

우리는 “인터넷 감시사회”로 가고 있는가?:

열린 네트워크와 닫힌 사회

송 경 재

(경희대 인류사회재건연구원 학술연구교수)

I. 인터넷 유토피아와 디스토피아

인터넷을 위시로 하는 정보통신기술(Information and Communication Technologies: 이하 ICTs) 발전은 사회구조를 웹(web)이라는 형태의 새로운 네트워크로 연결시켰다. 네트워크(network)는 방송통신장비의 기술용어였다. 그러나 최근 네트워크라는 용어는 다양한 노드(node)로 구성된 집합체로서 사회·정치·문화·자연과학·경영학 등 이론으로 확정적으로 적용되고 있다. 그런 맥락에서 본다면 네트워크는 그 의미가 확장되면서 다양한 함의(implication)를 포괄하게 되었다(민병원, 2005: 99-100).

이로 인해 인간의 지적활동은 ICTs과 정보가 결합되면서 새롭게 재구성된다. 정보(information)는 개념 자체에서도 확인 가능하듯이 기본적으로 이동 내지는 전파를 목적으로 한다(한국데이터진흥센터, 2006: 9). 이러한 장점을 가진 정보는 ICTs와 함께 지식으로 축적되고 발전적인 순환과정을 통하여 새로운 지식국가-지식사회를 가능케 한다. 이를 가속화하기 위하여 정보의 효율적인 이동수단인 인터넷과 통신 네트워크와 미디어가 만들어진 것이다. 인터넷을 네트워크의 네트워크(A network of networks)로 부리는 것도 이런 맥락이다(김상배, 2008). 현대사회는 ICTs발전으로 참여의 아키텍처로 구성된 개방적인 네트워크사회(open network society)로 진화하고 있다.

일반적으로 정보가 네트워크에서 집성되면, 그 존재가치를 실현하고 다시 재가공, 창조되면서 수요와 효능은 증가한다. 그리고 정보가 산업사회의 물질재화와 마찬가지로 정보재화로 부각되면서, 인간의 인식과 지식의 양은 기하급수적으로 증가한다. ICTs는 단순히 인간이 활용한 도구를 넘어서 사회적으로 상호진화하면서 발전하는 사회적인 도구(social tools)가 된 것이다. 이런 차원에서 ICTs와 인간의 인식은 사회 속에서 재구성 되고 있는 것이다(서키, 2008).

정보가 자유롭게 유통되는 네트워크 사회로의 진입은 전통적 산업사회의 패러다임과 다른 형태의 사회구조가 형성된다. 첫째, 인터넷 네트워크는 인류 역사상 처음으로 등장한 다대다(many-to-many) 규모의 지구적 커뮤니케이션 네트워크 구조이

다. 인터넷은 과거 어떤 미디어도 수행하지 못했던 방대한 정보를 공급·유통·소비하는 구조를 가지고 있으며, 시·공간 제약이 없이 정보를 확산, 수렴할 수 있다(Chadwick, 2006; Castells, 2001).

둘째, 앞서도 언급했지만 네트워크 사회는 정보를 기반으로 한다는 점에서 물질과 자본을 바탕으로 한 산업사회와는 차별성을 보인다. 정보의 본질적인 속성인 비경합성(non-rivalrous)와 비배재성(non-excludable)으로 정보는 가진 자와 그렇지 않은 자 간의 격차가 발생한다(한국데이터진흥센터, 2006: 11-12). 따라서 사회는 정보를 매개로 하는 새로운 권력구조가 형성되는 것이고 김상배(2008)가 지적하는 바 네트워크 지식국가로 재구성되는 것이다.

본 연구자가 천착한 것은 이상과 같은 네트워크사회에서 새롭게 형성되는 사회구조에서 발견되는 2가지 빛과 그림자이다. 그것은 ICTs의 낙관성을 강조하는 인터넷 유토피아론과 비관적인 입장을 강조하는 디스토피아론이다.

인터넷 유토피아론의 이론적인 맥락은 초기 정보사회론자들로 거슬러 올라간다. 다니엘 벨(Bell, 1973)은 『후기산업사회의 도래』에서 컴퓨터와 같은 지적 기술을 장구하는 합리적인 사회의 도래를 예측했다. 그리고 토플러(Toffler, 1980)가 제3의 물결로서의 정보혁명을 선언한 이후 정보사회론은 후기 정보사회론자들과 네트워크 사회론자들로 계승되면서 반다이크(van Dijk, 1999), 카스텔(Castells, 2001) 등으로 학문적 영역을 확장한다. 최근에는 이런 학자들의 영향으로 인터넷을 탈집중화된 기술과 수평적인 구조로서 네트워크 사회의 진화와 발전 나아가 네트워크로 형성된 공론장의 가능성을 지적하기도 한다.

한편, 디스토피아론을 주장하는 학자들은 인터넷 네트워크의 등장은 면대면 접촉을 줄이고 클릭으로 모든 것을 해결하는 즉자적이고 감성적인 반응으로 시민권을 침해할 소지가 많다고 비판한다. 학자들은 인터넷에서의 여러 문제점이 있는 새로운 네트 내에서의 이슈가 등장하고 이는 참여적 인터넷 특성이 빅 브라더(big brother)의 위협보다 이웃에 의한 감시와 프라이버시 침해로 나아갈 것을 우려하고 있다. 또 정보 원형 감옥(information panopticon)이나 제도화 되지 않은 네트워크 사회에서 감시사회를 우려하고 있다(배영, 2008; Castells, 2000; 2001; 강상현, 2006: 129-137; Gandy, 1989: 65).

이러한 정보사회 또는 네트워크사회를 바라보는 2가지 관점은 결국 인터넷 네트워크의 기술적인 진화가 인간과 사회구조에 어떤 변화를 가져올 것인가에 대한 고찰과 연계되어 있다. 본 연구에서 고민하고자 하는 것은 네트워크 사회에서 제기되는 새로운 위험요인으로서 “감시사회(surveillance society)”의 등장이다. 네트워크 기술의 효율적인 활용으로 ICTs를 적용하지만 그것이 부메랑으로 다시 인간을 감시하는 기술로 적용된 것이 인간과 사회구조가 직면할 수 있는 최악의 형태가 감시사회이다.

