

U-컴퓨팅의 사회문화적 수용: 프라이버시 보호의 관점에서 본 전망과 대책

윤 영 민*

요 약

유비쿼터스 컴퓨팅은 정보주체의 자기정보관리를 요구한다. 우리나라에서는 최근 프라이버시 보호에 관해 몇 가지 주목할만한 진전이 있었지만 아직 정보주체의 자기정보관리를 효과적으로 뒷받침할 수 있는 법제도나 기술개발이 충분히 이루어지지 못하고 있는 실정이다. 특히 사회적 신뢰는 매우 낮은 수준에 있다. 만약 지금 상태로 u-컴퓨팅 시대를 맞이한다면 우리사회는 심각한 혼란에 빠지게 될 지도 모른다. 국가적으로 프라이버시 보호에 관한 획기적인 대책이 요구된다. 선도적 집단들은 우리 사회의 신뢰수준을 높이는데 진력해야하고 정부는 관련 법제도 정비와 PETs 개발에 적극 나서야 할 것이다.

I. 서 론

10여 년 전부터 정보사회학자들은 '네트워크 사회'의 도래를 예견했다. 사회의 모든 구성 조직과 구성원들이 통신네트워크로 촘촘히 연결되면서 중심이 없는, 혹은 다중심의 매트릭스 구조로 된 사회가 출현하리라는 것이었다^[7].

최근 논의가 분분한 유비쿼터스 컴퓨팅은 바로 그 네트워크 사회가 실제로 구현되는 기술 환경을 가리키는 것으로 이해된다. 언제 어디서나 어떤 맥락에서든 통신이 가능한 네트워크 환경을 말하는 것이다.

기술적인 측면에서 보면 유비쿼터스 컴퓨팅은 더 이상 은유(metaphor)가 아니라 이미 실제(reality)로 우리 앞에 놓여 있다. RFID 태그, IPv6, 스마트카드, 멀티미디어 휴대단말기 등 아직 완성된 모습은 아니지만 그것의 구현에 필요한 기반 기술과 요소 기술은 무서운 속도로 발전해가고 있다.

문제는 '프라이버시'라는 깊은 강을 어떻게 건널 것인가이다. 사용자가 언제든 어느 곳에서나 통신 네트워크에 몰려 있다는 것은 한편으로는 엄청난 편의를 가져오지만 다른 한편으로는 사적(私的) 공간의 해체를 수반하기 때문이다. 개체든 사용자든, 정지하고 있

던 움직이고 있던, 지속적으로 외부세계와 통신하기 위해서는 유무선 네트워크를 통해 끊임없이 나의 세계를 타인의 세계와 접속시켜야 한다^[2,9].

동전의 양면처럼 분리가 불가능해 보이는 이 문제를 풀지 않고는 유비쿼터스 컴퓨팅 환경에 기반을 둔 미래의 네트워크 사회가 바람직한 모습으로 실현될 수는 없을 것이다. 최근 프라이버시에 관한 우리 사회의 경험을 보면 그 냉엄한 진실을 감추거나 호도하면서 네트워크 시대로 들어갈 수 없다는 사실이 명백해진다.

이 글에서는 최근에 프라이버시와 관련해 진행되고 있는 현안과 논쟁을 짚어보고 프라이버시 문제의 해결을 위해 필요한 조건을 제시하고자 한다. 그렇게 함으로써 유비쿼터스 컴퓨팅과 프라이버시 보호의 문제를 추상적 논쟁이 아니라 구체적인 역사적 맥락 속에서 바라보고자 한다.

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환하고 있다.

II. 프라이버시, 2003년

국내외적으로 지난해는 프라이버시 보호의 관점에

* 한양대학교 언론정보대학 정보사회학전공(youngmin@ihanyang.ac.kr)

서 결코 산뜻한 출발이 아니었다. 미국의 9.11 사태로 말미암아 테러로부터 국가와 국민의 안전을 지키는 것-즉, 안보-가 무엇보다 중요하다는 사회적 분위기가 형성됨으로써 적어도 당분간 프라이버시 보호에 관한 목소리가 안보와 안전에 대한 강조 뒤에 가려지게 되었다.

국내에서도 소위 1.25 인터넷 대란은 해킹에 대한 대비의 중요성을 법사회적으로 인식시키는 계기가 되었다. 그러나 그로 인해 프라이버시(privacy)가 보안(security) 담론에 상당부분 밀려나는 형국이 되었다.

사실 네트워크에서 프라이버시 보호는 보안 기술과 정책에 크게 의존하고 있다. 개인정보에 대한 부적절한 접근, 모니터링, 이전, 저장 등의 문제는 암호화, 접근제어 등의 보안 기술과 정책에 의해 상당부분 해결된다.

