적인 부문(private sector)에서도 부패가 구조화되고 있는 것이 현실이다.

〈표 1〉 실제공간에서의 부패에 관한 주요학설

접근방법 (approach)	주요내용	분석의 단위 (unit of analysis)	대표학자
윤리 및 도덕설 (moral approach)	공직의 비윤리적 및 비도덕적 이용	관료와 사회(관료의 행위)	E. C. Banfield R. Wraith J. T. C. Liu
제도적 접근설 (institutional approach)	제도적 취약성과 사회적 기강의 해이	후진국이나 개발도상국의 관료제도, 연성국가(Soft State)	S. P. Huntington E. V. Roy G. Myrdal
시장/교환설 (market/exchange approach)	특수이익을 추구하는 시장교환관계	관료와 고객집단(관료의 직책)	J. V. Klavern R. O. Tilman A. J. Heidenheimer H. Simon
공익설(public interests approach)	공익위반의 결과	관료의 행태, 의사결정과정 (이해관계 집단의 공존된 이익)	R. W. Friedrichs H. D Lasswell
기능주의설 (functionalism approach)	발전과정의 부산물	관료제도, 기업가, 사회(후진국)	N. H. Leff J. S. Nye B. F. Hoselitz
후기기능주의 (post-functionalism approach)	보편적 현상과 자기영속성 현상	선진국의 관료제도 후진국의 관료제도	S. B. Werner
권력관계설 (power-relations approach)	관료의 권력남용과 역기능 부산물	관료제와 권력	F. W. Riggs H. H. Werlin J. C. Scott
사회문화적규범 (socio-cultural approach)	사회문화적 환경과 정통의 부산물	사회문화적 환경, 관료제의 역사성	R. Wraith E. Simpkins
통합설 (intearated approach)	복합적 행정현상:선진국과 후진국의 공통성과 특수성, 부패의 제변수(예:제도. 행태. 환경)의 복합적 다면적 현상, 제도, 행태, 환경의 상호부적응에서 발생하는 복합행위, 공직의 사회문화적 규범위반과 기대가능성의 일탈행위	선진국과 후진국의 관료제도의 특징 비교 관료제도, 행태, 그리고 사회문화적 환경의 주요변수분석, 발전의 특수성과 보편성, 목표와 과정, 질양 그리고 가치변화, 또는 문제발견과 문제해결의 통합적 분석	필자는 이 접근 방법을 개발하려고 한다.

자료: 김영종, 부패학(서울: 숭실대 출판부, 2001), p .38.

7) 김영종, 부패학 (서울: 숭실대출판부, 2001), pp.1-103.

2. 가상공간(사이버)에서의 부패의 개념과 이론

1) 정보화사회의 역할

오늘날 정부는 과거의 통치적인 권력기구로서의 의미인 정부(government) 개념에서 거버넌스의 개념으로 변모하고 있다. 즉 다양한 행위자들과(actors)과 이들간의 상호작용과정(process)과 그 산물인 조직(organization)과 제도(institution), 그리고 이들간의 조정기제(mechanism) 및 규범(rule)들이 포함된다[8]. 정부가 지향하는 정치행정의 궁극적인 목적은 무엇일까? 한마디로 그것은 국민의 삶의 질(quality of human life)을 향상키 위하여 존재하는 조직이다. 국민의 행복을 위하여 봉사하는 것이 정치행정의 몫이다[9]. 따라서 고객중심의 봉사행정이 철저하게 이루어 져야 한다. 이러한 것의 요체는 얼마나 정직하게 친절하게 그리고 깨끗하게 행정업무를 수행하는가를 고객인 국민들로부터 매년 평가받아야한다. 최근에 우리 나라는 전세계적인 추세에 상응하여 행정 정보화 시스팀의 구축이 급진적으로 진행되고 있다. 이러한 것은 행정의 발전에 따른 미래패러다임에 엄청난 변수로 작용할 것이다. 그러나 가상공간의 활용이 증가되는 것이 국민의 삶의 질이 향상된다고 보는 긍정적인 면이 있으나 한편 가상공간에서의 윤리적인 타락과 부패는 심각한 국가사회문제로 등장하고 있는 것도 사실이다. 21세기는 정보화사회라고 한다. 먼저 정보화사회의 특징을 살펴보자.[10]

첫째, 정보사회에 있어서 정치적인 특징은 미래학자들의 시각에 따라서 다르다.[11] 예컨대 Alvin Toffler는 소수에 의한 의사결정과 엘리트 민주주의를 주장하였고, D. Bell은 대표민주주의는 변동하고 의사결정의 주축은 컴퓨터라고 하였으며, J. Naisbitt는 대표민주주의 재진단을 주장하고 있다.

둘째, 경제적인 면에서 과학과 기술의 발달로 인하여 국민들의 다양한 수요를 공급하기 위한 서비스산업이 발달하고, 특히 정보산업의 발달과 지식 집약적인 고부가가치형 산업구조가 성장할 것이다. 그리고 국제화와 개방화에 따라서 무역과 경제의 활발한 교류, 그리고 기술혁신의 수요도 일어나게 된다.

셋째, 사회적인 면에서 정보사회에서는 점점 다원화되고 다양화되며 사회적인 이동성도 커지게 될 것이다. 사회적인 지위는 바로 정보를 주도해 가는 사람이 하게 될 것이며 도시사회는 지방과의 격차가 감소되고 보편화된 사회가 될 것이다.

넷째, 과학 기술적인 차원정보사회는 과학과 기술의 발달에 의하여 안간의 삶의 질은 향상되고 의사결정의 핵심은 바로 컴퓨터에 의하여 결정된다. 컴퓨터는 인간의 모든 삶의 중요한 수단으로 활용되고 삶의 패턴은 크게 달라지게 되다. 예컨대 교육의 수단도 재택수업을 활용하고, 직장에서의 업무도 재택에서 가능하고 그것이 일반화되는 사회가 된다는

---

8) 김석준외 3 인 공저, 『뉴거버넌스연구』 서울: 대영문화사, 2000, pp. 56-57.

9) H. George Frederickson,(ed.). *Ethics and Public Administration*, (New York: M.E. Sharpe, Inc.. 1993), pp.1- 55.

10) 김영종, 신발전행정론 (서울: 법문사, 1997), pp.471-491.

11) Daniel Bell, *The Coming of Post-Industrial Socicy* (New York: Basic Book, Inc..1973), pp. 3-145.

것이다.

다섯째, 외형상으로는 컴퓨터에 의한 원격통신(telecommunication)이 핵심 기술의 기능을 수행하며 산업에 있어서도 정보산업이 주종을 이룬다. 특히 통신면에서 음성정보, 문자정보, 그림정보, 등이 보급되고 정보매체도 종이에서 디스크나 테이프 형태로 전환하게 된다.

2) 가상공간에서의 부패의 특징

그 다음에는 사이버 부패의 특징은 어떤 것일까?[12]

첫째, 컴퓨터는 다원적인 변화를 일으킬 수 있는 첨단과학기술의 산물이지만 그 컴퓨터를 이용한 부패는 엄청난 피해를 줄 수 있는 고도의 과학 기술적 . 지능적 . 역기능적 산물이 될 수 있다.

둘째, 사이버 부패는 범죄자체가 컴퓨터를 범죄도구로써 사용하게 되며 이것은 폭력주의(vandalism)와 고의적인 속임수 그리고 장난 등이 혼재 되는 경우가 많다.

셋째, 사이버 부패는 고도의 전문성, 기술성 그리고 과학적 지능성이 범죄에 이용되므로 엄청난 피해가 일시에 발생하는 경우가 많다. 특히 컴퓨터 범죄는 그 범죄의 속성상 수사하기가 매우 까다롭고 어렵기 때문에 관계기관의 전문성이 요청되고 면밀한 공조체제가 필요하다.

넷째, 사이버 부패는 가장 빠르고 가장 넓은 장소에 걸쳐서 일어날 수 있는 것이므로 때로는 국내뿐만 아니라 국제 공존체제가 필요한 경우가 많다.

다섯째, 사이버 부패는 대부분 정보의 누설과 자료를 절취, 횡령, 또는 사기하는 경우가 많으며, 그것은 재산에 관한 범죄가 대부분이다. 이상과 같은 부패와 범죄속성을 가지는 것은 폭력, 마약, 밀수 등의 실제공간에서의 사회적 부패(social corruption) 못지 않게 정보사회화에 부응하여 증가 일로 에 있는 세계적이고 국제적인 범죄라고 하여도 과언이 아닐 것이다. 특히 우리 나라도 최근에 행정전산화가 앞당겨지고 국가사회의 제반구조가 정보 사회화됨에 따라 컴퓨터는 이제 국가의 모든 영역, 예컨대 정치, 행정, 경제, 산업, 금융, 군사, 문화, 교육, 학술 그리고 국민의 일상생활정보에 보편화되기까지 일반화 . 보편화되는 추세에 있음은 주지의 사실이다. 이에 부응하여 가상공간의 부패와 범죄도 심각한 사회문제로 부각될 것이 예상되므로 여기에 대한 정부의 철저한 종합대책이 강구되어야 하므로 이러한 문제를 논의하는 것은 매우 의미 있다고 하겠다. 정보화가 삶의 질을 높인다는 보장은 없다. 어떤 면에서는 행정의 전산화는 심각한 가상공간에서의 부패문제를 야기 시키고 있다. 부패현상의 통제는 처벌위주의 강제적이고 외압적인 통제만으로는 소기의 성과를 기대할 수 없다. 그 대신에 부패의 서식이 가능한 조직의 문화를 변화시키는 통제전략은 조직구성원과 그 조직의 책임자들로 하여금 부패통제의 공동책임성을 유발시키고 나아가서는 구성원으로서의 연대의식과 응집력을 강화시켜 조직의 문화를 변화시키는 중요한 변수로서의 기능을 발휘할 수 있다. 가상공간에서의 부패문제는 위험수위를 넘을 정도로 심각하다. 예컨대 가상공간을

12) 김영종, "정보부패의 패러다임 정립과 치유" 한국 부패 학회 보, 제3호, 서울: 한국부패학회, 1999, pp.25-40.

이용한 정보의 오용과 남용 그리고 개인의 프라이버시에 대한 침해 등을 들 수 있다.

결론적으로 우리는 가상공간이 우리의 삶을 반드시 행복하게 해 주리라고 지나치게 기대해서는 아니 된다. 가상공간의 부패를 막아내겠다는 단호한 의지와 종합대책이 강구되어야 한다. 따라서 앞으로는 현행 부패방지법에는 사이버부패도 포함되어야한다.

3) 사이버부패와 컴퓨터범죄의 비교

먼저 컴퓨터 범죄(computer crime)란 무엇을 말하는가?[13] 여기에 대한 몇몇 학자들의 개념정의를 우선 살펴보자.[14] John Taber는 "컴퓨터 범죄란 직접적으로 그리고 컴퓨터의 수단에 의하여 발생하는 범죄"라고 정의한다. 한편, Donn Parker는 보다 광범위한 정의를 내리고 있다. 그에 의하면 컴퓨터 범죄란 "피해자가 고통을 받거나 받을 수 있는 컴퓨터와 관련된, 어떤 형태로든 고의적인 행위(intentional act)"라고 말하고 있다. 나아가서는 그에 의하면 컴퓨터 범죄는 컴퓨터 범죄관련법에 관련된 특별한 행위가 될 것이라고 법적인 정의를 내리고 있다. 예를 들면 캘리포니아의 컴퓨터 범죄법 SB 835에 의하면 "컴퓨터 범죄란 어떤 사람이 다른 사람의 신용정보 (credit information)에 관한 권한 밖의 정보를 얻기 위하여 악의로 컴퓨터 시스템이나 컴퓨터 연결망에 접근하거나 접근할 원인제공을 하는 것이다."라고 정의하고 있다.[15] (Any person who maliciously accesses or causes to be accessed any computer system or computer network for the purpose of obtaining unauthorized information concerning the credit information of another person). 이 경우 최고 $ 5,000까지의 벌금이나 16개월간의 징역에 처하도록 되어 있다. 그리고 1984년 6월에 입법된 연방정부의 컴퓨터 사기 및 남용방지법(Computer Fraud and Abuse Act of 1984)에 의하면 컴퓨터 범죄(컴퓨터를 이용한 불법적인 정보나 재산취득)에 있어서 경범일 경우는 $5,000 벌금이나 1년의 징역에 처해지나 중죄의 경우는 벌금 $10,000과 10년까지의 징역에 처할 수 있도록 규정하고 있다는 점이다.