본 연구에서는 현 단계 한국의 인터넷 네트워크를 둘러싼 법·제도적인 논쟁이 인터넷 감시사회로의 가능성을 가지고 있다고 간주한다. 그런 맥락에서 연구는 감시사회의 폐해와 현재 진행되고 있는 다양한 법·제도규제가 가져올 수 있는 악순환 구조 내지는 부메랑 효과에 대해 구체적으로 분석하고자 한다. 연구는 세부적으로 첫째, “감시사회”의 이론적인 구조와 맥락에 대한 체계적인 논의를 정리한다. 둘째, 한국에서의 감시사회의 가능성과 문제점을 “부메랑 효과(boomerang effect)” 모델로 제시하고자 한다. 마지막으로 셋째, 이러한 악순환구조를 형성하기 전에 고려해야 할 사회적인 노력에 관한 정책 대안을 모색할 것이다.

II. 네트워크 감시사회의 이론적 뿌리

1. 원형감옥(panopticon)과 빅브라더

일반적으로 감시사회라고 이야기 할때 가장 먼저 이야기 되는 것은 영국의 공리주의자인 제레미 벤담(Bentham)의 원형감옥인 판옵티콘과 소설가 조지 오웰(Orwell, 2003)의 『1984』이다.

먼저, 판옵티콘은 18세기말 영국의 철학자이자 법학자인 벤담이 설계한 근대적인 감옥을 지칭한다.¹⁾ 원래는 죄수를 감시할 목적으로 만들어진 이 감옥은 중앙에 간수가 감시할 수 있는 어두운 중앙 탑이 있고 그 주변에 죄수들의 방을 동그랗게 위치하게 만들었다. 따라서 판옵티콘이란 감옥은 중앙에서는 주변을 볼 수 있지만 주변에서는 중앙을 볼 수 없는 ‘시선의 비대칭’을 통해 죄수들이 언제나 감시당하고 있다고 감시를 내면화하도록 만들고 있다(강상현, 2006: 134). 이렇게 되면 안에 있는 죄수들은 비록 감시자가 없더라도 자신들이 늘 감시받고 있다는 느낌을 가지게 되고, 결국은 죄수들이 규율과 감시를 스스로 내면화해서 자기를 감시하게 된다는 것이다.

그러나 판옵티콘은 벤담이 설계한 뒤 주목을 받지 못하다가, 프랑스의 철학자 푸코(Foucault, 2003)가 그의 저서 『감시와 처벌 Discipline and Punish』에서 감옥의 역사를 소개하면서 판옵티콘의 감시체계 원리가 사회 전반으로 파고들어 규범사회의 기본 원리인 판옵티시즘(panopticism)으로 바뀌었음을 지적한다. 그는 감시 처벌의 기구를 근대사회의 감금 및 관리 감시사회로 이해한다.

한편 홍성욱(2002: 96-97)는 판옵티콘은 전자적인 형태로 제시한 정보 판옵티콘

1) 판옵티콘의 어원은 pan(모두, 전체)과 opticon(본다)을 합성한 용어로서 모두를 본다는 의미로 만들어졌다고 한다. 시초는 고대 그리스 철학자 플라톤이 감시 장치로 주위를 둘러싼 건물 안에서 수용자들의 일거수 일투족을 감시하는 일종의 원형감옥을 제안했다고 한다.

에서는 사람에 대한 정보 수집, 직접적 통제와 규율이 하나로 합쳐지고, 정보는 벤담의 판옵티콘에서의 시선을 대신하여 규율과 통제의 기제로 작동하는 것으로 보았다. 그는 벤담의 판옵티콘에 갇힌 죄수가 자신이 감시를 당하는지 아닌지를 모르듯이, 전자 판옵티콘의 정보망에 노출된 사람들 또한 자신의 행동이 국가나 직장의 상관에게 열람될지 않을지를 확신할 수 없기 때문에 자신의 행동이나 작업에 주의를 기울이는 감시구조를 만들게 된다고 지적한다.

< 그림 1 > 판옵티콘



* 출처 :

<http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=028&aid=0000202266>(검색일: 2009년 4월 7일)

또 다른 네트워크 감시사회 논의는 조지 오웰의 『1984』이다. 그는 1949년 이 책을 발간하면서 전체주의라는 거대한 지배 시스템 앞에 놓인 주인공 윈스턴 스미스 한 개인의 저항을 보여준다. 주목할 만한 것은 빅 브라더(big brother)라는 인물이 독재유지를 위해 ‘텔레스크린’이라는 장치를 이용한다는 점이다. 텔레스크린은 선동 도구인 동시에 감시 도구이기도 하다. 주인공은 텔레스크린의 감시를 피하기 위해 집 밖의 장소를 이용하거나 사각지대를 찾는 등 나름대로 노력하지만, 결국 감시망을 피할 수 없었다. 텔레스크린과 마이크론을 통해 경찰들은 시민을 감시하며, 사람들은 오랜 세월동안 세뇌되어 간다. 물론 이런 상황은 오웰이 작품을 썼을 때는 가능하지 않았지만 네트워크 사회에는 이미 진행형이다.

2. 현대의 감시사회 논의

전통적인 벤담과 푸코, 오웰의 감시사회에 대한 논의와 함께 ICTs가 발전함에 따라 형성된 감시사회론자는 정보사회학자 갠디(Gandy, 1989: 61-63)이다. 그는 정보 네트워크 사회를 산업사회가 감시사회화 되어가는 것을 은폐하는 명칭으로 보았다. 그리고 그는 ICTs가 새로운 감시기술의 주된 원동력이며, 그러한 기술을 통해 생산·저장·유통되는 정보가 점차 정치·경제 부문의 관료적 통제를 위한 핵심적인 자원이 되고 있음을 비판한다(강상현, 2006: 133).