그러나 동시에 보안 기술과 정책은 과도한 개인정보 수집, 정보주체의 접근제한, 모니터링 등을 수반하기 때문에 프라이버시 침해를 초래할 수 있다. 예컨대 사무실에 설치된 CC-TV는 근로자의 수치심을 유발하거나 심리적 위축을 가져올 수 있다. 또한 접근제어는 정보주체의 권리를 심각하게 제한할 수 있다. 접근제어 기술과 정책은 흔히 정보주체들이 타인의 정보에 접근하는 것 뿐 아니라 자기정보에 대한 접근도 제한하게 되기 때문이다.

연초에 프라이버시 보호에 관한 담론의 출발이 가법지는 않았지만 NEIS(교육행정종합정보시스템) 구축, 주택가 골목 CC-TV 설치 등 여러 가지 정책 현안, 공공기관개인정보보호에관한법률의 개정 등 정부의 입법 활동과 그에 대한 시민단체들의 대응, 그리고 주민등록번호 도용과 스팸으로 인한 네티즌들의 피해 등 여러 가지 계기들 덕분에 연중 내내 국민들의 관심을 비교적 잘 묶어둘 수 있었다.

아마도 지난해는 우리나라에 프라이버시에 관한 논쟁이 가장 뜨겁게 달아올랐던 한 해로 기록될 것이다. NEIS만 해도 교육현장을 혼란스럽게 하여 영문을 모르는 적지 않은 국민들을 짜증나게 만들기는 했지만 단시간 내에 국민들의 프라이버시에 대한 인식을 제고하는 데 있어 수백억 원의 TV광고보다도 더 큰 기여를 했다고 생각된다. 프라이버시를 국민들 관심의 전면에 부각시키는 효과를 가져 온 것이다. 2003년은 프라이버시 보호가, 전문가들 사이에서 논의되는 추상적인 쟁점에서, 일반 국민들이 피부로 느낄 정도의 구체적인 현안으로 전환되는 분수령이었다고 할 수 있을 것이다.

III. 프라이버시 보호의 현안과 쟁점

먼저 개인정보의 오·남용과 관련해서는 주민등록번호의 악용이 가장 먼저 떠오른다. 우리나라에서 국민이면 누구나 갖게 되는 주민등록번호는 대표적인 ID이며 전자상거래에 광범위하게 이용되고 있다. 거의 대부분의 인터넷 사이트들이 회원가입 때 주민등록번호입력을 필수항목으로 요구하고 있으며, 이름과 함께 회원가입자나 서비스 이용자의 실명 확인 혹은 성인 인증에 사용한다.

미국 보스턴 소재의 리서치 기관인 에버던 그룹(Aberdeen Group)의 보고서에 따르면, 운전면허번호, 사회보장번호 등과 같은 ID의 절도로 인해 정부나 기업, 그리고 개인이 입는 재정적 피해가 2003년 한 해만도 세계적으로 약 2,210억 달러에 달한 것으로 추정된다⁽⁶⁾. 우리나라에는 유사한 통계가 없지만 우리나라가 보편적 ID 제도를 시행하면서 인터넷 이용률이 가장 높은 국가 중 하나라는 점을 고려할 때 아마도 ID 절도에 의한 재정적 피해가 대단히 심각한 수준일 것으로 추측된다.

2003년 한국정보보호진흥원의 조사에 의하면, 조사에 참여한 448개의 업체 중 447개의 사이트가 회원가입 때 주민등록번호를 요구하고 있으며, 500명의 네티즌 중 20%가 주민등록번호를 도용당한 경험이 있고, 12%가 타인의 주민등록번호를 도용한 경험이 있는 것으로 나타났다⁽⁵⁾. 또한 2003년 한 해 동안 한국정보보호진흥원의 개인정보침해신고센터에 접수된 신고·상담 약 2만 건 중 25% 정도인 4천 건 이상이 주민등록번호 도용과 관련된 것으로 파악된다⁽⁵⁾.

주민등록번호의 도용과 관련된 네티즌들의 그러한 경험은 우리 사회에 개인정보보호에 대한 인식이 단기간 내에 매우 높아졌음을 시사한다. 많은 사람들이 주민등록번호가 유출되면 자신이나 자신이 속한 기업이 재정적 손실을 입을 수 있을 뿐 아니라 자신의 의사와 반해서 사생활이 공개되는 피해를 입을 수 있음을 깨달은 것이다. 하지만 개인정보침해에 대한 우려가 잘못된 대응을 초래하고 있다. 아이러니컬하게도 적지 않은 사람들이 자신의 주민등록번호가 유출될까 두려워 남의 주민등록번호를 도용하고 있는 것이다.