이상에서 서술한 개념정의 외에도 컴퓨터 범죄의 개념은 다양하게 표현될 수 있다. 예를 들면, 다음과 같다.[16] ① 재산범죄의 수단으로서 컴퓨터를 사용하는 경우 ② 컴퓨터의 조작이나 오용에 의하여 저질러진 사기, 횡령, 공갈, 그리고 다른 범죄(fraud, embezzlement, blackmail, and other crimes). ③ 범죄수행에 직접적으로 컴퓨터가 관련된 경우 ④ 범행을 위하여 특별한 컴퓨터 지식이 필요한 불법적 행위 ⑤ 컴퓨터에 의하여 자행되는 일종의 전문직업인의 범죄(whitecollar crime)라고 할 수 있다 이상의 여러 정의를 종합하여 볼때, 컴퓨터 범죄란 정보의 불법취득이나 재산적 가치를 불법적으로 취득할 목적으로 컴퓨터를 조작하거나 오용하는 개인이나 조직의 모든 불법적인 행위라고 할 수 있다.

---

13) 김영종, "정보부패의 패러다임 정립과 치유" 한국 부패 학회 보, 제3호, 서울: 한국부패학회, 1999, pp.25-40.

14) Buck Bloom Becker, Spectacular Computer Crime(Homewood: Dow Jones-Irwin, 1990), pp. 67-73.

15) J. Van Duyn, The Human Factor in Computer Crime(Princeton: Detrocelli Books, 1985), p.14.

16) August Bequai, Technocrimes(Lexington: Lexington Books, 1987), p. 47.

사이버부패와 컴퓨터범죄는 공통점이 있으나 다음과 같은 점에서 차이도 있다.

첫째, 컴퓨터 핵커(hacker)의 경우는 사이버 세계의 평화를 송두리채 뒤흔들어 놓는 무서운 파괴력을 가지고 있는 무서운 범죄이다. 이러한 범죄는 국경을 초월하고 전세계 어느 곳에서나 침범하는 가상 공간의 부패의 극치이다. 우리는 이러한 부패의 도전에 무든 행정력과 기술의 힘을 동원하여 평화파괴의 주범을 막아야 할 것이다.

둘째, 사이버 부패는 바로 정보의 오용과 남용과 깊은 관계가 있다. 정보를 불법적으로 수집하고 팔아먹고, 그리고 함부로 사용하고 하는 모든 행위는 사이버 부패에 포함된다. 이것은 정보를 악용하여 자기의 이기적인 탐욕을 채우고자 하는 부패이다. 이미 많은 경우 이러한 부패현상이 기업에도 정부간에도 그리고 개인에도 일어나고 있음은 주지의 사실이다.

셋째, 사이버 부패는 비도덕적이고 비윤리적인 행위를 포괄하는 개념이다. 폭력과 사기, 그리고 음란이 모두 속한다. 가상공간의 편리성을 악용하여 인간의 존엄성과 가치를 파괴시키는 사이버 부패이다.

넷째, 사이버부패는 컴퓨터 범죄를 동반하는 경우가 많다. 컴퓨터 범죄(Computer Crime)의 개념은 광의로는 일본 경시청에서 "컴퓨터 시스템에 가해지는 범죄 내지 이를 악용하는 범죄의 총체"라고 할 수 있다. 미국 정부는 "컴퓨터 범죄는 컴퓨터 프로그램을 조작하는 것과 같은 극히 기술적으로 세련된 범죄는 물론이고, 컴퓨터 시스템에 대한 허위입력과 출력의 오용에서 유래되는 것"이라고 한다. 한마디로 콤퓨터가 행위의 수단이자 목적인 모든 범죄행위"를 지칭하는 것이 광의의 개념다. 반면에 협의로는 컴퓨터 범죄가 컴퓨터 자료와 관련하여 발생한 재산적 침해행위를 야기시키는 고의의 범죄행위의 총체라고 할 수 있다. 즉 협의로는 컴퓨터 범죄의 개념에서 재산 이외의 법익에 대한 침해는 제외된다. 정보사회가 진전됨에 따라서 기존의 재산군에 대한 개념을 탈피한 기술, 정보 등 새로운 형태의 재산권에 개념이 태동하는 현실을 감안할 때, 컴퓨터 범죄의 개념은 광의적으로 해석하는 것이 타당하다.[17]

다섯째, 사이버부패는 컴퓨터 범죄만 아니라 가상공간을 이용하여 특정한 이익을 도모하는 도덕적 윤리적인 책임과 비난을 받을 수밖에 없는 불건전한 일체의 공익(public interests)위반의 불법적, 비도덕적 일탈행위(deviant behavior)를 총칭한다. 이 경우 컴퓨터범죄 보다 더 포괄적인 개념으로 사용된다.[18] 구체적으로 컴퓨터는 다원적인 변화를 일으킬 수 있는 첨단과학기술의 산물이지만 사이버부패는 엄청난 피해를 줄 수 있는 고도의 과학기술적 . 지능적 . 역기능적 산물이 될 수 있다.

여섯째, 사이버 부패는 범죄자체가 컴퓨터를 범죄도구로써 사용하게 되며 이것은 폭력주의 (vandalism)와 고의적인 속임수 그리고 장난 등이 혼재 되는 경우가 많다. 따라서 사이버 부패는 고도의 전문성, 기술성 그리고 과학적 지능성이 범죄에 이용되므로 엄청난 피해가 일시에 발생하는 경우가 많다. 특히 컴퓨터 범죄는 그 범죄의 속성상 수사하기가 매우

17) 김종범, "정보화사회에 있어서의 역기능 대책", 서울: 한국행정연구, 1996년 가을호, pp.90-100.
18) 김영종, "컴퓨터범죄의 원인과 대책", 교정연구 제4호, 서울: 한국교정학회, 1994, pp.371-389.

까다롭고 어렵기 때문에 관계기관의 전문성이 요청되고 면밀한 공조체제가 필요하다. 사이버 부패는 가장 빠르고 가장 넓은 장소에 걸쳐서 일어날 수 있는 것이므로 때로는 국내뿐만 아니라 국제 공존체제가 필요한 경우가 많다.

일곱째, 사이버 부패는 대부분 정보의 누설과 자료를 절취, 횡령, 또는 사기하는 경우가 많으며, 그것은 재산에 관한 범죄가 대부분이다. 이상과 같은 부패와 범죄속성은 폭력, 마약, 밀수 등의 사회적 부패(social corruption) 못지 않게 정보사회화에 부응하여 증가 일로에 있는 세계적이고 국제적인 범죄라고 하여도 과언이 아닐 것이다. 특히 우리 나라도 최근에 행정전산화가 앞당겨지고 국가사회의 제반구조가 정보 사회화됨에 따라 컴퓨터는 이제 국가의 모든 영역, 예컨대 정치, 행정, 경제, 산업, 금융, 군사, 문화, 교육, 학술 그리고 국민의 일상생활정보에 보편화되기까지 일반화·보편화되는 추세에 있음은 주지의 사실이다. 이에 부응하여 가상공간의 부패와 범죄도 심각한 사회문제로 부각될 것이 예상되므로 여기에 대한 정부의 철저한 종합대책이 강구되어야 하므로 이러한 문제를 논의하는 것은 매우 의미 있다고 하겠다. 정보화가 삶의 질을 높인다는 보장은 없다. 어떤 면에서 행정의 전산화는 심각한 가상공간에서의 부패문제를 야기시키고 있다. 부패현상의 통제는 처벌위주의 강제적이고 외압적인 통제만으로는 소기의 성과를 기대할 수 없다. 대신에 부패의 서식이 가능한 조직의 문화를 변화시키는 통제전략을 위해 조직구성원과 그 조직의 책임자들로 하여금 부패통제의 공동책임성을 유발시키고 나아가서 구성원으로서의 연대의식과 응집력을 강화시켜 조직의 문화를 변화시키는 중요한 변수로서의 기능을 발휘할 수 있게 해야한다. 가상공간에서의 부패문제는 위험수위를 넘을 정도로 심각하다. 예컨대 가상공간을 이용한 정보의 오용과 남용 그리고 개인의 프라이버시에 대한 침해 등을 들 수 있다.

여덟째, 사이버부패의 파괴력(destructive power)은 실제공간의 파괴력을 능가하는 경우가 많고 다양한 행태를 보인다. 예컨대[19] ① 전자기폭탄: 강한 전자기를 내뿜는 이 폭탄은 국가 통신시스템, 전력, 물류, 에너지 등의 사회인프라를 일순간에 무력화시킬 수 있는 엄청난 파괴력을 가지고 있다. ② 온라인폭탄: 데이터량이 큰 메일 수백만통을 동시에 보내 대형 컴퓨터시스템을 다운시키는 수법이다. 공공기관및 대형 사업장의 업무를 마비시킬 정도의 파괴력을 보이고 있다. 온라인폭탄은 서비스를 중단시킬 목적으로 악용되는 경우가 많아 분초를 다투는 금융 등의 분야에서는 치명적인 피해를 입기도 한다. 미국의 유명 전자쇼핑몰업체인 웹콤의 경우 최근 정체불명의 온라인폭탄을 맞고 40시간동안 시스템이 마비돼 엄청난 피해를 입은 바있다. ③ 사이버갱: 세계 유명 금융기관이나 중개거래소에 침입, 보안망을 뚫고 거액을 훔쳐내는 최첨단 범죄조직. 미 국가안전국(NSA)에 따르면 1993-2000년까지 사이버 테러리스트와 사이버갱으로부터 협박당한 테러건수는 모두 40여건. 피해금액도 4,800억원에 이르고 있다. 97년 10월 체코의 한 은행이 사이버갱단으로부터 테러를 당해 1,900만달러를 털렸다. ④ 사이버스파이: 원격에서 사용자ID와 비밀번호를 알아내 전산시스템을 장악, 정보를 빼는 테러리스트들이다. 통신케이블에서 흘러나오는 전자파를 잡아내 전송되는 정보를

19) http://www.sed.co.kr/11_8/199909/h1851104.html

빼내는 범죄이다. ⑤ 기타: 시스템이 보유한 메모리능력이상의 데이터를 보내 시스템을 혼란에 빠뜨린 뒤 각종 관리자의 권한을 빼내는 기억용량초과수법이 있다. 원격검색법은 보안상의 취약점을 찾아내기 위해 개발됐던 프로그램을 해킹에 역이용한 경우 등이다.

요약하면 사이버부패는 컴퓨터범죄를 포함하여 사이버공간에서 행해지는 모든 부패를 말한다. 반면에 컴퓨터범죄(computer crime)는 독립적인 컴퓨터시스템에서의 범죄이다. 사이버범죄의 특징은 ① 비대면성 ② 익명성 ③ 전문성과 기술성 ④ 시간적·공간적 무제약성 ⑤ 빠른 전파성과 천문학적 재산피해 ⑥ 죄의식이 희박 ⑦ 발견과 증명, 고의 입증이 곤란하다는 점이다. 결론적으로 우리는 가상공간이 우리의 삶을 반드시 행복하게 해 주리라고 지나치게 기대해서는 안 된다. 가상공간의 부패를 막아내겠다는 단호한 의지와 종합대책이 강구되어야한다. 따라서 앞으로는 현행 부패방지법에 사이버부패도 포함되어야한다고 본다.
이상에서 논의한 것 중에서 사이버부패와 컴퓨터부패를 비교하면 다음과 같은 <표 2>와 같다.