그의 논의에 따르면, 현대 네트워크 사회에서의 ICTs는 일반 시민들을 부지불식간에 원격감지 환경에서 감시와 통제의 대상으로 전락시킨다고 보았다. 여기서 중요한 것은 스스로도 인식하지 못하는 사이에 ICTs를 활용하고 있는 와중에 감시당한다는 점이다. 즉 제도나 기술의 적용을 통한 효과에 대한 인식이 없을 경우 그것이 다른 문제점으로 인한 파생현상이 발생하는데 그러한 것이 바로 감시사회에서 발생한다. 이러한 전자적인 감시 장치는 사회적으로 강화되면서 인터넷을 감시의 공간이나 정보수집과 해킹의 공간, 쿠키를 통한 정보유출이 가능함에 주목한다.

네트워크 사회에서 시민권 침해와 감시사회 논의는 ICTs의 효율적인 이용의 가능성을 주장하는 학자들도 오래전부터 경고한 바다. 즉 식견있는 시민과 국가가 대처하지 못했을 경우 ICTs의 장점과 기능은 제한되고 감시와 통제가 강화될 것을 경고한다. 아무리 수평적인 네트워크가 형성되어도 권력에 의한 네트워크 차단이 가능하다. 이러한 대표적인 인터넷 네트워크 탄압사례가 중국이다. 중국은 인터넷 만리장성(Great Firewall)이란 차단장치를 통해 반정부적인 웹사이트나 블로그 등의 접근을 차단하거나 정치적 내용을 담지 않은 인터넷 내용에까지 검열을 강화하고 있다(International Herald Tribune, 2008년 2월 5일). 이런 네트워크의 차단에 대해 골드스미스와 우(Goldsmith & Wu, 2006)는 정부에 의한 네트워크 통제로 분석하고 국가에 의한 새로운 인터넷 네트워크의 지배라고 주장한다.

감시사회론에 대한 논의는 올리히 벅의 위험사회와 함께 최근에도 계승되고 있다. 마티선(Mathiesen, 1997)은 한발 더 나아가 현대사회를 서로 바라보는 사회라고 명명하여 상호 감시하는 사회의 무서움을 지적한다. 즉, 현대 네트워크의 발전은 과거에 소수가 다수를 바라보는 형태의 감시에서 다수가 소수를 바라보는 감시인 시놉티콘(synopticon)도 가능하게 한다(강상현, 2006: 134-5).

채드윅(Chadwick, 2006: 257-258)도 네트워크로 인한 새로운 사회의 장점을 인정하지만 이로 인해 생길 수 있는 문제에 대한 대안도 같이 고민해야 한다고 지적한다. 즉, 감시와 프라이버시 등의 문제로 네트워크사회에 있어 다른 형태의 시민 기본권 위축을 우려하기도 했다. 그런 차원에서 레식(Lessig, 2000)이 강조한 새로운 인터넷 아키텍처, 새로운 코드(CODE)는 통제의 근본적인 도구가 되어 전통적인 국가 권력 형태에 의해 규제와 경찰력 행사를 가능하게 한다는 점에서 감시사회의 가능성을 예견한 학자이다(Benkler, 2006).

이처럼 기존 연구는 각각 네트워크화와 ICTs의 발전에 따른 편익과 함께 부지불식간에 발생하는 감시의 문제를 다양한 시각에서 분석하고 있다는 점에서 의미가 있다. 네트워크사회의 낙관론은 네트워크화로 인한 참여적이고 민주적인 요소가 확대될 것을 강조한 반면 감시사회론은 새로운 위험요인의 등장을 경계한다. 이러한 감시사회에 대한 논의의 저변을 분석하면 ICTs의 발전의 이중성을 확인할 수 있다.

첫 번째 측면은 효율성과 신속성, 상호작용성을 통한 새로운 네트워크 사회로의 진전을 통한 지식기반의 새로운 사회를 바라보는 관점이다. 그렇지만 반대로 ICTs 자체를 하나의 감시기술화 할 수 있다는 점에서 그 위험성을 경고한다. 예컨대, 정치권력이나 경제권력이 기술을 통해 감시대상에 대해 더 정확하고 많이 알 수 있게 되었다는 것은 위험한 것이다. 정보사회학자인 카스텔(2001)이 인터넷은 정부가 시민을 감시하기 위한 것이 아니라, 시민이 정부를 감시하기 위하여 사용될 수 있음을 경고한 것도 이와 같은 맥락이다.

그러나 현실적으로는 이미 감시사회는 가속화되고 있다. 휴대폰의 전원을 켜놓은 동안에는 다른 사람이 위치를 파악할 수도 있고, 인터넷 사이트를 통해 우리의 신상정보가 전혀 알지 못하는 사람에게 흘러들어갈 수도 있다. ICTs이 발전함에 따라 사회환경은 새로운 정치경제적 기회구조를 만들고 있다. 디지털 컨버전스(digital convergence)로 일컬어지는 디바이스의 융합, 온라인과 오프라인의 융합, 커뮤니케이션 방식의 융합 등 다층적인 현상이 새롭게 대두되고 있다. 이런 현상은 한편으로는 긍정적으로, 다른 한편으로는 부정적으로 묘사된다. 그렇다면 ICTs발전은 필연적으로 감시사회로 직결되는가? 감시사회에서 이득을 보는 집단(세력)은 누구인가?

Ⅲ. 감시사회의 도구

1. 국가의 인터넷 규제

근대 유럽의 민주주의 과정은 국가로부터 시민권을 형성하는 과정이었다. 네트워크 사회에서도 이러한 과정은 반복된다. 민주주의 역사에서 인터넷 규제논의는 국가 개입이 심화될수록 결국 시민권은 훼손되고 더욱 강한 국가권력에 의한 통제를 필요로 한다. 이점은 민주주의의 가장 중요한 근본이 다원주의에 있음을 간과한 인식론적 오류의 발현이기도 하다. 따라서 국가는 사회 질서 유지라는 명분으로 인터넷 역기능 현상을 제어해야 시각에 머물러 있다. 그러다 보니 다양한 규제와 통제를 시도하는데 이러한 규제와 통제가 자신도 모르게 그리고 실제적으로 감시사회로 가는 방향인 것을 모르고 있다는 점이 큰 문제다.