주민등록번호 도용의 사회적 심각성은 지금 시점에서 우리로 하여금 주민등록번호 제도를 유티쿼터스 컴퓨팅 시대에 가지고 들어갈 것인가를 고민해보도록 일깨워 준다. 우선 보편적 ID로서 주민등록번호라는 제도 자체를 유지할 것인가, 아니면 그것을 폐지하고 다

소 불편하지만 프라이버시 침해 가능성이 낮은 ID 제도를 채택할 것인가를 원점에 놓고 검토해 보아야 한다. 또한 만약 주민등록번호 제도를 유지한다면 현재와 같은 상업적 이용을 계속 허용할 것인가도 고민해 보아야 한다. 주민등록번호제도가 유비쿼터스 컴퓨팅에 꼭 필요하다면 그것의 잠재력을 살리면서 동시에 그것의 오용으로 인한 피해를 최소화할 수 있는 방안을 마련해야 할 것이다.

최근에는 개인정보의 악용뿐만 아니라 스팸(spam) 메일과 인스턴트 메시징 스팸도 사람들의 업무나 휴식을 방해하는 심각한 프라이버시 침해 유형으로 등장했다. 2003년 11월 유엔국제무역개발기구(UNCTAD)는 연말까지 세계 모든 전자우편의 약 50%가 스팸 메일로 채워질 것이며 그 같은 기술 자원 낭비를 금액으로 따지면 무려 205억달러에 달할 것이라고 경고했다⁽¹⁰⁾.

정보통신부가 발행한 '2003정보통신백서'에 따르면 우리나라에서 1인당 1일 스팸 메일 수신량은 2001년 5통에서 2002년에는 35통, 2003년에는 40통으로 8배정도 증가했다. 또한 2003년 스팸 메일의 91.6%가 음란물 광고, 불법복제 등 불법컨텐츠 광고로 나타났다.

최근에는 인스턴트 메시징 스팸-스팸(spim)이라고도 불린다. 이 네티즌들을 괴롭히고 있다. 미국의 컨설팅 업체인 웨리시리시치는 2003년 한 해 동안 세계적으로 약 5억 개의 스팸이 발송되었다고 추산했다⁽⁴⁾. 이는 매일 20억 개 가량 발송되는 스팸 메일에 비하면 매우 적은 양이지만 스팸은 시도 때도 없이 불쑥 불쑥 튀어나와 업무도중 산만하게 되고 짜증을 받게 되기 때문에 스팸보다 더 심각하게 업무를 방해한다.

휴대폰 문자메시지 스팸도 스팸 메일이나 스팸 못지않게 프라이버시 침해의 심각성을 일상생활 속에서 절실하게 느끼게 해 주었다. 검찰 발표에 따르면 2003년 한 해 동안 휴대폰 스팸 메시지는 25억 5천만 통이 발송되었으며, 그중 80%정도가 폰팅업체에 의해 발송된 음란전화나 음란사이트 광고였다⁽⁵⁾.

스팸은 개인의 전자우편 주소나 휴대폰 번호가 불법적으로 수집되거나 부당하게 활용되었다는 점에서 개인정보침해 문제의 일부로 다루어지지만 일반적으로 그 자체가 개인정보침해로 간주되지는 않고 있다. 그러나 앞으로 스팸은 개인의 사적 공간에 대한 부당한 침입으로서 개인정보침해 행위로 해석되어야 할 것이다.

만약 획기적인 기술적 그리고 사회적 대책을 마련하지 않는다면 유비쿼터스 환경에서 스팸과 같은 사적 공간의 침해 현상은 더욱 심각해 질 것이다. 어쩌면 스팸이야말로 유비쿼터스 환경에서 발생하게 될 프라

이버시 침해를 일반인들이 미리 체험해볼 수 있게 해 주고 있는 지도 모른다. 과연 유비쿼터스 컴퓨팅의 혜택을 누리기 위해서는 국민과 소비자가 사적 공간의 침해를 꼭 감수해야 하는 것인가? 만약 u-컴퓨팅을 위해 사적 공간의 개방이 필연적이라면 그것이 어느 정도나 어떤 방식으로 허용되어야 하는 것인가에 대한 사회적 합의도 필요하고, 사적 공간의 관리를 뒷받침하는 기술도 개발되어야 할 것이다⁽⁹⁾.

최근에는 CC-TV에 의한 프라이버시 침해 가능성도 주목을 받았다. 사실 CC-TV가 공장이나 백화점 등 작업장을 모니터링하기 위해 사용된 것은 상당히 오래된 일이다. 그런데 2003년에는 CC-TV가 주택가, 전철, 도서관 등 공공장소에 확대 설치됨으로써 그것의 프라이버시 침해 가능성이 사회적 쟁점으로 부상하였다.