〈표 2〉 사이버부패와 컴퓨터 부패의 공통점과 차이점 비교

비교 / 종류	컴퓨터범죄 (Computer Crime)	가상공간에서의 부패(사이버부패) (Cyber Corruption)
목 적	특수한 이익취득 혹은 타인의 권익침해	자기 또는 제3자 이익추구 혹은 개인의 탐욕의 추구
수 단	컴퓨터의 이용	컴퓨터이용과 전자장치 오용,악용,남용
특 징	비대면성, 익명성, 전문성, 시공의 무제한, 신속성, 죄의식의 희박, 입증의 곤란성	컴퓨터범죄의 특징 + 비도덕성 + 심리적 무규범성(anomie)
역기능	무서운 파괴력	파괴력 + 정치사회의 신뢰성위기+ 실제공간 부패와의 커넥션 경향
성립 원인	컴퓨터 사용자의 구성요건 해당성, 위법성, 책임성.	개인의 부패심리 + 통제시스템의 결여 + 사회문화적인 환경
실제공간과의 관계	가상공간보다 새로운 범죄유형으로서 고도의 전문성과 기술성을 가진 고로 전파성이 빠르고 대량성이 있으며 국경을 초월하여 확대가능성이 더욱 큼	실제공간보다 은밀성은 약하나 미래사회에서는 급속도로 증가될 전망이며 나아가서는 사회적으로 파괴력도 확산될 전망임
유형	형사법이나 컴퓨터범죄관련 실정법상 위반되는 경우의 일체의 범죄행위	사회적인 비난과 윤리적인 판단에 저촉되는 일체의 일탈행위, 특히 재산취득부패가 주종임
행정윤리적 통 제	컴퓨터범죄의 형사처벌, 기술적인 보안장치필요, 반 컴퓨터범죄 교육훈련 실시	관련 부패 방지 법에 사이버부패의 방지관련 보완필요; 관련공직자 일반인을 위한 특별교육의 실시, 사회 문화적인 통제실시, 범국민적인 사이버 반부패 윤리의식 교육의 필요

자료: 이 도표는 필자가 직접 구상하여 작성한 것 임

Ⅲ. 가상공간(사이버)에서의 부패의 역기능

21세기에는 정보화가 가속화되고 있다. 여기에서 정보화의 역기능을 요약하면 다음과 같다. ① 공장 자 동화로 인해 실업에 대한 우려가 증가한다. ② 개인의 정보가 유출됨으로써 사생활 침해가 대두된다. ③ 소수의 집단이 정보를 독점함으로써 불평등의 문제가 대두된다. ④ 컴퓨터를 사용할 줄 모르는 집단의 상대적 박탈감이나 인간 소외 문제가 발생한다. ⑤ 정보의 독점 및 소외로 인한 문화 지체 현상이나 다른 나라의 문화에 대한 문화 종속 등의 문제가 대두된다. ⑥ 너무 많은 정보가 쏟아져 나옴으로써 유효한 정보를 더욱 더 얻기 힘든 문제가 발생한다. ⑦ 컴퓨터를 이용한 신종 문제가 발생한다. ⑧ 유언비어나 음란물과 같은 불건전 정보가 빠른 시간 내에 폭넓게 유포된다. ⑨ 잘못된 정보의 광범위한 유포나 국가 기간 네트워크 망의 이상으로 인한 사회적인 혼란이 발생할 수 있다. ⑩ VDT(visual disply terminal) 증후군과 같은 신종 직업병이 발생한다.

"우리나라에서는 1971년 대구의 미군기지 컴퓨터 센터에서 일하는 Y등 일단의 한국인들이 연간 약 1천 7백만불어치의 미군 보급물품을 컴퓨터를 이용하여 빼돌린 사건이 공식적인 컴퓨터 범죄의 최초로 보고 되었다. 이들은 컴퓨터를 통해 훔쳐가기 용이한 시간과 장소로 원하는 물품을 옮겨 놓도록 지시하고 물건을 빼돌린 후에는 컴퓨터에 수록된 기록을 모두 지워 버려서 이 물품들에 대한 자취를 남기지 않았다. 수년에 걸친 피해액은 1억불에 이르러 당시 대구에서는 미군들이 긴급한 부품의 조달을 한국 암시장에 의존할 정도였다. 이 범죄수법은 그 당시에도 이미 잘 알려진 수법이었는데 미군 사령관 Baird장군이 이 사건에 대한 상세한 보고서를 작성, 미상원 청문회에 보고함으로써 이 사건은 이런 종류의 컴퓨터범죄 중 최초로 상세한 보고서가 작성된 사건이 되었다."[20]

최근에 우리는 정보화의 세계적인 추세에 따라서 우리나라도 정보화가 가속화되고 있다. 예를 들면[21] 서울시민 10명 가운데 6명이 컴퓨터를 사용하고 있으며 시민의 절반 가량은 인터넷을 이용하고 있는 것으로 나타났다. 또 인터넷 이용 시간은 하루 1시간18분으로 조사됐다. TV시청 시간은 2시간30분 안팎이다. 이같은 사실은 서울시가 2000년 5월에 실시한 15-64세의 시민 1천5백명을 대상으로 벌인 설문조사에서 밝혀졌다. 이에 따르면 인터넷 이용 시민은 47%로, 이 가운데 71%는 전자우편(e-메일)을 보유하고 있으나 인터넷 쇼핑몰 이용경험(18%)은 비교적 낮았다. 컴퓨터 이용 장소는 가정(45%)이 가장 많았고 ▶PC방(24%) ▶직장(16%)▶학교(10%)순이었으며 인터넷 이용 장소도 비슷한 분포였다. 또 시민들은 사설 학원(38%)에서 주로 컴퓨터 교육을 받고 있어 학교와 직장, 공공기관의 컴퓨터 교육이 더 확대돼야 할 것으로 분석됐다. 컴퓨터 교육을 받지 못한 시민들의 74%가 교육을 희망하고 있으며 무료교육 시설의 확대를 요구했다. 이밖에 조사 대상자의 77%가 가정에 컴퓨터를 보

---

20) 김세헌, 『컴퓨터범죄와 프라이버시침해』, 서울: 희성출판사, 1989, p.40.

21) 이 자료는 서울특별시가 2000년 5월에 실시한 여론조사 결과이다. 자세한 것은 다음의 참고문헌을 참조할 것.
서울특별시, 『정보화에 대한 서울시민 여론조사』 (서울: 서울특별시정보화기획실, 2000). pp.1-244.

유하고 있었고 컴퓨터가 없는 가정의 79%가 컴퓨터 구입 의사를 밝혔다. 한편 시민들은 정보화를 연상시키는 매체(중복 응답)로 ▶인터넷과 PC통신(61%)▶컴퓨터(59%)▶TV(34%)▶신문(16%)을 꼽았다. 정보화는 인간의 삶의 질을 향상시켜 나가는데 절대적으로 필요한 요건이 되고 있다. 그러나 이와 반대로 정보화가 주는 엄청난 역기능은 바로 몰 인간성, 획일성, 비윤리성, 그리고 정보의 오용과 남용, 그리고 정보의 공해(pollusion)로 인한 가상공간에서 혹은 실제공간에서의 새로운 부패의 증대 등을 지적 할 수 있다. 따라서 우리는 미래 행정발전의 초점이 될 가상공간의 극대화가 가져 올 역기능 문제를 심층 깊게 다루는 반부패의 새로운 전략이 시급하다.

Ⅳ. 사이버 부패의 유형

사이버부패의 실태를 보면 비도덕적인 부패현상의 것과 재물의 이득을 취하는 경우가 있다. 먼저 비도덕적인 경우를 보면 다음과 같다.

첫째, 사이버 매매춘의 경우이다.

사이버 매매춘이란 가상공간을 이용하여 매춘의 의사를 담은 메시지를 띄워 매매춘을 가능하게 하는 모든 행위를 의미한다. 특히 최근 들어 화상채팅이 가능해짐에 따라 사이버 매매춘이 더욱 기승을 부릴 것으로 추정되고 있다. 최근 물의를 빚고 있는 원조교제는 시작의 단계에서 매매춘을 알선하는 인터넷 사이트나 개인간의 채팅을 통해 매매춘에 대한 서로의 의사를 타진하는 형태로 이루어지고 있는 경우가 많다. 사이버 매매춘의 대표적인 유형으로는 게시판이나 대화방을 중심으로 이루어지는 독립적인 매매춘과 국외의 서버를 이용하여 인터넷 매매춘 사이트를 개설하여 매춘 알선을 주도하는 기업적인 매매춘의 형태가 대표적이다. '99년도 말 검찰이 원조교제를 단속한 결과 검거된 10대 청소년의 90%가 사이버 매매춘을 통해 원조교제의 대상자와 접촉을 하였던 것으로 나타나 사이버 매매춘에 대한 경각심을 불러 일으키고 있다. 특히 최근 들어 인터넷 상의 익명성을 이용하여 전문적으로 매매춘을 알선하는 기업형 조직들이 나타나고 있어 산업사회의 윤락가가 사이버 상에 등장하는 형태로 발전되고 있어 사이버 매매춘은 앞으로 더욱 증가할 가능성이 있다.

사이버 매매춘의 피해자가 상당수 청소년일 가능성이 있다는 점을 주목할 필요가 있다. 청소년들은 쉽게 통신 이용이 가능한 환경 속에 있으며 동시에 외부로부터 소비·향락 지향적인 문화에 자극을 받음으로써 쉽게 매매춘의 함정에 빠져들 위험성을 안고 있다. 현재 사이버 매매춘을 방지하기 위하여 제도적으로 뒷받침된 감시요원이 적다고 하는 사실과 사회도처에 만연한 왜곡된 성문화가 청소년들을 사이버 매매춘의 피해자로 몰아가는 상황을 가속화시키고 있다고 하겠다.

둘째, 사이버 사기 [22]의 사이버부패이다.

---

22) 자세한 것은 다음을 참고할것
http://ict.use.go.kr/attach/classhome/6/L26/tict2/tict208.htm

사이버사기란 컴퓨터 통신망 또는 인터넷을 이용하여 이용자들에게 물품이나 용역을 제공할 것처럼 기만하는 메시지를 보내어 금품 등을 탈취하는 행위를 의미한다. 인터넷을 이용한 전자상거래가 활성화되면서 앞으로 통신을 이용한 사기 행위는 다양한 형태로 진행될 것으로 예상된다. 인터넷 사기의 가장 대표적인 예로는 인터넷 경매 사기가 있다. 인터넷 경매 사기란 물건값을 올리기 위해 거짓정보를 유포시키거나, 낙찰이 된 물건을 배달하지 않는 것을 의미한다. 미국의 경우 1997년 인터넷 피해관련 신고에 있어 사기관련 신고가 전체의 26%를 차지하였으나, 1998년에는 68%로 증가하여 앞으로 인터넷 관련 사기의 피해가 속출될 것으로 전망되고 있다.

사이버 사기부패의 현황을 보면 국내의 경우 전자상거래가 크게 활성화되지 못하였기 때문에 아직까지 통신판매를 통한 사기의 사례 수와 규모가 정확히 밝혀지지 않고 있다. 정보통신윤리위원회가 인지하여 시정을 요구한 인터넷 관련 사기 영업 행위는 '99년 상반기 중 244건으로 대부분 '6천원으로 8억을 버는 법' 등과 같은 허위광고를 통해 자행된 통신 피라미드 영업행위인 것으로 나타나고 있다.

〈표 3〉 최근 3년간 미국의 인터넷 사기 현황

순위	1996년	1997년	1998년
1	피라미드/다단계 판매	온라인 서비스	인터넷 경매
2	사업기회 및 독점권	일반상품 판매 사기	일반상품 판매 사기
3	하드/소프트웨어 판매	인터넷 경매	하드/소프트웨어 판매
4	온라인 서비스	피라미드/다단계 판매	온라인 서비스
5	재택근무 사기	사업기회 및 독점권	재택근무 사기
6	회원권 사기	재택근무 사기	사업기회 및 독점권
7	잡지	상품 및 경품	피라미드/다단계 판매
8	광고	신용카드 발급	신용카드 발급
9	장학금 사기	도서	선수수료 대부

출처 : 정보통신부, 「정보화역기능방지종합대책(안)」, 1999, 재구성

따라서 국내에서 발견되는 인터넷을 통한 통신사기는 허위광고를 통한 사기행위에 국한되고 있으나 향후 피해는 <표 3> 에 나타나는 미국의 인터넷 사기현황과 비슷한 유형으로

다양하게 나타날 가능성이 높다. 특히 1999년 6월 현재 국내에는 약 800여 개의 인터넷 쇼핑몰이 운영 중에 있으며, 1998년 매출 총액은 152억 2천만원에 달하는 것으로 나타나고 있어 인터넷을 통한 전자상거래가 증가하면 할수록 인터넷 사기에 대한 피해도 증가할 것으로 예측되고 있다.