그러나 본질적으로 자유로운 의사소통의 공간에서 누구나 정보에 액세스할 수 있는 인터넷은 권력의 입장에서는 부담이다. 그래서 국가권력은 통제되지 않는 인터넷을 싫어한다. 국가는 인터넷이 상업화 된지 15년 동안 지속적으로 인터넷을 통제하려 했고 네티즌들의 말하고 쓸 권리를 제한하고자 한다. 다양한 참여와 토론을 통한 의사결정방식, 정보의 소통과 숙의는 기득권을 유지하려는 세력에게는 심각한 위험요소로 인식한다.

이는 전 세계적으로 가장 민주화가 진전되었다는 미국에서도 마찬가지이고 한국은 더할 나위없다. 미국은 1998년 존 포스텔(Postel)과 함께 인터넷 관리 기구를 만들 때 직접적인 국가 참여를 노골화했지만 당시 인터넷 운영자들과 네티즌들의 반발로 인해 국제인터넷주소관리기구 ICANN(The Internet Corporation for Assigned Names and Numbers)을 NPO로 독립시킨 것은 대표적인 사례이다(카스텔, 2001).

중국에서 진행되고 있는 인터넷 규제는 더욱 심각하다. 중국정부는 강력한 인터넷 통제정책을 실시하고 있는 대표적인 나라이다. 중국 당국의 검열과 제제조치는 인터넷 공간에 난무하는 음란·폭력물과 저작권 침해 사이트를 대상으로 했지만 본질적으로는 반체제 사이트에 대한 검열과 유통금지가 목적이다. 베이징 올림픽을 전후해서 다소 완화됐던 인터넷에 대한 정부 통제가 2008년 말부터 한층 강화되는 추세로서 대표적인 사례가 ‘뉴보왕(牛博網, bullog.cn)’ 폐쇄사건이다. 뉴보왕은 중국 정부를 비판했던 사이트로, 쓰촨성 대지진 때 피해자 지원을 위한 모금운동을 벌이고 모금과정과 모금액의 사용내역을 투명하게 공개함으로써 중국 네티즌들 사이에서 호평을 받았던 사이트였다. 이 사이트는 중국 정부를 자극하는 정치적 의견을 거르지 않고 게재했던 것이 폐쇄의 직접적인 원인이 되었다고 한다(고민경, 2009).

그리고 중동의 많은 국가들은 서구의 정치적인 사고의 유포와 외설확산이라는 두려움으로 인터넷 접속을 차단한다. 그래서 중동의 일부 지도자들은 인터넷을 정치적 전복을 목적으로 하는 서구의 첩자로 간주하기도 한다(RAND, 2002: 6). 이런 현상이 초기 미국이나 중국, 중동만의 현상은 아니다. 미국과 유럽정부는 테러와의 전쟁의 한 일부분으로 인터넷을 차단하는데 활용하고 있다. 미국은 2001년 제정된 <애국법(Patriot Act)>에서 테러조직의 웹 사이트를 일방적으로 차단하거나 폐쇄한다(Atton, 2007: 23).

전 세계적으로 이렇듯 국가에 의한 인터넷 규제는 전 방위적으로 나타난다. 그리고 이를 기술적으로 적용한 시도도 있다. 다양한 인터넷과 네트워크 통제기술들이 업계와 국가 간 서로 얽힌 이해관계로부터 출현하고 있다. 패스워드 기능, 쿠키(cookies), 인증절차를 통제하는 신원확인 기술과 종류는 다르지만 개별 사용자의 위치를 파악할 수 있는 신분확인 기술의존, 감시와 정기적으로 기록된 정보 저장

결과로부터 데이터베이스를 축적하는 방식의 기술은 이미 개발된 지 오래다(카스텔, 2001).

한편, 이러한 국제적인 움직임과 함께 한국에서도 2008년 미국산 쇠고기 촛불집회와 하반기 경제위기에서 보여준 인터넷 미디어와 토론문화를 목도하면서 국가권력이 미치지 않는 공간으로서의 사이버문화를 다시금 확인할 수 있는 계기가 되었다. 이후 2008년부터 우후죽순처럼 정당과 정부에 의해 인터넷 규제를 위한 법제화가 시도되고 있으며 그 핵심은 인터넷에서의 자유로운 토론을 제한하고 규제를 강화하려는 움직임이다. 하지만 법안의 문제점을 차치하고라도 만약 이러한 법안들이 통과되었을 때의 사회상을 한번이라도 상상해 본다면 국가에 의한 감시사회가 예견되고 있다는 불안을 떨칠 수 없다.

국회에 제출되어 있는 대표적인 인터넷 및 통신 규제만 나열해도 ▷ 사이버모욕죄 신설, ▷ 게시판 임시조치, ▷ 제한적 본인 확인제의 확대, ▷ 일정기준 이상의 인터넷 서비스 사업자의 모니터링 의무화, ▷ 불법복제 유통 금지, ▷ 통신비밀보호법 개정안, ▷ 국가대테러활동에 관한 기본법 제정안과 국가사이버위기관리법 제정안 등 그 수를 헤아릴 수 없다. 이러한 하나하나의 규제조치가 단기적으로는 반정부적인 행위에 대한 감시 장치이지만 장기적으로는 사회 전체적인 감시 장치가 될 수 있다는 점에서 그 무서움은 더하다. 주요 내용을 간략하게 살펴보자(송경재, 2009에서 재인용).

첫째, 전 세계에서 한국에만 도입하려고 하는 <정보통신망 이용촉진 및 정보보호 등에 관한 법률>(이하 <정보통신망법>)의 사이버모욕죄 도입은 심각한 민주주의 권리의 훼손이란 비판을 받고 있다. 사이버 모욕죄가 가지고 있는 “반의사불벌죄” 조항은 법리적인 논쟁 면에서 문제의 소지가 있다. 학계와 정치권, 시민단체는 벌써부터 위헌시비가 있어서 법의 도입자체를 반대하고 있다. 여기에 불법정보의 유통금지조항(제44조 7의 제1항)에 ‘모욕’을 포함시켜 불법정보의 범위를 확대해석함으로써 인한 과다규제라는 비판을 받고 있다.