강남구청은 밤길에 보행자들의 안전을 보호하기 위해 골목길에 CC-TV를 설치하기로 결정하였고 논현동 주택가 4곳에 시범사업을 시작하였다. 이 결정은 CC-TV에 의한 프라이버시 침해 문제에 관해 국민들의 관심을 불러일으켰다. CC-TV가 범죄를 예방하는 데는 도움이 되겠지만, 그것이 모든 주민을 잠재적 범죄자로 간주할 뿐 아니라 촬영된 필름이 불법 유출될 경우 주민의 프라이버시 침해를 초래할 수 있다는 점에서 논란의 대상이 된 것이다⁽⁶⁾.

또한 서울지하철공사는 CC-TV를 서울 지하철 1-4호선의 전 객차에 설치하여 운전실과 역무실, 종합사령실에서 객차 내 상황을 감시토록 하여 비상상황 발생시 승객들의 안전을 도모하겠다는 계획을 발표하였다. 서울지하철공사의 이 계획에 대해서도 적지 않은 승객들과 직원들이 반발하였다. 승객들의 프라이버시를 침해할 소지가 있을 뿐 아니라 직원들의 노동을 감시하여 노동강도를 높일 가능성이 있다는 것이다⁽⁵⁾.

다소 오래되기는 했지만 CC-TV에 관해서는 대학가에서도 논란이 일었다. 서울대학교에서는 이용자들의 소지품 도난 및 분실 사고의 예방을 위해 도서관에 CC-TV를 설치해야하는가를 둘러싸고 대자보 논쟁이 벌어졌다. 도난방지를 위해 CC-TV를 설치하자는 의견과 도서관 이용자들의 프라이버시가 침해되기 때문에 설치해서는 안 된다는 의견이 팽팽하게 맞섰다⁽⁵⁾.

CC-TV는 감시도구로서 그것이 지닌 편리함과 효과 때문에 더욱 확산될 것이고 앞으로 계속 논란의 대상이 될 것으로 보인다. CC-TV에 관해서는 프라이버시 보호의 관점에서 아직 설치 기준이나 보관 자료의 처리 기준 등이 마련되어 있지 않다.

CC-TV는 그 자체도 중요한 논쟁거리이지만, 나아가 앞으로 국민과 소비자가 처하게 될 정보기술의 혜택과 감시(surveillance)의 강화라는 딜레마를 상징적으로 보여준다. CC-TV의 경우 안전이나 도난방지가 기대되는 혜택이 되지만 다른 정보기술은 시간절약, 경비절감, 고객지향 서비스 등과 같은 편의를 가져오면서 동시에 감시의 부작용을 수반할 수 있다.

영국의 사회학자 안소니 기던스의 지적처럼 현대 복지국가는 출발부터 감시사회였는지도 모른다⁶⁾. 국가가 국민들에게 높은 수준의 복지서비스를 제공하기 위해서는 당연히 복지수혜자인 국민 개인에 대한 많은 정보가 필요하다. 그런 점에서 감시가 반드시 부정적인 것만도 아니다.

어쩌면 네트워크 사회를 살아가야하는 현대인에게 감시는 저항이 아니라 관리의 대상인지도 모른다. 많은 사람들은 감시가 통제의 수단일 수 있기 때문에 그것을 두려워한다. 만약 감시가 가져오는 긍정적인 복지효과를 극대화하는 반면 그것이 가져오는 부정적인 통제효과를 최소화할 수 있는 기술적 혹은 사회적 대안을 찾을 수 있다면 감시를 우리가 마냥 기피할 이유는 없을 것이다. 미래의 u-컴퓨팅 환경을 구현하기 위해 우리가 풀어야할 숙제 중 하나는 바로 그 대안을 찾는 작업이 될 것이다.

2003년 후반에는 지난 1998년 전자주민카드, 2001년 전자건강보험증 도입을 둘러싸고 사회적 논란을 불러 일으켰던 스마트카드 논쟁이 다시 수면위로 떠올랐다.

지난 해 6월 KAIST 지식기반전자정부연구센터, 삼성 SDS, LG CNS, 서오 텔레콤 등 SI업체와 은행, 카드사 등 금융기관이 공동으로 스마트카드 컨소시엄을 구성하고 정부를 견인하여 공공부문에 스마트카드 도입을 추진하겠다고 나섰다⁵⁾. 국내 시장 형성을 통해 궁극적으로 세계 스마트카드 시장을 선점하려는 업계의 강력한 욕구가 반영된 것이다.

이미 민간부문에서는 스마트카드가 적지 않게 사용되고 있다. 케이캐시(K-Cash), 몬덱스(Mondex) 등 전자화폐의 사용이 꾸준히 증가하고 있으며, 여러 대학들은 스마트카드 신분증을 도입하고 있고, 일부 기업은 사원증으로, 병원은 진료카드도 이용하고 있다. 공공부문에서는 스마트카드 형태의 공무원신분증이 시범적으로 운용되고 있으며 여러 지방자치단체들이 스마트카드 형태의 교통카드를 도입하고 있다. 우리나라는 이미 세계 최고 수준의 교통카드 활용국이다.