우리나라에서 전자상거래는 1995년 도입되었다. 처음에는 전자상거래 업체의 규모나 매출이 영세하고 사용인구가 적어 피해사례 발생건수 및 피해규모가 적은 편이었으나 최근 인터넷 사용인구의 폭발적 증가와 발생건수와 피해규모가 급증하고 있다. 국경을 초월하여 사기행위가 이루어지고 있다. 피해유형은 주로 PC통신사기판매 및 해킹 등이 있는데 일반적인 피해유형을 분류해 보면 다음과 같다.[23]:

① 인터넷 경매 낙찰이 되어도 물건이 배달되지 않거나, 물건값을 부풀리기 위해 고액의 허위 응찰을 하여 바람을 잡는 행위. ② 일반상품 판매 광고내용과 다른 상품이 배달되는 경우 ③ 인터넷 서비스가 무료인 것처럼 가장하여 사용을 유도한 후 비용을 청구하거나 제공되지 않은 서비스에 대해 비용을 청구하는 경우. ④ 피라미드 및 다단계 판매 상품 및 서비스 판매가 아닌 회원을 끌어들임으로써 영리를 취하는 행위 ⑤ 신용카드 불법유용으로 카드번호와 유효기간만 입력하면 결제 가능한 허점을 악용, 타인의 카드정보를 이용하여 인터넷상에서 물품을 구매하는 경우

셋째, 전자상거래를 이용한 포르노물 유통[24]의 경우이다.

포르노물은 다양하게 그 정의를 다르게 내릴 수 있다. 특히 청소년들의 경우 포르노정보로 인식되는 폭은 대단히 넓고도 다양하다. 음란물로 인식하는 정보는 연령과 인식의 차이에 따라 매우 다양하다. 그러나 대체로 음란정보라 함은 여성과 남성의 성 관계가 지나치게 직접적이며, 노골적으로 표현된 정보를 의미한다. 이러한 음란정보는 성에 대해 나름대로의 분별력을 지니고 있는 성인들에게는 큰 문제가 되지 않을 수도 있다. 그러나 성에 대해 분별력을 갖추기 시작하여야 할 청소년기에 음란정보가 청소년들에게 미치는 영향은 대단히 크다. 특히 성에 대한 논의가 음성적으로 이루어지는 한국사회에서 올바른 성교육을 제대로 받지 못한 채 음란정보에 접하게 될 때 청소년들은 성에 대한 왜곡된 인식을 가지게 됨으로써 성인이 되었을 때 성과 관련된 많은 문제를 야기할 가능성이 있다. 따라서 성 관련 정보는 청소년기에 매우 선별적이고 체계적으로 제공되는 것이 바람직하다. 그럼에도 불구하고 인터넷과 같은 정보통신기술의 발달은 청소년들로 하여금 음란정보에 접촉할 수 있는 기회를 용이하게 함으로써 청소년기의 성 관련 범죄를 증가시키는 직접적인 영향을 초래하기도 한다. 또한 성에 대한 책임감보다는 성은 단지 쾌락을 위한 행동이라는 오도된 인식을 갖게 만들 수 있다.

---

23) http://www.npa.go.kr/ctrc/ctrc_04.htm

24) 자세한 것은 다음을 참조할 것
http://ict.use.go.kr/attach/classhome/6/L26/tict2/tict202.htm

포르노의 종류는 정보 통신 기술의 발달로 인해 다양한 방식으로 제작이 가능하기 때문에 여러 가지 형태로 제작될 수 있다. 인터넷상에서 구할 수 있는 음란정보를 다운 받아 복사하여 판매하는 경우도 있으며, 이를 또한 인터넷을 통해 다시 업로드시키거나 다운 받아 유통시키는 경우도 많다.

최근 들어 성인들을 위한 음란물 사이트들이 급속히 늘어나 인터넷을 통한 음란물 접촉이 거의 대중화되었다. 물론 이들 사이트들은 미성년자들의 접속을 막기 위해 접속하는 사람의 신용카드 번호를 입력하거나 하는 방법 등을 사용함으로써 성인들만이 접속할 수 있게 하고는 있으나, 접속을 유도하는 안내 광고가 이미 음란물이어서 접속의 유무를 떠나 이미 음란물을 청소년들에게 제공하고 있는 상황이기도 하다.

정보통신윤리위원회가 1998년 실시한 음란물 접촉실태에 관한 연구에 따르면 PC 통신을 통한 청소년들의 음란물 접촉 실태는 전체의 38.6%인 것으로 나타나 청소년 10명당 4명 정도가 PC를 통해 음란물에 접촉되고 있는 것으로 나타나고 있다. 그러나 이러한 조사 결과는 PC를 보유하고 있지 않은 청소년들도 포함되어 있기 때문에 PC를 보유하고 있는 청소년들의 실제 음란물 접촉비율은 이 보다 높을 것으로 추정된다. 청소년들의 음란물 접촉이 증가할 수밖에 없는 이유로는 인터넷의 일반적인 보급에 의해 인터넷을 통한 음란물 접촉이 별다른 차단장치 없이 거의 무방비로 공개된다는 데에서 비롯된다. 청소년보호위원회에 대한 정무위 국감에서 지난해 2000. 1-2001. 8월말까지 국내 4대 PC통신업체에 접수된 음란대화 음란물유통 등에 관한 신고건수가 모두 20만8410건에 이른다. 대응책으로서 청소년들의 음란물 접촉을 방지하기 위한 차단 프로그램이 개발되어 보급되고 있다.[25] 법적·제도적 대응으로서 정보통신윤리위원회를 설치하여 모니터링을 강화하고 있다.[26] 최근 들어 인터넷 내용 등급제를 실시함으로써 불건전 정보로부터 청소년들을 보호하는 제도적 장치가 논의되고 있다. 검찰은 컴퓨터통신회사·PC동우회·학부모 등 자원봉사자 등으로 '민간자율감시단'을 만들고 정보통신윤리위원회·청소년보호위원회·시민단체등과 협조해 컴퓨터를 통해 음란물을 유통시키는 사람을 발견하면 '전담수사반'에 통보하도록 하는 한편 각 검찰청·경찰서에 신고전화 및 '컴퓨터범죄신고창구'를 만들기로 했다.

또한 각급 학교에 인터넷 사용을 위한 전산망이 보급됨에 따라 학교에서도 인터넷을 통해 유해한 정보에 접촉할 수 있는 가능성이 증가하고 있다. 최근 조사한 결과에 따르면 학교에 불건전 정보 차단 프로그램이 설치되어 있는 비율은 1.7%인 것으로 나타나고 있어 학교에서의 음란물의 접촉이 의외로 높게 나타날 가능성을 보이고 있다. 또한 <표 4>에서 보

25) 이차단 프로그램은 1997년 정보통신윤리위원회의 요청으로 한국전산원에서 개발한 PC용 불건전 정보 차단 프로그램인 NCA Patrol 1.0을 시작으로 현재 약 20가지 정도의 PC 용 차단 프로그램이 시판되고 있으며, 서버용 프로그램도 개발되어 보급되고 있다. 그러나 한국청소년문화연구소가 실시한 불건전 정보차단 소프트웨어 평가대회를 통해 이들 차단 소프트웨어의 차단 능력은 60~70% 정도인 것으로 나타나고 있어 앞으로 차단 프로그램의 기술 향상 및 유해사이트 목록의 지속적인 갱신이 상당히 필요하다는 사실이 밝혀졌다.

26) 예컨대 음란정보 유통행위에 대한 처벌을 위해 전기통신기본법과 전기통신사업법, 그리고 특히 청소년을 대상으로 한 음란정보의 유통행위를 처벌하기 위해 청소년보호법 등을 제정하여 시행하고 있다

는 바와 같이 학교 컴퓨터실에서도 음란물 접촉이 얼마든지 가능한 실정이다.[27] 1999년 6월 22일 경찰청 사이버범죄수사대는 전자우편이나 PC통신 게시판을 이용하던 방식에서 벗어나 전자상거래 방식을 이용한 음란·불법물 판매사범 2명을 검거하여 구속하였다. 이들은 홈페이지를 개설하고 600여장의 포르노 사진과 '빨간 마후라', 'LA아리랑' 등 유명 몰래카메라, 음란 비디오, 게임, 상용 프로그램 등 300여 프로그램을 1998년 7월부터 1999년 6월까지 11개월 동안 판매하여 1억여원의 부당이득을 취한 혐의이다.[28]

〈표 4〉 포르노 발견 학교수

구 분	포르노발견 학교 수	비율(%)
초등학교(12)	3	25
남녀공학중학교(10)	2	20
남자중학교(7)	3	42.9
여자중학교(4)	1	25
남녀공학중학교(11)	4	36.4
남자고등학교(9)	6	66.7
여자고등학교(7)	1	14.3
합계	20	33.3

자료: 어기준, 『학교컴퓨터실의 음란물 접촉 실태조사연구』, 한국 컴퓨터생활연구소, 1999. pp.1-20.

넷째, 정보통신망 이용 명예훼손을 하거나 거짓정보를 유출하여 피해를 주는 경우이다.

명예훼손이란 공연히 사실 또는 허위의 사실을 적시하여 사람의 명예를 훼손하는 것을 말한다(형법 307조). 최근 PC통신이나 인터넷 사이트를 통해 허위사실 유포나 명예훼손이 이루어지는 경우가 많다. 대개 통신망의 게시판, 토론방, 대화방 등이 이용된다. 통신망에서의 명예훼손은 아무런 여과 없이 직접 글을 올릴 수 있어 불특정 다수인에게 전파성이 강하고, 증거보전이 어렵다. 미국, 영국 등은 정보통신망 이용 명예훼손을 방지하기 위해 명예훼손법을 제정하였고, 각 나라들도 법률 제정에 논의가 이루어지고 있다. 통신상에서 자신의 신분이 나타나지 않는다는 사실을 이용하여 거짓정보를 유통하는 것은 바람직한 사회 건설에 커다란 지장을 초래한다. 거짓정보를 퍼뜨리는 경우는 거짓정보를 사실로 믿고 퍼뜨리는 경우도 있으며, 고의로 남을 골탕 먹이기 위해 퍼뜨리는 경우도 있다. 두 경우 모두 거짓정보를 유통시킴으로 해서 서로가 서로를 믿지 못하는 분위기를 만들게 됨으로써 신뢰할 수 없는 사회를 만든다고 하는 것에서는 차이가 없다. 개인정보란 성명, 주민등록번호 등에 의

27) 어기준, 『학교컴퓨터실의 음란물 접촉 실태조사연구』, 한국 컴퓨터생활연구소, 1999.

28) http://my.netian.com/~hahyoung/anti_tech.htm

해서 개인을 식별할 수 있는 정보를 말한다. 예컨대 메일 폭탄 즉 메일시스템이 감당하기 어려울 정도로 덩치 큰 자료를 단시간 내에 무수히 반복하도록 특별한 명령들을 사용해서 메일을 보냄으로써 시스템에 과부하가 걸려 결국 시스템이 다운되게 하는 것이다.

정보사회에서는 정보통신 기술의 발달로 인해 개인에 관련된 여러 가지의 정보(성별, 주소, 나이, 재산정도, 학력정도, 취미 등)들이 전자기록으로 컴퓨터 속에 저장되어 보관되기 때문에 관리하기 쉬운 장점이 있는 반면에 컴퓨터에 접근할 수 있는 사람들이나 해커들에 의해서 개인 정보가 쉽게 노출될 수 있는 위험성이 있다. 우리는 우리 자신의 정보는 물론 타인의 정보도 우리 자신의 정보와 마찬가지로 중요하다는 것을 깨닫고 타인의 정보를 보호하기 위해서 노력해야 한다. 아울러 우리는 우리 자신의 개인 정보가 함부로 유출되지 않도록 주의를 기울여야 한다.

다섯째, 금융사기 유형이다.