둘째, 모니터링제도의 강화도 시장과 학계에서 동시에 비판받고 있다. <정보통신망법> 개정안은 불법정보의 유통방지를 위하여 불특정 다수에게 공개되는 정보에 대하여 정보통신서비스 제공자에게 모니터링을 강제하고 있다. 이법이 통과되더라도 서비스 사업자들에게 과다한 집행비용 부담으로 인해 인터넷 산업의 위축이 우려되는 조항이기도 하다. 주요 인터넷 서비스 사업자가 하루 수백만 개의 게시물을 모두 모니터링 하는 것은 기술적으로나 현실적으로 불가능하다. 모니터링 의무화는 인터넷 서비스 사업자로 하여금 수백만 개 게시물에 대해 신고가 없더라도 모니터링하고 불법정보를 찾아내라고 요구하고 있는 셈이다. 이에 대해서는 이미 국회입법조사처의 보고서에서도 폐해가 예상되는 조항으로 평가되고 있다.

셋째, 지난 4월 1일 통과된 <저작권법 개정안>은 불법 복제물을 올리는 인터넷

게시판에 대해 문화체육관광부 장관이 3회 이상 삭제 명령을 내린 뒤 게시판을 최대 6개월 동안 폐쇄시킬 수 있도록 하고 있다. 이는 결국 저작권과 관련된 조항이지만 아직 국내에서 불법복제물에 대한 인식이 제대로 정립되지 않은 상황에서 법을 시행할 경우 작가는 범죄자의 양산을, 크게는 정부 비관적인 게시판이나 토론방의 폐쇄를 할 수 있는 심각한 법조항이다. 개정안의 문제는 명령권을 문화부 장관이 갖고 있다는 점이다. 저작권 침해로 인한 피해자의 문제제기 없이도 정부가 자의적으로 저작권 침해를 판단할 수 있다는 것이다(연합뉴스 2009년 4월 2일).

넷째, 또 다른 문제는 감청장치 설치의무화를 요구하고 열람권을 제시한 <통신비밀보호법> 조항이다. 한나라당에서 제기한 <통신비밀보호법> 개정안은 개인의 휴대전화 감청, 이메일, 인터넷 IP추적에서 수사기관이 법원의 영장이 없어도 가능하게 하는 법안이다. 이를 위해 통신업체에서는 개인의 통신사실 확인 자료를 보완해야 하고 국가기관의 요청 시, 제출하도록 되어있다. 이 법은 국민의 통신을 하는데 있어 누군가가 사생활과 프라이버시 침해를 한다는 것이고 결국 국가(더 엄밀히 국정원 또는 검찰, 경찰)는 국민의 휴대전화나 이메일의 감청을 가능케 한 것이다. 여기에 관련법인 <전기통신기본법>, <형법> 등을 보태면 가히 전 방위적인 인터넷 탄압이라 할 수 있다(송경재, 2009에서 재인용).

2. 감시사회는 눈앞에 와있다.

우리는 앞서의 분석에서 가치중립적인 ICTs의 활용에 대한 낙관적인 그리고 비관적인 관점에 주목했다. 그리고 비관적인 관점으로 제기한 감시사회의 논의는 과다한 ICTs의 활용이 아니라 전체주의적인 권력이나 국가에 의해 주도되고 있음을 알 수 있었다. 즉, 현대 자본주의 사회에서 지배의 관철을 위해 특정한 역사적 맥락에서 독특한 방식으로 이어진 것이 감시사회이다. 우리는 과연 그러한 감시사회가 먼 훗날의 이야기로 치부할 수 있을까? 본 발제에서 진행되고 있는 인터넷 및 통신관련법이 모두 통과되었을 때의 미래상을 제시하면 감시사회는 우리 눈앞에 와 있다.

1) 인터넷

인터넷 네트워크 환경의 변화는 다층적이고 사전·사후적인 형태로 나타날 것이다. 먼저, 다층적인 측면은 인터넷의 전방위 규제가 진행되고 있다. 골드스미스와 팀우(Goldsmith and Tim Wu, 2006: 127-142)에 따르면 현재 인터넷 규제 논의는 국가의 크기, 중개자인 ISP의 수, 합법적 요소와의 혼합이라는 3가지 변인에 따라 가변적으로 나타난다. 이를 층위적으로 본다면 첫째, 기간망으로서 도메인 네임통제가

있다. 이 방식은 가장 강력한 국가통제 모델이고 유해 도메인을 접속 차단하는 방식이다. 최근 중국에서 반국가 사범의 사이트나 유튜브를 차단하는 것도 바로 이 방식이다. 둘째 층위는 중개자인 ISP를 통한 통제이다. 가장 널리 쓰이는 방식이면서 국가입장에서는 효과적인 규제 양식이다. 이러한 통제는 임시조치나 인터넷 실명제의 실시, 모니터링 의무 부과 등이 대표적이다. 셋째 층위는 개인에 대한 직접 법집행이다. 이는 실제 콘텐츠나 정보 작성자, 유통자, 소비자에 대해 처벌하는 방식이다.

< 표 1 > 인터넷 규제

| No. | 방식 | | 내용 |
|-----|--------------|-------------------|---|
| 1 | 사전적 규제 모델 | 도메인 네임 규제 | <ul style="list-style-type: none"> - 가장 강력하고 본질적인 국가통제 모델(망법) - 유해 도메인 명을 차단하는 방식 - 권위주의 국가에서 주로 시행 - 중국에서 파룬궁이나 반국가사범 등에서 도메인 네임 통제 실시 - 한국에서도 유해정보 (음란물)는 통제 |
| 2 | | 중개자 규제 | <ul style="list-style-type: none"> - ISP 사업자를 통제하는 방식(망법/저작권법) - 다양한 규제조항과 법적·문화적 통제가능 - 글로벌 기업인 구글의 중국사업 진출 시 현지 법 규제 준수나 유럽에서 나찌 관련 상거래 금지 등의 규제에서 쓰이는 방식 - 한국의 유튜브도 인터넷 실명제 도입도 이와 비슷한 사례라고 할 수 있음 - 시장 검열의 우려 증가 |
| 3 | | 개인에 대한 법 집행 | <ul style="list-style-type: none"> - 실제 콘텐츠나 정보 작성자, 유통자, 소비자에 대한 처벌(저작권법/망법/형법/사이버모욕죄) - 역시 3가지 층위를 가지고 법집행이 가능 (작성죄/유포죄/소지죄) |
| 4 | 사후적 규제 모델 | | <ul style="list-style-type: none"> - 겁주기 효과 - 글의 작성 시부터 스스로 검열(자기검열)을 야기 |