지난 해 하반기에는 금년에 착수될 스마트카드 사업들이 속속 발표되었다. 2004년 4월에는 은행들이

금융IC카드 발급을 시작할 예정이고, 6월에는 서울신교통카드가 도입될 예정이며, 12월에는 한국도로공사가 하이패스카드 시범사업을 실시한다는 것이다⁵⁾.

새해 벽두에는 한·중·일 3국을 주축으로 추진되는 '실크로드 카드' 프로젝트가 발표되었고, 국무회의에서는 2006년을 목표로 전자건강보험증 도입이 추진되는 내용이 포함된 '참여복지 5개년 계획'이 확정되었다. 실크로드 카드 프로젝트는 민간이 중심이 되어 스마트카드를 이용해 아시아를 하나의 통화권으로 묶겠다는 야심찬 계획이다. 그 프로젝트에는 싱가포르와 홍콩도 참여할 예정이며, 1차적으로 전자여권의 일종인 전자통행카드를 5개국에 통용시킬 계획이다⁵⁾.

스마트카드는 프라이버시 보호에 있어 중대한 도전이다. 스마트카드를 사용하게 되면 개인정보의 광범위한 공유를 통해 각종의 편의를 얻게 되는 반면 익명성의 영역은 그만큼 줄어들기 때문이다. 어쩌면 그것은 우리 사회가 개인들이 자기정보를 소극적으로 보호하는 시대로부터 적극적으로 관리하는 시대로 전환되고 있음을 의미하는 지도 모른다. 동일한 맥락에서 유비쿼터스 컴퓨팅 시대는 한마디로 정보주체의 자기정보 관리 시대라고 집약적으로 표현할 수 있을 것이다.

프라이버시와 관련해서 2003년이 저무는 시점에서 세계인들의 주목을 받은 사건은 무엇보다 미국 당국이 2004년 1월 5일부터 테러방지를 위해 무비자입국을 허용하는 28개국 입국자들을 제외하고 모든 입국자들에 대해 지문채취와 얼굴사진촬영을 시행토록 한 조치이다.

앞으로 특정 영역 혹은 특정 목적의 신분확인에 있어 생체인식 기술의 도입은 불가피할 것으로 예상된다. 그러나 신분확인에 있어 그것이 지닌 확실성만큼이나 프라이버시 침해의 가능성과 그것으로 인한 피해도 심각해질 것이다. 이미 민권단체들은 미국당국의 그러한 조치가 테러예방에는 실효성이 없고 수집된 개인정보들이 원래 목적 이외의 용도로 활용됨으로써 프라이버시를 침해할 우려가 있다고 비판한다⁵⁾.

현재 미국사회에 안보논리가 프라이버시보호 주장을 압도하고 있기 때문에 이 조치는 당분간 계속될 것으로 예상된다. 그러나 장기적으로 결국 그 조치의 성패는 누가, 어떤 정보를, 어떤 방식으로 수집해서, 어떻게 이용하는가에 관한 문제가 어떻게 풀리는가에 달려있을 것이다. 즉 안보정책과 프라이버시 보호 정책을 조화시키는 능력이 그 정책의 성패를 좌우하게 될 것이다.

미국의 조치에 대한 브라질을 비롯한 여러 나라의

반응을 보면 프라이버시 침해의 문제는 특정 국가나 집단이 일방적 결정할 수 있는 사안이 아님을 알 수 있다. 앞으로 프라이버시 보호 문제는 국제적 협력을 통해서 풀릴 것이고 우리나라는 이 영역에 있어 선도국가가가 되도록 노력해야 할 것이다. 유비쿼터스 컴퓨팅 시대의 지도자(혹은 지도국가)는 프라이버시 보호에 관한 높은 식견과 정책의지를 가진 자가 될 것이다.

IV. 프라이버시 보호 대책

최근 프라이버시 침해가 사회적 현안으로 부상함에 따라 그에 대한 국가적 대책을 요구하는 목소리도 힘을 받고 있다. 시민·사회단체들은 프라이버시보호기구의 설립을 요구하고 나섰다. 정책 당국도 이 문제의 심각성을 인식하고 법제도 정비를 추진하고 있다.

공공부문에 관해서는 행정자치부가 공공기관의개인정보보호에관한법률의 개정을 통해, 민간부문에 관해서는 정보통신부가 정보통신망이용촉진및정보보호등에관한법률을 개정하여 각각 프라이버시 보호를 강화하려고 시도하였다. 또한 대통령 자문 정부혁신지방분권위원회 소속 전자정부전문위원회는 대통령의 지시를 받고 프라이버시보호를 위한 종합적인 대책 수립에 나섰다.