한국의 경우 40억원대 인터넷 공모주 사기사범[29]의 사례를 들 수 있다. 2000년 9월 29일, 유령회사홈페이지를 개설하여 거액의 공모주 사기행각을 벌인 崔想汶(가명, 22, 관악구 신림동)을 검거 구속영장을 신청했다. 피의자는 올해 초 벤처투자 붐으로 단순한 인터넷공모주 모집광고만으로도 많은 투자자금을 끌어 모을 수 있다는 점에 착안, 2000년 6월 (주)웹존시스템(http://webzone.com.ne.kr)이라는 유령 인터넷회사 홈페이지를 만들어 2000년 하반기 코스닥에 등록할 예정으로 총 5억원의 주식을 공모한다는 내용으로 광고를 내고 이를 유명 증권관련 정보제공 홈페이지와 연결시켜 소액투자자들을 끌어 모으는 등 5월부터 8월까지 총 5개 홈페이지를 개설, 40억원대의 인터넷 공모주 사기행각을 벌여왔으며 경찰은 추가범행에 대해서 여죄를 조사 중이다. 한편 피의자는 현행 제도상 10억원 미만의 공모주 청약의 경우 특별한 신고절차 없이도 시행할 수 있고 투자자들도 광고내용에 대한 정확한 사실확인 없이 손실에 대한 위험을 감수한 채 수십 내지 수백만원의 분산투자를 하여 비교적 문제제기 사례가 적다는 점을 악용하였으며 실제로 각각의 홈페이지에서 10일내외의 짧은 기간을 통해 공모한 결과 60여명의 피해자로부터 6,000여만원의 부당이득을 취한 것으로 나타났음.

여섯째, 바이러스사범의 경우도 사이버부패에 해당된다.

세계 최초의 바이러스사범 검거[30]의 경우이다. 컴퓨터바이러스란 컴퓨터를 동작시키는 기본소프트웨어에 몰래 침투, 사용자의 프로그램 및 입력된 정보를 망가뜨리거나 컴퓨터시스템의 기능을 물리적으로 파괴하여 운용을 방해하는 불법프로그램을 말한다. 컴퓨터 바이러스 프로그램의 유포는 상상할 수 없을 정도의 많은 사람에게 막대한 양의 피해를 미칠 수 있다. 컴퓨터가 바이러스에 한 번 감염되어 고장이 날 경우 원 상태로 돌아가기 위한 시스템 복구작업에 따르는 경제적인 손실은 대단히 크다. 따라서 컴퓨터 바이러스 프로그램의 유포는 개인과 국가에 경제적으로 막대한 손실을 끼칠 수 있는 잘못된 행동이며 범죄행위이다. 근래 들어 바이러스처럼 보이는 유사바이러스 '조크(Joke) 프로그램'과 존재하지 않는 바

29) http://www.npa.go.kr/ctrc/ctrc_03.htm

30) http://www.npa.go.kr/introduction/policeact/page_140_2.html

이러스를 조심하라는 장난편지 '혹스(Hoax)' 등이 있는데, 이 프로그램들은 시스템에 문제를 일으키지는 않지만 바이러스로 오인하게 하는 증상을 나타나게 함으로써 사용자들에게 혼란을 주는 프로그램이다.

경찰청 사이버범죄수사대는 1998년 2월 인터넷 상에서 CVC(Corean Virus Club)라 는 이름으로 한국을 대표하는 바이러스 제작 그룹으로 활동하며, 악성 바이러스를 제작·유포한 혐의로 서모군(13)등 4명을 검거하였다. 이들이 만들어 유포시킨 바이러스는 안철수 바이러스 연구소에 의해 최대 악성 바이러스 10종으로 밝혀진 FCL 바이러스, 율곡 바이러스 등이다. 이들 바이러스는 여러 단계의 암호화와 고도의 자체 수정 기법 등을 동원하여 바이러스 발견, 분석 및 치료를 어렵게 하여 광범위한 피해를 입혔다. 더 나아가 국경과 지역 개념이 없는 사이버공간의 특성을 고려한 종합적 대응체제를 구축하고, 사이버테러의 위험성 및 암호의 부정이용에 대비한 장기대책 마련 및 사이버순찰, 사이버범죄 피해 방지대책 수립 등 예방적 활동을 강화하기 위해 1999년 12월 23일 25명의 전문 수사요원으로 구성된 '사이버범죄수사대'를 출범하여 종합적인 사이버치안체제를 구축하고 다각적인 활동을 전개하고 있다.

일곱째, 해킹(hacking), 핵티비즘(hacktivism)의 경우이다.

해킹은 실제공간에서는 절도에 해당하고 호주의 New South Wales 주의 부패방지위원법(ICAC, Independent Commission Againt Corruption Act)제8조에서의 실제공간에서의 부패의 개념에 해당한다.[31] 이것은 컴퓨터범죄에도 해당되나 이미 논의한 바와 같이 보다 넓은 의미의 가상공간의 부패에 해당한다. 해킹을 하는 사람들은 자기가 하는 행위의 범죄적 성격을 이해하지 못하고, 해킹이 마치 자신의 컴퓨터 작동기술을 과시하는 것으로 잘못 생각하고 범죄를 저지르는 경향이 있다. 아무런 생각 없이 해킹을 저지르는 해커들은 자신의 행동에 대한 법적인 처리를 받게될 뿐만 아니라 자신이 훔친 정보로 자신의 이웃을 포함한 여러 사람에게 피해를 줄 수 있는 행동을 함으로써 결과적으로 자신에게도 피해가 돌아가게 된다. 핵티비즘이란 '해커(hacker)'와 행동주의를 뜻하는 '액티비즘(activism)'의 합성어로 급진적인 정치·사회적 목적을 달성하기 위한 컴퓨터 해킹을 말한다. 자기 과시용 파괴나 신용카드 번호를 훔치는데 그쳤던 해킹과는 목적이 다르다. 정치적 목적이나 종교적 목적으로 정치적 이념이나 사상이 서로 다른 국가의 정부기관에 해커들이 침투하여 정보망을 교란시키거나 마비시키는 행위를 가리킨다. 해킹의 경우 다음과 같은 사례를 들 수 있다[32]

"회사원 모(25)씨는 얼마 전부터 모르는 사이트에서 회원을 대상으로 보내는 메일이 자신에게 계속

---

31) ICAC 에서는 부패행위를 포괄적으로 다루고 있다. 즉 독직(official misconduct), 뇌물(bribery), 사기(fraud), 절도(theft), 횡령(embezzlement), 선거뇌물(election bribery), 세금포탈(tax evasion), 불법마약거래(illegal drug dealings), 불법도박(illigal gambling), 기업위반(company violations), 폭력(violation) 등이 포함된다. 자세한 것은 다음의 문헌을 참고할 것
김영종, "감사원의 은행계좌추적: 부패학적 접근을 중심으로", 감사원법 개정안 관련자료집 (서울: 감사원, 1993), pp.103-120.

32) 중앙일보, 2000. 7. 20.

날아오는 것을 의아하게 생각, 경찰에 신고했다. 경찰수사결과 씨의 이름으로 경품 사이트에 가입한 사람은 K대 전자계산학과 3학년 이모(23)군. 이군은 군씨의 주민등록번호 등 기본 신상 자료는 물론 ID·비밀번호·증권계좌번호·증권거래성향 등의 정보까지 갖고 있었다. 친구가 다니는 증권정보 제공업체 서버에서 5만명의 개인 정보를 자신의 PC에서 다운받아 보관해 왔다는 것이다. 이군은 이중 9백여명의 신상정보를 이용해 경품 사이트에 등록, 70만원어치의 상품을 챙겨온 것으로 드러났다.

인터넷이 급속도로 확산되고 있는 가운데 사이버 공간의 허술한 보안 때문에 개인의 신상 정보들이 무방비 상태로 유출되고 있다. 벤처회사를 운영했던 명문대 휴학생 최모(24)씨는 얼마 전 초등학교 동창회 홈페이지를 개설했다. 최씨는 홈페이지에 등록한 동창생 중 모 정보시스템사에 다니는 A씨(24·여)의 접속주소(IP)를 역추적했다. 최씨는 A씨의 회사시스템에 인터넷으로 침입, 11만명 고객의 근무지·직책·전화번호 등의 정보를 빼왔다. 네트워크 기술의 발달로 회사내 모든 컴퓨터 자료가 공유되고 있는 허점을 악용한 것이다. 최씨는 인터넷에 이 정보를 5백만원씩 팔기 위해 e-메일 광고를 냈다가 경찰에 붙들렸다. 경찰청은 19일 최씨를 정보통신망 이용촉진 등에 관한 법률위반 혐의로 구속하고 이씨에 대해 같은 혐의로 구속영장을 신청했다."

여덟째, 재산권 침해이다.

컴퓨터 프로그램은 최초로 만든 이에게만 그 프로그램에 대한 소유가 인정되고 그 프로그램을 팔아 얻어지는 모든 수익에 대한 권리를 인정한다. 이것을 바로 '지적 소유권'이라고 한다. 따라서 다른 사람이 만든 컴퓨터 프로그램을 사용하고자 할 경우에는 지적 소유권을 소유한 사람의 승인이 있어야만 사용할 수 있게 된다.

정품의 소프트웨어를 구입하지 않고 남이 사용하는 소프트웨어를 몰래 복사하여 사용할 경우 지적 소유권을 가진 사람의 물건을 몰래 훔쳐 사용하는 범죄를 저지르는 것이 된다. 그리고 대다수의 사람들이 정품 소프트웨어를 사용하지 않고 불법 복제 소프트웨어를 사용한다면, 아무도 소프트웨어를 개발하려고 하지 않을 것이고, 그렇게 되면 우리 나라의 소프트웨어 산업은 발전할 수 없을 것이며, 그 만큼 정보사회의 발전도 지체될 것이다.

아홉째, 무단 광고(spam)이다.

무단 광고(spam)은 뉴즈넷 spam과 메일상의 spam으로 나뉜다. 이들 무단 광고(spam)의 대부분은 음란사이트의 선전이나 특정제품의 광고 및 홍보 등을 목적으로 하고 있으며, 무단 광고(spam)을 보내는 spammer들은 인터넷상의 메일링리스트를 가로채거나 뉴즈넷에 포스팅되는 헤더를 스캔하는 방법 등으로 예비고객 명단을 확보한 후 뉴즈넷 뉴스그룹과 인터넷 메일사용자를 대상으로 무분별하게 기사를 포스팅하거나 메일보내고 있다. 이들이 합법적인 메일링리스트 개설등의 방법을 통하지 않고 이러한 편법을 사용하는 것은 이런 무단 광고(spam)의 대부분은 내용면에서 불법성이나 사기성을 띠기 때문이다. 흥미있는 것은 최근에 스팸메일에 대한 인격권침해로 인한 처벌을 주고 있음은 바로 사이버부패의 통제가 이제 본격적으로 이루어진 사례로 본다. 구체적인 살케는 다음과 같다:[33]

"서울지법 동부지원 민사31단독 이 혁 판사는 21일 스팸메일로 정신적 피해를 입었다며 조모씨가 e-메일 발송업체들을 상대로 낸 손해배상 청구소송에서 원고 일부 승소 판결을 내렸다. 재판부는 "수신

33) http://www.msn.co.kr/exredir.asp?STARTID=news_breaking&adgroup=KRMNWG&URL=http://www.joins.com/news/2002/01/21/all/20020121094811104146.html

거부 의사를 분명히 했는데도 계속 메일을 보낸 것은 원고에 대한 인격권 침해에 해당된다"며 "광고메일 발송업체는 조씨에게 78만원을 배상하라"고 판시했다. 재판부는 "발신전용 메일주소를 사용한 업체들이 원고의 수신거부 의사표시를 받지 못했다고 주장하고 있으나 이 또한 회사측 책임이다"며 "그러나 수신거부 의사표시 이전에 발송된 메일에 대해서는 피해를 인정할 수 없다"고 밝혔다. 조씨는 지난해 11월 자신의 e-메일 주소로 5-8건의 광고성 e-메일을 보낸 4개 회사에 대해 메일 수신 거부의사를 표시하고 정보통신부에 신고를 했는데도 메일이 계속 들어오자 이들 업체를 상대로 소송을 냈다. 정부가 스팸메일 발송자를 처벌키로 한데 이어 개인의 정신적 피해에 대한 배상판결까지 나옴에 따라 메일을 주요 홍보수단으로 사용하는 인터넷 업계에 파장이 예상된다."