* 자료 : Goldsmith and Tim Wu(2006: 127-142)의 모델을 바탕으로 연구자가 재구성

마지막으로, 사후적인 규제로서 법안이 통과되었을 때 발생하는 겁주기 효과도 상당할 것이다. 언제라도 글을 쓰면 잡혀갈 수 있다는 불안감은 글의 작성 시부터 스스로 검열(자기검열)을 야기할 것이다. 그럴 경우 국가는 시장에게는 개인의 정보와 통신을 모니터링하고, 감청장치를 설치하는 “시장검열”을 하고 정부정책에 반대되는 글을 쓰거나 말하는 네티즌들은 수사를 함으로 “국가검열”을 네티즌들은 겁을

먹고 “자기검열”을 하게 하는 방식으로 감시당하게 되는 것이다.

현재 한국에서는 이러한 국가에 의한 규제 방식 4가지가 모두 통합적으로 표현되고 있다. 전 세계적으로 인터넷 상의 부가서비스에 대한 법적 규제는 최소화하는 경향을 보이고 있는데, 선부른 법적 규제가 산업적인 차원에서의 기술발전과 서비스 개발, 신규 산업에 대한 진입장벽으로 작용할 가능성이 다분하다. 먼저 문제가 되는 사이트에 대해서는 방문조차 못하고, ISP에 의해 모니터링이 강화되고, 나아가 개인에 대한 법집행이 가능하다. 무엇보다 ISP에 대한 전 방위적인 규제는 최근 몇 차례 발생했던 국가기관에 의한 개인정보 요구나 로그파일, 방문자 조회, ID검색 등을 가능케 할 것이다. 이러한 다양한 형태가 인터넷에서 발생한다면 개인은 인터넷이 그야말로 감시의 공간이 될 것이며 개인정보의 제공은 물론, 쿠키에 의한 개인 컴퓨터 추적, IP주소 추적, ID확인 등이 가능하게 된다. 여기에 마지막으로 본인 실명제의 도입까지 추진된다면 인터넷에서 더 이상의 공적인 영역은 사라지고 “국가와 시장이 감시하는 공간”으로 재구성 될 것이다. 여기에 이런 두려움으로 자기 감시까지 한다면 인터넷은 그야말로 갠디(Gandy, 1989)의 감시사회에 다름 아닌 것이다.

2) 통신

통신감시는 이번 법 개정에서 중요한 쟁점 중의 하나이다. 앞서 지적한대로 <통신비밀보호법> 관련 재·개정안은 휴대전화 감청, 전화 통화내역, 인터넷 로그기록 보관을 의무화, 댓글 추적, 이메일, 인터넷 IP추적이 가능하다는 점에서 사회적으로 문제시 되고 있는 조항이다. 그리고 이를 위해 통신업체에서는 개인의 통신사실 확인 자료를 보관하고 국가가 요구 시 제출해야 한다. 마지막으로 교통카드나 신용카드를 이용한 교통이용내역도 기록하도록 규정하고 있다.

관옵티콘이 감시탑에서 실제로 감시를 하고 있느냐 여부와 무관하게 사람들에게 규율과 감시를 내면화하여 복종을 이끌어내는데 있다면 이러한 통신감시는 이용자들이 시민들의 불안감을 자극할 수 있다. 결국 전자적인 감시사회가 가능한 것이며 유리온실에 갇혀 국가로부터 감시당하는 존재로서의 시민을 상정하고 있는 것이다. 이 법안은 모든 국민이 언제 어디서나 범죄를 저지를지 모른다는 이유만으로 통신비밀에 해당하는 내용들을 사업자가 보관 혹은 관리토록 하고, 수사기관이 원할 때 제출할 수 있는 시스템을 만든다는 점에서 감시사회의 백미라 할 수 있다.

개인의 사적 공간은 없어지고, 사적공간에 귀를 세우고 있는 공적기관의 존재를 느끼게 된다. 누구라도 꼬투리를 잡아서 처벌할 수 있을 것이고 인터넷에서는 한마디도 하지 못하는 그런 입막음 구조가 형성될 수 있다. 인터넷과 휴대전화, 유선전화를 국가권력인 수사기관이 감시망 속에 가두어 두는 국민 감시체계를 만들어 빅

브라더가 되고자 하는 것과 다를 바가 아니다. 이럴 경우 수사기관의 자의적인 판단에 의한 인권유린이나 민주주의 시민권의 훼손은 자명하다. 이것이 감시사회가 아니면 무엇이 감시사회일까?

< 표 2 > 통신비밀보호법 규제

| | 주요 내용 |
|---------|---|
| 통신비밀보호법 | <ul style="list-style-type: none"> - 통신사업자가 직접 녹취 장비를 구비하고 1년간 통신자료를 보관 - 통신사실 확인 자료에 인공위성 위치추적 시스템(GPS)을 활용한 위치 정보를 추가하고 휴대전화, 이메일, 메신저에 대한 감청을 허용 - 감청 협조 의무가 부과되는 대상이 접속서비스 제공자, 포털, 웹호스팅 업체와 같은 부가통신사업자 포함 |

사실, 2009년 정보통신부/방송통신위원회의 “08년 하반기 감청협조, 통신사실확인자료 및 통신자료 제공 현황” 발표에 따르면 이미 개정 법안이 통과되지 않아도 전년대비 통신감청²⁾, 통신사실확인자료 제공³⁾, 통신자료제공⁴⁾ 등이 모두 2007년에 비해 증가세를 보였다. <통신비밀보호법>은 국가기관에 의한 불법 감청을 막기 위해, 모든 감청에 영장을 발부해야만 하는 것을 목적으로 1994년에 만들어졌다. 이런 사실로 미루어 보아도 <통신비밀보호법>이 통과될 경우, 수사기관의 자의적인 판단에 의한 통신감청과 자료요구, 자료제공은 기하급수적으로 증가할 것이고 결국 통신에서의 본격적인 감청 감시사회가 도래하게 될 것이다.