아마도 프라이버시 보호 정책의 추진에 있어 가장 강력한 원동력을 제공한 사건은 NEIS를 둘러싼 갈등일 것이다.

2002년 가을부터 시작된 NEIS의 도입을 둘러싼 교육계의 갈등은 2003년 마지막 순간까지 국민의 관심을 끌었다. 초점은 NEIS가 지닌 프라이버시 침해 가능성이었다. 교육, 입·진학, 보건의 3개영역에 관한 정보 집적으로 NEIS가 인권을 침해할 우려가 있다는 국가인권위원회의 판결은 정보프라이버시가 인권의 중요한 부분임을 국민들에게 인식시키는 계기가 되었다.

실제로 NEIS 문제를 해결하는 과정에서 여러 가지 프라이버시 보호 제도에 관한 논의가 탄력을 받게 되었다. 독립적인 프라이버시보호기구의 설치, 프라이버시 영향 사전평가제, 심지어 공공부문에 있어 개인정보삭제청구권의 도입 등이 논의되었다. NEIS 문제를 계기로 정부는 대통령의 지시에 따라 공공기관에 의한 개인정보의 수집과 이용에 관한 실태를 파악하고 대책을 수립하는 작업에 착수하기도 했다.

NEIS 문제를 푸는데 있어 합의가 가장 어려웠던 부분은 소위 통합론과 분산론의 충돌이었다. 교육인적

자원부는 16개시도 지역별로 D/B를 구축하여 상호연동 시키더라도 제도적 장치와 기술적 해법이 충분히 뒷받침되면 효율성과 프라이버시보호라는 두 가지 가치를 동시에 구현할 수 있다고 주장하였다. 반면에 전국교직원노동조합은 학생들의 개인정보가 그것의 수집과 관리에 일차적 책임을 가진 각 학교의 담장을 넘어서 공유되면 필연적으로 학생들의 인권 침해를 낳게 된다고 주장하였다.

NEIS 논쟁은 우리 사회에 정보시스템의 통합과 분산에 관해 쉽게 조화될 수 없는 시각이 병존하고 있다는 사실을 보여주었다. 특히 그 대립은 정부에 대한 뿌리 깊은 불신의 결과이기도 했다.

1. 개념적 발전

근래에 대두되었던 프라이버시 보호에 관한 현안들을 돌이켜보면 프라이버시를 위호한 개념적 인식이 점차 정교해 지고 있음을 알 수 있다. 다시 말해 개인정보보호란 뜻이 D/B에 수집된 개인정보가 부당하게 유출되거나 오·남용되는 것을 방지한다는 비교적 단순한 의미에서 벗어나고 있다.

첫째, 개인정보보호는 수집에서부터 보관, 관리, 이용, 이전, 그리고 폐기에 이르기까지 개인에 관한 정보가 사회적으로 활용되는 모든 과정과 방식에 관해 개인정보에 관한 정보주체의 권리가 어떻게 보장될 수 있는가라는 의미로 확대되었다.

둘째, 개인정보보호의 의미가 그렇게 확대됨으로써 프라이버시 개념을 그 안에 포섭하게 되었다. 프라이버시도 오랫동안 '홀로 남아 있을 권리' 혹은 '사생활의 보호'라는 좁은 의미로 해석되었으나 최근에는 정보주체의 자기정보결정권이라는 의미로 해석되는 경향이 있다. 프라이버시가 개인이 자신의 어떤 정보가, 누구에 의해, 어떻게 수집되고, 어떻게 보관되며, 어떻게 이용되는가에 대해 스스로 결정할 수 있는 권리로 인식된다는 말이다.

이러한 개념적 변화에서 가장 주목할만한 경향은 프라이버시 보호에 관한 담론에서 정보주체라는 존재가 확실히 자리 잡기 시작했다는 사실이다. 다시 말해 정보주체가 정보소유자로부터 구분되고 정보주체의 권리가 새롭게 인식되고 있다는 것이다. 이는 우리사회가 개인정보를 담고 있는 수많은 데이터베이스에 의존해서 움직이는 정보사회-그래서 어떤 학자들은 그것을 데이터베이스 사회라고도 부른다-로 전환됨에 따라 나타나는 자연스런 인식변화이다.

데이터베이스가 발달하지 않았던 과거에는 정보소유자와 정보주체의 구분이 사실상 불필요했다. 개인정보의 오·남용이란 연예인이나 정치인과 같은 사회적 저명인사의 사생활 폭로가 대부분이었고 따라서 그 피해도 대체로 그들에게 국한되었기 때문이다. 그러나 수많은 데이터베이스가 일반대중의 개인정보를 담고 있고 그것의 상업적 활용이 일상적으로 벌어지는 작금의 상황에서는 정보주체를 정부, 기업, 혹은 단체 등 데이터베이스 소유자로부터 구분해서 그 권리를 인정하고 보호해 주어야 하게 된 것이다.