V. 사이버부패의 대응: 행정 윤리적 접근

1. 주요국의 대응전략

사이버부패나 사이버범죄에 대한 세계주요국의 대응은 매우 활발하다. 그러나 엄격하게 말하여 사이버부패에 대한 대비책은 거의 전무한 실정이다. 그러나 이미 논의한 바와 같이 컴퓨터범죄는 사이버부패의 일부분이므로 여기에서는 이미 이루어진 사이버범죄에 대하여 미국, 일본, 영국, 그리고 기타 주요국의 순서대로 논의하고 다음장에서 사이버부패를 탐색적으로 연구한 결과를 제시한다.

첫째, 미국의 경우이다. 미국내에서는 사이버 범죄에 대해 대응하고 있는 기관은 FBI의 NIPC (National Infrastructure Protection Center), OSI(Office Specific Investigation, 공군범죄수사대), USSS(United State Security Service, 재무부소속) 등 국가기관과 CERT (Computer Emergency Response Team, 침해사고대응팀) 등 민간기관에서 다양하게 활동하고 있지만 그 중의 대표적인 것은 연방수사기관인 FBI의 NIPC이다. NIPC는 특히 국가 주요 전산망에 대한 해킹 사고에 대한 예방, 수사, 수사요원 교육 등의 임무를 지니고 있으며 '98년에 설립되었다. 원래 FBI는 '96년부터 CITAC(Computer Investigations and Insfrastructure Threat Assesment Center)를 설립, 컴퓨터 범죄수사업무를 담당해 왔으나 '97년 대통령 특별위원회 발간 보고서에서 NIPC설립이 제안되었고, '98년에 설립, 국가의 주요기반 전산망에 대한 사이버적 공격으로부터 보호 임무를 받아 활동 중에 있다. 인원은 현재 본부에만 140여명이상의 컴퓨터전문가로 구성되어 있으며 컴퓨터조사·활동반, 분석·경고반, 훈련·관리·지부운영반 등 3개반으로 구성되어 있고 국가의 주요기반 진산망에 대한 예방, 사후 조사, 수사관들에 대한 지원, 교육업무를 담당하고 있다. 또한 워싱턴, 뉴욕, 샌프란시스코, 달라스, 보스톤, LA, 시카고 등에 지역사무소를 개설하고 지역 컴퓨터범죄수사반을 운영하고 있으며 계속 확대해 나갈 예정에 있다. 나아가 민·관기관을 회원으로 하여 협조, 대응체제도 구축하고 있다.

둘째, 일본의 경우이다. 일본은 지난 80년대부터 컴퓨터범죄에 관심을 가지고 대응해 왔으

나 부분적이었다. 경찰청이나 각 지방경찰에서 컴퓨터전문가를 경찰관으로 특채하여 컴퓨터 범죄수사관으로 활용하는 수준이었고 컴퓨터범죄수사만을 전담하는 독자적 기구는 없었다. 그러나 일본은 경찰청에서 주도적으로 관련 범죄에 대응하여 '99년 들어 혁신적인 대응책을 마련하여 시행하고 있다. '99년 4월에는 경찰청에 하이테크 범죄에 대응하기 위해 40여명의 전문컴퓨터기술자들로 『기술대책과(Hitech Crime Technology Division)』를 신설하여 하이테크 범죄와 관련된 수사기법 교육, 증거수집·분석 및 도도부현 경찰의 범죄수사시 직접지원 등의 업무를 맡고 있으며, 동경경시청에서도 '99년 5월 경시청 부총감을 본부장으로 『하이테크범죄종합대책본부』를 설치하고 경시(경정급)를 하이테크범죄대책관으로 하여 『하이테크범죄대책센터』를 신설하였다. 하이테크범죄대책센터는 60여명의 컴퓨터전문가와 수사요원으로 구성되어 있으며 중요사건에 대한 직접수사, 일선 경찰서 수사지원 및 사이버 공간에 대한 24시간 검색활동체제를 구축하고 활동 중에 있다.

셋째, 영국의 경우이다. 영국은 런던 경시청에 컴퓨터범죄수사과가 설치되어 있어 관련범죄에 대응하고 있다. 그러나 최근 내무성 산하의 국가경찰기구인 국가형사정보국에서는 사이버 범죄에 대응하는 조직은 중앙수사기관에 두는 것이 가장 효율적이라는 보고서를 내고 "사이버범죄수사대"를 설립하는 것을 추진하고 있다.

넷째, 선진 8개국의 협력 대응이다. 선진국가에서는 이미 사이버 범죄에 대한 대응이 국경을 넘어서는 국제적인 협력이 없이는 불가능하다는 사실을 인식하였다. 이에 '97년 12월 선진 8개국은 법무·내무장관 회의를 개최하면서 정보통신의 비약적 발달로 인한 하이테크 범죄를 규정하고 이를 이용하는 범죄에 대응하는 공식발표문을 발표하고 그 부록에서는 하이테크 범죄에 대처하기 위한 원칙과 행동계획을 선언하였는데 이 내용은 우리나라에서 소위 하이테크 범죄에 대응하기 위한 기준이 되는 참고자료로 보아도 될 것이다. 구체적 내용을 보면 다음과 같다. ① 정보범죄를 남용하는 사람에게는 절대로 안전한 도피처가 있어서는 안 된다. ② 국제적인 하이테크 범죄의 수사와 기소는 피해발생지에 관계없이 모든 관련국가들간에 조화롭게 처리되어야 한다. ③ 수사요원(법집행요원)은 하이테크 범죄를 다루기 위해 교육훈련을 받고 지식을 갖추어야 한다. ④ 법체계가 불법적인 훼손으로부터 데이터와 시스템의 비밀성, 무결성, 가용성을 보호해야 하며 심각한 남용은 처벌받도록 보증해야 한다. ⑤ 법체계가 성공적인 범죄의 수사에 결정적인 전산데이터의 보존과 빠른 접근이 가능하도록 허용해야 한다. ⑥ 상호지원체제가 국제적인 첨단기술범죄와 관련된 사건에서 시기적절한 증거수집과 교환이 가능하도록 보증해야 한다. ⑦ 법집행에 의하여 공개적으로 이용가능한 정보에 대한 국경을 넘는 전자적 접근은 데이터가 존재하는 국가의 인가를 필요로 하지 않는다. ⑧ 범죄수사와 기소에 사용하기 위한 전자적 데이터의 검색과 법적 인증을 위한 과학수사(법정) 기준이 개발되고 사용되어야 한다. ⑨ 정보통신시스템은 네트워크 범죄의 방지와 탐지를 도울 수 있도록 설계되어야 하며 범인의 추적과 증거수집을 용이하게 하여야 한다. ⑩ 노력의 중복을 방지하기 위하여 이 분야에서의 연구는 다른 관련 국제포럼의 연구와 서로 조화되어야 한다.

2. 한국의 대응전략: 행정윤리적 접근

사이버부패를 차단하는 행정윤리적인 대응방안은 다음과 같은 방안이 제시될 수 있다.

첫째, 사이버부패에 대하여 정보윤리위원회가 불건전정보의 내용여부를 심의하는 것이다. 행정윤리적 차원에서의 심의를 들 수 있다. 구체적으로 다음과 같은 내용이 지적된다.[34]:

"① 반국가적인 내용 ② 인권 침해 내용 ③ 인명 경시 내용 ④ 법과 질서의 존엄성 저해 내용: 범죄 행위를 목적으로 하거나 범죄 행위를 교사하는 내용⑤ 공개 금지를 어긴 내용: 미성년의 피고인, 피해자 또는 혐의자 이름, 주소 등 본인임을 알 수 있는 내용등 ⑥ 성, 음담 패설 내용: 신체 부위의 지나친 노출 및 선정적인 묘사; 성을 상품화하거나 저속한 표현을 함으로써 혐오감을 주는 내용 ⑦ 위화감 조성 내용: 계층간 위화감 조성 및 사행심과 금전에 대해 지나치게 탐욕적인 사고를 심어주는 내용 ⑧ 비과학적인 생활 태도 조장 내용 ⑨ 공중 도덕과 사회 윤리 저해 내용: 공공의 안녕질서 및 미풍양속을 해치는 내용 ⑩ 국민 정서에 반하는 내용: 지나치게 잔인한 행위, 위험한 유희, 악덕 행위, 비행 행위 등 국민정서와 생활에 해가 될 수 있거나 정서적인 불안감을 조성하는 내용; 불쾌감이나 혐오감을 불러일으키는 저속한 표현 ⑪ 신앙의 자유에 반하는 내용 ⑫ 저작권 위배 내용; 타인의 저작권을 침해하는 내용 ⑬ 의약 의 오용, 남용 조장 내용: 과학적인 근거없는 의료 행위나 약품 등에 관한 내용으로 이를 과장하거나 오·남용의 우려가 있도록 표현한 내용 ⑭ 불건전 오락물 등의 내용: 저속하거나 비윤리적인 소재를 주로하는 내용; 성적 충동이나 폭력, 범죄 등을 유발할 수 있는 게임; 이용자 녹음을 통한 전화 데이트, 맞선등 교재를 제공하는 내용" 이다.

둘째, 사이버 부패방지를 위한 윤리교육이다.[35] 예컨대 컴퓨터 교육은 기능 양성과 함께 수반되는 윤리적 문제를 인식시켜야한다. 컴퓨터 교육의 최종적 목표는 기능인 양성이 아니다. 정보통신 기기 사용에 따른 윤리적 문제들을 바르게 인식토록 교육되어야 한다. 우리나라 정보통신윤리위원회에서 제정한 「네티즌 기본정신」은 다음과 같다.[36] 1) 사이버 공간의 주체는 인간이다. 2) 사이버 공간은 공동체의 공간이다. 3) 사이버 공간은 누구에게나 평등하며 열린 공간이다. 4) 사이버 공간은 네티즌 스스로 건전하게 가꾸어 나간다. 한편 정보통신 윤리위원회에서 제정한 네티즌의 「행동 강령」은 다음과 같다: ⓐ 타인의 인권과 사생활을 존중과 보호. ⓑ 건전한 정보를 제공과 사용 ⓒ 불건전한 정보의 배격과 유포금지 ⓓ 타인의 정보보호, 자신의 정보관리 ⓔ 비·속어나 욕설 사용을 자제와 바른 언어사용 ⓕ 실명으로 활동하며, 자신의 ID로 행한 행동에 책임 ⓖ 바이러스 유포나 해킹 등 불법적인 행동 금지 ⓗ 타인의 지적 재산권의 보호하고 존중 ⓘ 사이버공간에 대한 자율적인 감시와 비판 활동의 참여 ⓙ 건전한 네티즌 문화조성 등이다.

통신 상에서 사용하는 ID나 주소는 여러 개를 만들 수 있는 것이 현실이다. 따라서 개인간에 통신이나 인터넷을 통해 거래가 이루어질 때 거래자의 인적사항에 대한 확인을 반드시

34) http://contest.co.kr/99/bardo1981/public_html/bardo/profile/badinfo.htm
35) http://www.knky.kyongnam.kr/CyberInternet/webinform/inform421.htm
36) Ibid., http://www.knky.kyongnam.kr/CyberInternet/webinform/inform421.htm

필요로 한다. 따라서 통신사기를 방지하기 위해 다음의 사항을 확인할 것을 교육시킨다. 예컨대 지도 방법 및 예시로서 학생들이 가상세계와 현실 세계를 구분할 수 있는 가치관과, 인식의 부족으로 현실세계를 오해하고, 잘못된 행동, 잘못된 인성을 갖게될 수 있다. 그러므로 바람직한 성문화에 대한 올바른 인식을 심어주고 상업적으로 만들어진 가상 세계가 현실과 많은 차이가 있음을 설명한다. 학생들이 인터넷을 검색하면서 포르노를 본의 아니게 접했을 경우 그 내용이 상업 목적의 극단적인 묘사와 유혹이기 때문에 누구보다도 포르노를 보는 학생 본인이 심리적, 정신적 피해자가 될 수 있다는 점을 주지시킨다. 학생들이 포르노를 접했을 경우 학생 스스로 위험성을 느끼게 할 수 있는 사례 중심으로 지도한다. 포르노를 피해 사례 설명을 통한 지도 또는 수업 활동에서 토론을 통해 인터넷 포르노에 대한 유해성이 도출될 수 있도록 한다. 학교에서의 대처 방법으로서 포르노 차단 소프트웨어는 대부분의 포르노 사이트들을 입력시켜 놓아 해당 사이트에 대한 접근을 금지시키는 방식으로 구성되어 있다. 현재 포르노 차단 소프트웨어의 차단율이 미흡한 것으로 나타나고 있으나, 그럼에도 불구하고 현재 학교에서 학생들의 포르노 접속을 부분적이나마 예방한다는 의미에서 차단 소프트웨어를 설치하는 것이 바람직하다. 아울러 포르노 접촉과 관련하여 성교육을 실시하는 것이 필요하다. 어차피 완전한 차단이 불가능한 현실에서 학생들의 자정능력을 신장시키는 것이 중요하기 때문이다.