< 표 3 > 통신사실확인자료 및 통신자료 제공 현황

| 연 도 별 | 통신감청 | 통신사실확인자료 제공 | 통신자료제공 |
|-------|-------|-------------|---------|
| 2007 | 1,149 | 183,659 | 426,408 |
| 2008 | 1,152 | 212,745 | 213,897 |
| 증감 | +0.3% | +15.8% | 11.3% |

3) CCTV

- 2) 감청은 수사기관이 법원의 허가서를 통신 사업자에게 제시하고 수사 대상자의 통신내용을 확인하는 제도이다(정보통신부/방송통신위원회, 2009).
- 3) 통신사실확인자료제공은 수사기관이 법원의 허가를 받아 통신 사업자에게 수사 대상자의 통신사실조회를 요청하는 제도이다(정보통신부/방송통신위원회, 2009).
- 4) 통신자료 제공은 수사기관이 통신사업자에게 수사관서장의 요청서를 제시하고 수사 대상자의 인적사항을 요청하는 제도이다(정보통신부/방송통신위원회, 2009).

사실 이번 인터넷과 통신 관련 규제법과는 다른 맥락이지만 흉악범사건으로 인한 CCTV의 확대도 감시사회에서 장기적으로 문제가 될 소지가 있다. 현재 국내에서도 CCTV는 해마다 증가하고 있다. 전국 방범용 CCTV 설치 현황을 보면 2004년 538대, 2005년 1,100대, 2006년 1,978대, 2007년 5,044대, 2008년 8,761대이다. 경찰청에 따르면, 올해는 지난해의 2배 가까이 증가한 15,092대가 전국에 설치될 예정이다(동아일보 2009년 2월 20일).

그렇지만 CCTV가 장기적으로 시민의 권리를 제약할 가능성이 있다는 측면에서 사회적인 논의가 필요하다. 사실 CCTV를 통한 범죄예방이나 테러방지 활동은 영국을 그 모델로 한다. 영국은 CCTV를 매개로 하는 감시가 철저하다. 잘 알려져 있다시피, 1998년 개정된 “정보보호법”에 근거규정 명시했고, 2005년도 지하철역 연쇄테러사건 용의자 검거에 결정적 기여한 것도 CCTV 추적에 의한 것이다. 현재, 영국은 CCTV는 420만대로 인구 14명당 1대 꼴이고 런던 시민들은 30초당 한 번, 하루에 300번씩 CCTV에 노출되고 있다. DNA DB도 전체 국민의 7%에 달해 미국의 0.5%보다 높다(MBC <W> 영국 CCTV 르포, 2007년 8월 10일 방송, http://mbcinfo.imbc.com/news_view.asp?idx=6460. 검색일 : 2009년 4월 7일).

그러나 최근 영국에서도 감시사회에 대한 우려가 발표되고 있다. 상원 헌법위원회가 2009년 2월 6일 발표한 『감시: 시민과 국가(Surveillance: Citizen and the State)』에 따르면 테러와 범죄예방을 목적으로 도입된 CCTV와 DNA DB가 개인의 자유를 침해하고 있다고 지적한다(연합뉴스 2009년 2월 6일). 그런데 중요한 것은 헌법위원회조차 만연되고 일상화 된 전자감시와 개인정보의 수집이 당연시 되고 있다고 경고했다. 그리고 실제 범죄를 예방하는지, 지역 경찰이 감시권력을 사용해도 되는지에 대한 의문이고 CCTV 설치와 함께 이를 효과적으로 활용하기 위한 경찰의 순찰시스템 개선, 지역주민들의 치안관리 노력이 병행되어야 함을 지적한다.

영국의 경험에서도 나타나지만 현재 국내에서는 범죄예방 차원에서 CCTV를 확대하고자 하는 노력을 계속하고 있다. 하지만 이러한 노력이 결국엔 감시사회의 한 주춧돌을 세운다는 점을 자각해야 할 것이다.

IV. 결론에 대신하여; 인지하지 못한 부메랑 효과(boomerang effect)

이상 본 발제문에서는 ICTs 발전으로 인한 감시사회의 전망에 대해 한국적 맥락으로 진행 중인 인터넷 및 통신법 개정안을 중심으로 재구성했다. 연구에서도 확인했지만 결국, 논의 중인 <정보통신망법>, <사이버모욕죄>, <통신비밀보호법>, <전기통신기본법>, <형법>, <저작권법> 등은 전 방위적으로 시민의 기본권을 제한하고 오히려 국가가 시민을 감시하는 기제로 작동할 수 있음을 확인할 수 있다.

물론, 법안을 제출한 의원이나 정부의 입장에서 본다면 하나하나의 법률에 대한 명분이 없는 것은 아니다. 그리고 인터넷 공간이 언제나 깨끗한 청정구역(clean space)은 아니다. 그렇기 때문에 어느 정도의 규제와 정화는 필요하다. 인터넷으로 인한 악플러 문제, 프라이버시 침해, 욕설, 감정의 배설구 등은 인터넷에서 해소해야 할 문제임에 틀림없다. 하지만 그것을 철저히 규제한다고 인터넷과 통신의 긍정적인 기능마저 제한하는 것은 문제가 있다. 그리고 그것이 잘못 과도한 권력집중현상을 만들었을 때 시민들은 결국 유리온실에 갇힌 상태로 감시상태에 놓이게 될 것이다. 오히려 의도하지 못한 효과가 더 큰 문제를 낳을 수도 있다.

시민권은 한번 훼손되면 그것을 다시 찾기는 너무 긴 시간이 필요하다. 마치 공기와 같아서 우리 주변에 있을 때는 모르지만 그것이 사라질 경우 그 피해는 막대하다. 앞서 가상의 시나리오 형태로 “부메랑 효과(boomerang effect)”를 기술했지만 결국 현재 진행되고 있는 인터넷과 통신관련 규제 법안은 독재정권에 의한 감시사회의 우려를 안고 있다.