그러나 정보주체의 자기정보결정권이란 개념이 법규범으로서 정착하기 위해서는 앞으로 가야할 길이 멀다. 정보주체의 자기정보결정권을 불가침의 인권으로 이해해야 하는지 아니면 거래나 제약 또는 위임이 가능한 권리로 보아야 하는지, 정보주체와 정보소유자 각각의 권한은 어디까지인지, 개인정보의 수집과 이용에 있어 정보주체의 동의는 어떻게 받아야 하는 것인지, 개인정보를 상업적으로 이용하는 경우 각각의 정보에 대해 어떻게 또 얼마를 보상해 주어야 하는 것인지, 공공부문이나 민간부문에서 개인정보삭제청구권은 어디까지 인정해야 하는 것인지 등 많은 쟁점들이 학술적 연구, 사회적 논쟁, 입법, 재판 등 사회적 과정을 통해서 풀어야 할 것이다.

2. 법제도의 개선

지난해에는 프라이버시 보호를 위한 법제도 마련에 대한 논의는 비교적 활발했지만 실제로 제도화에 획기적인 진전은 없었다.

가장 주목할 조치로, 3월에 정보통신부가 개인정보 보호를 위한 온라인 개인정보 취급관리 가이드라인을 발표하고 정보통신업체, 호텔, 여행사 등 다량의 개인정보를 취급하는 업체들에게 그것의 준수를 요청하였다. 그 가이드라인은 개인정보를 안전하게 관리할 조직·인력·규정의 운영, 개인정보의 별도 관리, 개인정보보호 영향 사전 평가 등의 내용을 담고 있다^[5].

연말에는 정보통신망이용촉진및정보보호등에관한법률이 개정되어 프라이버시보호를 위한 몇 가지 주요한 제도적 개선이 이루어졌다.

첫째, 정보주체가 정보통신서비스제공자에게 자신의 개인정보에 대한 열람 뿐 아니라 개인정보를 이용하거나 제3자에게 제공한 내역을 요구할 수 있도록 하였다. 이는 정보주체의 자기정보결정권을 더욱 강화하는 조치로 해석된다.

둘째, 개인정보침해사건 발생시 신속하고 공정한 구제를 위해 개인정보분쟁조정위원회에 5인 이하의 위원으로 구성된 조정부를 두고 일부 분쟁에 대해서는 조정부에 일임토록 하였다. 정보통신부는 이 조정부제의 도입으로 1건당 평균 처리기간이 현행 64일에서 30일로 단축되고, 월평균 피해구제건수는 현행 39건에서 70건으로 확대될 수 있을 것으로 예상했다.

셋째, 수신자의 거부사에도 불구하고 불법적인 스팸 메일을 발송한 사람에 대한 처벌이 강화되었다. 즉, 위반자에 대한 과태료가 현행 1천만원 이하에서 3천만원 이하로 크게 늘어났다.

스팸 메일에 대해서는 이밖에도 정보통신부차관을 위원장으로 하는 '민관합동 스팸메일대책위원회'가 구성되어 적극적인 방지 대책 마련에 나서고 있다^[5].

지난해 비록 법제화까지는 이르지 못했지만 프라이버시 보호를 위한 여러 가지 획기적인 방안들이 논의되었다는 사실은 대단히 중요한 의미를 지닌다. 그 논의는 금년에도 지속될 것이며 몇 가지 대안은 실제로 법제화될 가능성이 높기 때문이다.

우선 주민등록번호의 오·남용을 막아야 한다는 대해서는 국민들 사이에 공감대가 널리 형성되어 있고 정부 일각에서 그에 대한 구체적인 정책 대안까지 제시되고 있다.

정보통신부는 정보통신사업자들이 회원모집시 주민등록번호를 수집하는 관행이 주민등록번호의 오·남용을 초래하는 경향이 크다는 사실에 착안하여, 정보통신사업자들에게 주민등록번호 대신 전자서명인증의 활용을 권장하고, 쇼핑몰, 게임사이트 등 전자상거래가 이루어지는 사이트에 대해서는 전자서명제도의 이용을 의무화하는 방안을 검토 중이다^[5].

실명확인과 성인인증을 위해 정부의 주민등록정보를 이용하는 관행에 대해서도 시민단체들이 꾸준히 문제를 제기하고 있어 대안 마련이 이루어질 것으로 보인다. 더구나 주민등록번호의 도용으로 인한 피해가 속출하고, 일부 시민단체는 주민등록번호 제도 자체의 폐기까지 요구하고 있기 때문에 어떤 방식으로든 주민등록번호 제도와 이용방식의 개선은 불가피할 것으로 예상된다.