학교의 교사는 학생들에게 윤리적 모범을 보여야한다. 교사는 정보화시대의 윤리적 문제들을 발견하는데 있어 매우 민감하면서도 치밀한 분석능력을 가져야 한다. 교사는 윤리적 문제들을 해결하기 위해서 심사숙고하는 자세가 필요하다. 교사는 확고한 윤리적 책임감을 소유해야한다. 정보통신 기기에 대한 윤리적 민감성(ethical sensitivity)을 제고시켜야한다. 윤리적 민감성을 제고시키기 위해서는 학생들에게 유추(analogy) 경험을 가지게 하면 효과적이다. 예를 들면 학생들에게 「남의 집 물건을 훔치는 것과 해킹의 공통점과 차이점」은?, 「둥산과 해킹의 공통점과 유사점」은? 등과 같음 질문을 제기하고 토론을 전개하는 식으로 접근 할 수 있다. 교사는 컴퓨터·정보통신 기기와 관련된 학생들의 윤리적 사유능력 발달을 위해서 다양한 체험·학습기회를 제공해야한다. 컴퓨터 범죄에 관련된 기사를 스크랩하고, 문제점을 분석하는 활동을 생활화시킨다. 책임감, 소유권, 프라이버시, 자율성 등과 같은 핵심개념에 대한 바른 이해를 시키도록 지도해야한다.

학교의 교사는 자아 정체성 확립을 위한 교육이 필요하다. 학생들이 가상현실과 실제현실(현실세계) 사이에서 이중적 자아를 지니지 않도록 확고한 자아정체성(self-identity)을 가지도록 지도해야한다. 가상세계에서 게임에 제왕 같은 존재인데, 현실세계에서는 주위의 모든 사람이 자기를 전혀 인정해 주지 않는데서, 발생하는 「이중적 자아」로 혼란을 겪는 경우가 많은 것으로 알려지고 있다. 학생들이 음란물에 중독되지 않도록 지속적 계도와 교육이 필요하다.

셋째, 행정윤리의 범위를 확대한 법적 제도적인 장치가 사이버부패를 통제한다. 구체적으로 컴퓨터범죄의 경우는 다음과 같은 제도적 방어장치가 있다. 예컨대 컴퓨터 범죄에 대한 법적 조치[37]이다.

종래의 형법은 인간의 행위에 위한 사무처리와 문서에 의한 사무처리를 전제로 하였기 때문에 컴퓨터에 의한 데이터처리에 대해서는 처벌할 수 있는 근거가 미약하였다.[38] 따라서 보완할 내용은 첫째, 전자적 기록의 부정제조와 훼기죄이다. 즉 타인의 사무처리를 그르치게 할 목적으로 권리, 의무 또는 사실증명에 관한 전자적 기록을 부정하게 제조한 자는 문서의 경우와 같이 처벌되도록 하였다.

둘째, 컴퓨터 손괴 등 업무방해죄이다. 즉 컴퓨터 손궤나 허위데이터, 부정한 프로그램의 입력 등의 방법에 의해 컴퓨터에 동작장해나 사용목적에 반하는 동작을 일으켜 업무를 방해하는 행위 역시 범죄로 규정하였다. 컴퓨터에 의한 업무방해는 사회적으로 중대한 영향을 미칠 우려가 있다는 판단에 따라 종래의 업무방해보다 형량을 무겁게 하였다.

셋째, 컴퓨터 사용 사기죄이다. 기존 형법에는 사람을 속이는 것에 대해 처벌하는 것에 국한되어 있었지만, 최근 들어 프로그램의 부정입력에 의하여 '기계를 이용한 사기'가 늘어나고 있다."

넷째, 사이버부패를 통제하기 위한 기술윤리적인 측면에서의 강화이다. 예컨대 행정 및 개인정보 등 중요한 자료를 보호하기 위한 자료의 암호화 등이 필요하며, 수시로 접근시 사용하는 패스워드를 바꾸어야 한다. 또한 시스템 전체에 대한 암호뿐만 아니라 파일별로 암호화가 필요하다. 불법침입 자동경보 시스템의 개발도 중요하지만 사용권한이 없는 자가 침입했을 경우 침입증거를 꼭 남기도록 만드는 프로그램의 개발도 시급하다. 또한 수시로 시스템 감시를 실시하여 내부자의 부정사용이나 범죄를 적발하고, 미비점을 보완하여야 한다. 동시에 컴퓨터 범죄 수사능력을 높여야 하며, 컴퓨터 관련 범죄를 전담하는 수사관, 검사, 법관을 양성할 필요가 있다. 한편 수해, 화재, 지진등 각종 재난에 대비한 안전장치의 개발이 시급하다. 정보화일 백업 시스템 강화는 물론 각종 재난에 내구적인 시스템 구축이 시급하다. 통신사기에 대한 기술적인 대응의 노력으로 전자서명 제도와 전자인증 기술 개발 등의 노력이 이루어지고 있다. 전자상거래에서 가장 중요한 신원확인을 정확히 하기 위하여 공인인증기관에서 거래 당사자의 전자서명을 공인 받는 체제가 전자인증이다. 현재 국내에는 한국정보인증, 한국증권전산, 금융결제원이 공인인증기관으로 등록되어 있다. 예컨대 통신사기에 제도적으로 대응하기 위하여, 많은 국가에서 통신사기를 미연에 알리고 경고할 수 있는 감시기능을 담당하는 기구를 설립하고 있으나 국내에서는 아직 이러한 기관이 설립되어 운영되고 있지 않은 실정이다. 통신사기를 처벌할 수 있는 법률적 근거는 형법, 방문판매 등에 관한 법률이 있으며, 통신 사기를 방지할 수 있는 전자서명 인증을 규정하는 전자 서명법이 시행 중에 있다.

다섯째, 컴퓨터 및 정보화에 대한 윤리교육 강화이다.[39]

---

37) 김종범, op.cit, pp.80-82.

38) 각국은 이러한 점을 보완하기 위하여 관련법을 제정하였다. 예컨대 독일은 1970년 Hessen주에서 '데이터 보호법'을 제정했고, 1977년에는 '연방정보보호법'(1986년 개정)을 제정했다. 영국은 1981년 '문서 및 위조법', 1984년 '데이터보호법'과 '경찰 및 형사증거법'을 제정하여 컴퓨터 범죄 처벌을 강화하고 있다.

예컨대 우편, 전화 등의 전통적 미디어에 대해서는 학교에서나 가정에서 많은 교육기회를 갖게 된다. 통신을 사용한 비즈니스분야에 있어서는 사업자간의 윤리를 요구할 수 있으며, 새로운 멀티미디어기기가 널리 사용됨에 따라 우편이나 전화와 같이 매너가 중요하다. 이런 점에서 고도 정보사회에 부응할 수 있는 정보통신의 윤리가 개발되고, 이것이 학교 및 사회 교육 등을 통해 정착되는 것이 필요하다. 미국 IBM은 "Computer didn't do it"이라는 모토를 표방하고 있는데, 이는 범죄의 주체는 사람이지 컴퓨터가 아니라는 말이다. 컴퓨터 범죄는 예방이 가장 중요하다는 점에서 컴퓨터 관련 윤리교육은 대단히 시급하고 중요한 문제이다.[40] 정보산업에 있어서도 경제가치는 인성가치(도덕성)인 정보윤리와 동시에 창조되어야 한다. 인성가치가 무시되는 경제가치는 삶의 질을 위협하게 된다. 기술교육과 전산교육에 윤리가 포함되어야 하고, 동시에 교재 출판 등과 같은 정보윤리 확립을 위한 사업도 추진되어야 한다."

여섯째, 사이버부패의 연루자와 연류 가능성 있는자 에게 특별교육의 프로그램을 설치 운용한다. 예컨대 가정에서의 컴퓨터 포르노에 대한 대응은 바른 성교육을 하거나 컴퓨터를 가족 공용화 하는 방안도 고려할 수 있다. 혹은 자녀들에게 밤 늦은 컴퓨터 사용을 자제시킨다. 그리고 부모가 컴퓨터를 배우든지 컴퓨터 외에 다른 취미 활동을 권한다. 그리고 신용카드를 잘 관리하는 방안도 고려할 수 있다. 기술적으로 음란물 검색 프로그램이나 인터넷 차단 소프트웨어를 활용하는 것도 하나의 방법이다. 마지막으로 PC통신 등에서 유통업자들의 움직임이 발견되면 즉시 신고해서 확산을 막는다.[41]

일곱째, 사이버부패의 통제를 위한 통합적인 시스템의 연결망 구축이다.[42] 예컨대 관계기관인 검찰, 경찰, 국정원, 정보통신부, 민간 기구등을 망라한 통합적인 통제시스템을 만드는 것이 필요하다. 예컨대 경찰청에서는 '95년 6월 수사국에 『지능과』를 설치하여 컴퓨터범죄 등 첨단신종범죄에 대응해왔고, '95년10월에는 외사관리관실에 해커수사대를 설치하여 해킹사건에 관한 수사를 맡아오다, '97년 8월 수사국에 『컴퓨터범죄수사대』를 창설하여 해킹, 컴퓨터바이러스 유포사범, 불법사이트 운영사범 등 사이버 범죄에 대한 적극적 대응을 해 오고 있다. 또한 지방경찰청과 각 경찰서에서도 컴퓨터범죄전담수사요원을 운용하고 있다. 경찰청에서는 최근 인터넷 사용인구의 폭증, 범죄발생율의 증가('99년 월평균 검거건수는 '98년 대비 5배 증가), 전문인력 양성의 필요 등 사이버 공간의 범죄에 대한 치안력 강화 필요성이 제기됨에 따라 '99년 10월부터 컴퓨터범죄수사대를 크게 확대하여 30명 수준의 전문인력을 갖춘 『사이버범죄수사대』 설립하여 2000년도에 지방경찰청에도 『컴퓨터범죄전단수사반』을

---

39) Ibid., p.82.

40) 문제는 사이바부패에서도 컴퓨터범죄와 같이 행위자가 윤리의식이 희박한 채 자신의 기술을 뽐내고 게임을 즐긴다는 의식이 강하다는 점에서 법적·기술적 대응 못지 않게 정보윤리의 정립이 필요하다고 하겠다. 더 나아가 정보사회에 부응할 수 있는 "인간과 기술"에 관한 윤리관의 정립도 필요하다.

41) 출처: 『컴퓨터 음란물 대처 요령 8가지』, 한국컴퓨터생활연구소, http://www.comkeeper.co.kr

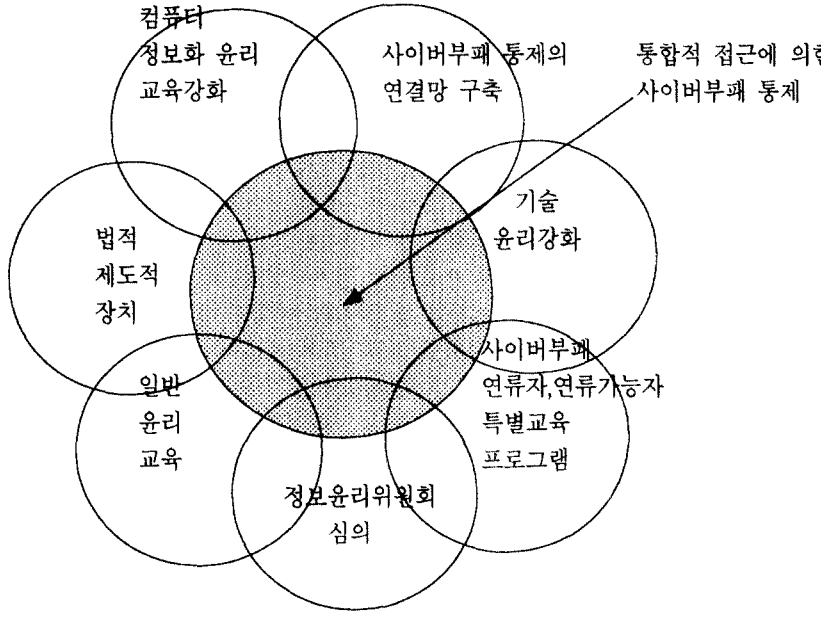
42) http://www.police.go.kr/user/cyber112/index6.htm

설치해 나갈 계획에 있다.