이미 민주화 된 국가에서 무슨 독재냐고 반문하겠지만 그것은 오산이다. 잘못된 권력이나 국가의 등장은 예견되어 있는 것이 아니다. 권력이 법률을 무기로 시민권을 제한하고 정치인과 언론인, 학자들을 사찰하고, 감시한다면 과연 민주사회라고 할 수 있을까? 따라서 인터넷과 통신관련 법안 개정은 단순히 정당간의 색깔차이 내지는 진보냐, 보수냐의 문제가 아니다. 바로 한국이 감시사회로 가느냐 아니면 지금과 같이 자유민주주의 사회에서 감시받지 않고 자유를 누리며 살 것이냐의 갈림길이다.

감시사회에 대한 우려는 결국 스스로 만든 법안에 스스로 감시당할 수 있는 부메랑이라는 점에 있다. 그것이 비록 정책결정권자가 의도하지 않았을 수도 있지만 중요한 것은 의도하건, 의도하지 않건 나타나는 결과는 인터넷 감시사회가 될 것이란 점이다. 지금 현재 법률안을 찬성하는 이들도 잘못한다면 결국 그 법률로 인해 감시당할 수 있는 것이 현재의 개정안이다. 이는 의도하지 않게 스스로를 옥죄는 부메랑 효과가 나타날 것이 자명하다.

이러한 감시사회가 예견되는 상황에서 보다 진중하고 고민해야 할 것은 장기적인 대책의 마련이다. 단기적인 처방이 반짝 효과는 낼 수 있지만 결국 그것이 모든 것을 해결하지는 못한다. 현재와 같은 강력한 규제 드라이브보다는 규제와 윤리교육, 진흥을 동시에 추구하고 사회적 책임성을 강조하는 합리적인 인터넷 및 통신 정책이 필요하다. 현재의 관련 법안은 과도한 시장부담과 중소기업에 대한 부담으로 귀결될 소지가 다분하다. 그리고 이들은 결국에는 시장규제의 주체가 된다는 점은 더욱 심각하다. 다시 강조하건대, 인터넷 규제 프레임은 재구조화하는 것은 규제원리와 권한의 분배 등의 차원, 그리고 행위자인 국가와 시장, 시민사회의 간의 역량과 권력구조 등의 교집합 속에서 형성되어야 한다.

중요한 것은 기술을 이용하는 것은 인간이라는 점이다. 기술은 가치중립적이고 사용하는 인간과 사회적인 구조와 맥락에 따라 재구성된다. 당장 눈앞의 정략과 이익에 따라 인터넷과 통신을 규제한다면 그 피해는 상상을 할 수 없을 정도로 내일 닥칠지도 모른다. 따라서 규제를 해야 한다면 그 문제점과 파급효과에 대한 다각적인 접근이 필요하고 영향과 문제에 대한 분석이 선행되어야 할 것이다. 그렇지 않고 일부 부정적인 사안에 대해 모두 법제화하고 규제한다면, 결국 인간의 자유권은 말할 것도 없고 사소한 행동자체가 모두 규제와 감시 대상이 되는 감시사회를 우리는 경험하게 될 것이다(Castells, 2001).

< 참고 문헌 >

- 강상현. 2006. “디지털 시대의 미디어 기술과 사회 변화,” 한국언론정보학회 엮음. 『현대사회와 매스커뮤니케이션』. 파주: 한울아카데미.
- 고민경. 2009. “중국 공산당, 인터넷과의 전쟁,” <http://www.umediajournal.com/entry/view.aspx?id=164&category=1000> (검색일: 2009년 4월 7일).
- 김상배. 2008. 『인터넷 권력의 해부』. 파주: 한울.
- 레식, 로렌스. 김정오 역. 2000. 『코드: 사이버공간의 법이론』. 서울: 나남.
- 민병원. 2005. 『복잡계로 풀어내는 국제정치』. 서울: 삼성경제연구소.
- 배영. 2008. “UCC와 네트워크 사회,” UCC문화미디어 & 융합기술연구소 세미나 자료집.
- 서키, 클레이. 2008. 『끌리고 쏘리고 들끓다』. 서울: 갈리온.
- 송경재. 2009. “인터넷 관계법 개정의 문제점,” 『시민과 언론』
- 오웰, 조지, 정희성 역. 2003. 『1984』. 서울: 민음사.
- 정보통신부/방송통신위원회. 2009. “08년 하반기 감청협조, 통신사실확인자료 및 통신자료 제공 현황”
- 푸코, 미셸, 오생근 역. 2003. 『감시와 처벌』. 서울: 나남출판.
- 한국데이터베이스진흥센터. 2006. 『웹 2.0은 지식정보 해방공간인가?』. 서울: 커뮤니케이션북스.
- 홍성욱. 2002. 『파놉티콘-정보사회 정보감옥』. 서울: 책세상.

뉴스검색서비스 KINDS <http://www.kinds.or.kr/>

- Atton, Chris. 2007. *An Alternative Internet: Radical Media, Politics and Creativity*. 민인철·반연 옮김. 『얼터너티브 인터넷』. 서울: 커뮤니케이션북스.
- Bell, Daniel. 1973. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. New York: Basic Books.
- Benkler, Yochai 2006. "The Wealth of Networks: How Social Production Transforms Markets and Freedom," <http://www.benkler.org> (검색일: 2008년 1월 20일).
- Castells, Manuel. 2001. *The Internet Galaxy : Reflections on the Internet, Business, and Society*. Oxford University Press.
- _____. 2000. *The Rise of the Network Society*. Blackwell Publishers.
- Chadwick, Andrew. 2006. *Internet Politics: States, Citizens, And New Communication Technologies*. Oxford University Press.
- International Herald Tribune. 2008년 2월 5일
- Gandy, Oscar. H. 1989. "The surveillance society: Information technology & bureaucratic social control," *Journal of Communication*, 39(3), pp.61-76.
- Goldsmith & Wu, 2006. *Who Controls the Internet?: Illusion of a Borderless World*. New York: Oxford University Press.
- Mathiesen, Thomas. 1997. "The Viewer Society: Michel Foucault's Panopticon Revisited," *Theoretical Criminology*, Vol. 1, No. 2.
- RAND. 2002. *Poor Connection: Trouble on the Internet Frontiers*. Santa Monica, CA: RAND.
- Toffler, E. 1980. *The third wave*. New York: Bantam Books.
- van Dijk, Jan. 1999. *The Network Society: Social Aspects of New Media*. London: Sage.