검찰에서는 '95년 4월 서울지검에 『정보범죄수사센터』를 설치하여 컴퓨터관련범죄 수사를 전담하고, '96년 6월에는 대검찰청에 『정보범죄대책본부』를 신설, '97년부터는 전국의 지방검찰청에 정보범죄전담수사반을 설치운영 하고 있다. '99년에는 대검찰청의 정보범죄대책본부가 『컴퓨터범죄전담수사반』으로 개칭하였다.

정보통신부 정보통신부내의 사이버 범죄와 관련된 정보화 역기능 대응부서는 정보보호과이다. 그리고 '96년에 『한국정보보호센터(KISA)』를 설립, 정보보호와 관련된 이론 및 기술연구, 대응전략 수립 등의 업무를 담당하고 있다. 한편 국가정보원에서는 '99년 8월에는 21세기 정보전(Information Warfare)에 대응하기 위해 『정보보안119』를 개설, 정보보안관련 최신 기술을 소개, 국가전산망 해킹관련 상담 및 처리 지원업무를 맡고 있다.[43] 이상에서 언급한 사이버부패의 통제를 위한 행정윤리적 접근을 <표 5>와 같이 표시할 수 있으며 실체에 관한 통합적 접근이 가장 바람직하다.

〈표 5〉 통합적 접근에 의한 사이버부패 통제



자료: 이 표는 필자가 지금까지의 사이버 부패통제전략을 통합하여 작성한 것이다.

43) 그밖에 민간단체로는 CERTCC, 정보통신윤리위원회, 학부모정보감시단 등에서 각종 사이버 공간에서의 불법활동을 감시하고 있으며 범죄혐의가 명백한 경우 경찰, 검찰 등 수사기관에의 수사협조 요청 등의 업무도 병행하고 있다.

Ⅵ. 요약과 결론

지금까지 우리는 사이버부패의 통제를 행정 윤리적 시각을 초점으로 논의하였다. 이것은 21세기에 들어와서 정보화가 가속화되고 있는 추세에 부응하는 기회와 도전의 동시적 전략과 맥을 같이한다. 정보화의 거대한 물결 속에서 순기능적 정보화 촉진정책 이면에는 정보화에 수반되는 각종의 역기능인 사이버부패의 통제전략 없이는 바람직한 삶의 질의 향상을 기대하기 곤란하다. 다시 말하면 컴퓨터는 인간의 삶의 질을 높이는데 크게 기여할 수 있는 문명의 이기이지만 문제는 그러한 기술을 어떻게 활용하는가 하는가에 있다. 정보기술을 발전시키는 것도 인간이고, 사이버부패를 일으키는 것도 역시 인간이다. 가속화되고있는 정보화가 컴퓨터범죄 비롯한 사이버부패를 적절하게 통제하지 못하면 정보화는 그 자체가 문명의 이기가 아니라 '문명의 흉기'가 될 소지도 있다고 할 수 있다. 따라서 정보화는 초고속통신망이나 구축이나 컴퓨터 하드웨어의 개발만으로는 성숙될 수 없다. 정보화의 역기능을 통제하는 행정윤리적 통제가 필요하다.[44] 실제공간에서의 부패가 망국병이듯이 가상공간에서의 만연된 사이버부패는 미래사회를 어둡게하는 유혹적인 덫이다. 따라서 우리는 행정윤리적인 통제전략을 통하여 정보화의 본래적인 기능을 다하도록 정책적인 배려가 시급하다.

참고문헌

강성남. (1994). 내부고발자보호입법에 관한 외국의 동향 서울: 국회도서관 입법조사분석실.
강정인. (1995). "정보사회와 민주주의", 정보사회 그 문화와 윤리 서울: 도서출판 소화.
김동현. (1990). "감사원 감사비리의 전말" 월간조선 7월호 통권 124, 188~203.
김석준외 3 인 공저. (2000). 뉴거버넌스연구, 서울: 대영문화사.
김세헌. (1989). 컴퓨터범죄와 프라이버시침해, 서울: 회성출판사.
김영래. (1996). "정치부패와 정치자금", 한국부패학회 발표논문집 1.
김영종. (1993). "부패문화의 개혁정책", 한국행정연구 2~1: 26~46.
_____. (1994). "컴퓨터범죄의 원인과 대책", 교정연구4: 371-389.
_____. (1997). "Korean Public Administration and Corruption Studies Seoul: The Hak.
_____. (1999). "정보부패의 패러다임 정립과 치유", 한국부패학회보 3:25-40.
_____. (2001). 부패학(4판개정증보판) 서울: 숭실대 출판부 Publishing Co.
김영평. (1988). "국가기관으로서의 정부관료제", 계간경향, 18: 198~209.
김종범. (1996). "정보화사회에 있어서의 역기능 대책", 서울: 한국행정연구.
김해동 외.(1994). 관료부패와 통제 서울: 집문당.

44) 김종범, op.cit. pp.99-100.

박홍식. (1990). "내부고발: 이론, 실제, 그리고 함축적 의미", 한국행정학보 25(3), 769~782.
부정방지대책위원회. (1995). 국제반부패활동의 동향 서울: 감사원.
백완기. (1989). 한국의 행정문화 서울: 고려대 출판부.
어기준. (1999). 학교컴퓨터실의 음란물 접촉 실태조사연구, 한국 컴퓨터생활연구소.
윤덕중. (1994). 범죄사회학 서울: 박영사.
서울특별시정보화기획실. (2000). 정보화에 대한 서울시민 여론조사, 서울: 서울특별시정보화 기획실.
정성호. (1991). "한국행정연구에 있어서 문화심리적 접근의 평가", 한국행정학보 25:3, 707~725.
중앙일보. (2000. 7. 20).
폴 히버트. 김동화외 4인 역. (1985). 선교와 문화인류학 서울: 죠이선교회출판부.
하태권. (1992). "민원행정에서의 행정부패", 한국행정연구 1(4), 108~127.
Allen, Francis. (1971), *Socio-Cultural Dynamics: an introduction to social change* New York: The MacMillan Co..
August Bequai. (1987), *Technocrimes* : Lexington: Lexington Books.
Beer, Michael. (1980), *Organization and Development: a system view* Santa Monica: Good Publishing Co., Inc..
Bell, Daniel. (1973), *The Coming of Post-Industrial Sociey* New York: Basic Book, Inc..
Buck Bloom Becker. (1990), *Spectacular Computer Crime* : Homewood: Dow Jones-Irwin..
Burnham, David. (1983). *The Rise of the Computer State.* New York: Vintage Books.
Burrell, Gibson and Morgan, Gareth (1979). *Sociological Paradigm and Organizational Analysis* London: Heinemann.
Caiden, Gerald E. (1969). *Administration Reform*, Chicago: Aldine Publishing Co., p.65.
Caudle, Sharon L. (1996). "Strategic information resouces management: fundamental practices". *Government Information Quarterly*(vol 13, no.1).
Coates, Joseph F. (1982). "Why Goverment Must Make a Mess of Technological Risk Management", in Christopher Hohenemser and J. Kasperson,(eds.) *Risk in the Technological Society.* Colorado Eoulder: Westview Press Inc..
Cooley, T. (1888). *A Treatise on the law of Torts.* 2nd. ed. Chicago: Callaghon.
Crane, Donald P. (1979). Personnel: *The Management of Human Resources* Belmont: Wadsworth.
Drucker, Peter F. (1993). *Post-capitalist society.* New York: HarperBusiness.
_____. (1995). *Managing in a time of great change.* Oxford, England: Butterworth Heinemann.
Frederickson, H. George(ed.). (1993). *Ethics and Public Administration*, New York: M.E. Sharpe, Inc..

Gould. David J. (1983). "The Effects of Corrupiton on Administrative Performance: illustration from Developing Countries". in *World Bank Staff Working Papers(No. 580)* Washington: D.C. The World Bank. pp. 1-41.

Heidenheimer, Arnold J.(ed). (1978). Political Corruption: *Readings in Comparative Analysis*, New Brunswick: Transaction Books.

Henderson, Gregory. (1968). *Korea: The Politics of the Vortex*, Cambridge: Harvard Unversity Press.

Holmes, Leslie. (1993). *The End of Communist Powr: anti-corruption campaigns and legitimization crisis*, New York: Oxford University Press.

Hoogvelt, Ankie M. M. (1976). *The Sociology of Developing Countries*, London: Mac Press.

Huntington, Samuel P. (1968). *Political Order in Changing Societies*. New Heaven: Yale University Press.

Johnston, Michael (1982). *Political Corruption and Public Policy in America*, Monterey: Brooks/Cole Publishing Company.

J. Van Duyn (1985). *The Human Factor in Computer Crime* : Princeton: Detrocelli Books.

Kim, Young Jong. (2nd ed, 1998). *Korean Public Administration and Corruption Studies*, Seoul HakMun Publishing Inc..

_____ et.al. (1998). *Public Sector Ethics*. Routledge: The Federation Press.

_____ et.al. (1999). *Organanized Crime: trends and perspectives of fight* Vladivostock: Far East University Press.

Klingner, Donald E. (1980), Public Personnel Management Englewood Cliffs: Prentice Hall, Inc..

Klitgaard, Robert. (1988). *Controlling Corruption*. Berkeley: Unversity of California Press.

Lewis, C. W. (1991), *The Ethics Challenge in Public Service* Washington, D.C.: ASPA.

Lingenfelter, Sherwood G. (1995), *Transforming Culture* Grand Rapids: Baker Book House.

Machlup, Fritz. (1962). *The production and distribution of knowledge in USA*. Princeton, NJ: Princeton University Press.

Naisbitt, Jone. (1982). *Megatrends*, New York: Warner Books, Inc..

Marqurardat, M.,& A. Reynolds. (1994). *The Global learning organization*. Chicago: Irwin.

Martin(ed.). *Public Administration and Domocracy*, Syracuse: Syracuse University Press.

Masuda, Yoneji. (1981). *The Information Society as Postindustrial Society*. Bethesda, MD: World Future Society.

Robbins, Stephen P. (1976). *The Administative Process*. Englewood Cliffs: Prentice-Hall.

Spradley, James P. (1979), *The Ethnographic Interview* New York: Holt, Rinehart and Winston.

Toffler, Alvin(1980), *The Third Wave* New York: Batan Book, Alvin.
Werner, Simcha B. (1983), "New Direction in the Study of Administrative Corruption" in *"Public Administration Review"*, pp.146-154..
한국컴퓨터생활연구소. "컴퓨터 음란물 대처 요령 8가지". http://www.comkeeper.co.kr
http://contest.co.kr/99/bardo1981/public_html/bardo/profile/badinfo.htm
http://icic.sppo.go.kr/
http://www.icic.sppo.go.kr/statistics/table01.htm
http://ict.use.go.kr/attach/classhome/6/L26/tict2/tict202.htm
http://ict.use.go.kr/attach/classhome/6/L26/tict2/tict208.htm
http://www.icic.sppo.go.kr/statistics/table01.htm
http://www.jlogis.com
http://www.knky.kyongnam.kr/CyberInternet/webinform/inform421.htm
http://www.npa.go.kr/ctrc/ctrc_03.htm
http://www.npa.go.kr/ctrc/ctrc_04.htm
http://www.npa.go.kr/introduction/policeact/page_140_2.html
http://my.netian.com/~hahyoung/anti_tech.htm
http://www.police.go.kr/user/cyber112/index6.htm
http://www.sed.co.kr/11_8/199909/h1851104.html
http://www.transparency.org