2003년에는 연초부터 여러 곳에서 프라이버시 영향 사전평가제 도입의 필요성이 제기되었다^[5]. 앞에서 언급했듯이 민간부문에서는 정보통신부가 개인정보보호 가이드라인을 통해 정보통신업체들에게 그것의 시행을 적극 권장하고 있으며, 공공부문에서도 그것의 도입에 관한 주장이 지속적으로 제기되고 있다.

행정자치부는 공공기관의개인정보보호에관한법률 개정안에 프라이버시 영향 사전평가제 도입을 포함하고 있지는 않지만 앞으로 그것의 도입을 적극 검토하겠다는 입장을 밝혀 왔으며, 정보통신부는 범정부 ITA 구축을 위한 법안에 전자정부사업에 대한 프라이버시 영향 사전 평가제를 포함하는 것을 검토 중이다. 이러한 동향으로 볼 때 2004년 중에는 공공부문에도 프라이버시 영향 사전 평가제가 도입될 것으로 예상된다.

2003년에는 정보주체의 자기정보결정권을 강화하기 위한 몇 가지 주요한 제도적 방안들도 심도 있게 논의되었다.

그중 가장 비중 있는 주제는 독립적인 프라이버시 감독기구를 설치에 관한 것이다. 현행법규에는 프라이버시 감독기구에 대한 규정이 없고, 개인정보보호 제도가 공공부문과 민간부문으로 이원화되어 있다. 공공부문에는 공공기관의개인정보보호에관한법률에 따라 국무총리실 산하에 개인정보보호심의위원회가 설치되어 있다. 원래 법규에 그 위원회는 공공기관의 개인정보 보호정책에 관한 심의를 수행하는 것으로 되어 있지만 지금까지 활동은 미미하다. 민간부문에는 한국정보보호진흥원에서 운영하는 개인정보침해신고센터가 설치되어 있어 피해구제를 수행하고 있다. 이 센터는 개인정보침해에 대한 신고와 상담을 처리하기 위해 활발하게 운영되고 있지만 정책의 개발이나 심의 기능은 갖고 있지 않다.

실제로 현재까지는 프라이버시 보호에 관한 정책 개발과 집행 기능을, 공공부문은 행정자치부가, 민간부문은 정보통신부가 직접 수행해 왔다. 이점에 관해서는 비판의 목소리가 높다. 정보화 사업을 수행하는 부처들이 스스로에 대한 규제 기능을 수행해야 하기 때문에 프라이버시보호 정책을 적극적으로 수행하기 어렵다는 것이다. 때문에 시민단체들은 행정 부처들로부터 독립적인 프라이버시 감독기구가 필요하다고 역설하고 있다.

그 감독기구는 프라이버시 영향 사전 평가, 정책 개발과 심의, 정책 집행, 그리고 피해구제 등의 역할을 수행할 수 있을 것이다.

행정자치부가 마련한 공공기관의개인정보보호에관한법률 개정안은 이미 개인정보보호심의위원회의 기능을 강화하는 내용을 담고 있으며, 대통령 자문 정부혁신지방분권위원회 산하 전자정부전문위원회가 프라이버시 감독기구 설치를 포함한 프라이버시보호 대책을 마련 중에 있기 때문에 2004년에는 어떤 형태로든 프라이버시 감독기구가 구성될 것으로 예상된다.

NEIS 갈등을 푸는 과정에서 제기된 자기정보삭제 청구권의 도입 문제도 주목할 만하다. 민간부문에는 그것은 이미 법제화되어 있지만, 공공부문에는 아직 도입이 고려되지 않고 있다. 행정기관에 의한 개인정보수집은 언제나 법적 근거를 갖고 분명한 공공 목적을 갖고 수행되는데, 국민들이 선택적으로 그러한 개인정보수집으로부터 빠질 수 있게 하는 자기정보삭제 청구권은 행정행위를 무력화시킬 우려가 있다. 그러나 앞으로 정보주체의 자기정보결정권을 강화하는 과정에서 자기정보삭제청구권에 대한 논의는 다시 등장하게 될 것이며, 보다 깊은 연구와 다각적인 논의를 거쳐 제한적 수준에서나마 도입이 고려될 것으로 예상된다.

끝으로 스팸 메일과 관련하여 관계당국에 의해 옵인(opt-in) 제도의 도입이 검토된 것도 의미 있는 사건이다. 정보통신부는 이용자가 원하지 않는 불법적 스팸을 줄이는 방안의 하나로 이 제도의 도입을 검토하고 있다. 이 제도는 사전에 동의를 받은 사람들에게 한해 스팸을 발송할 수 있도록 하자는 것이다.

그 제도가 중소기업들의 기업활동을 위축시킬 수 있다는 우려 때문에 그동안 도입을 시도하지 않았지만, 이메일 중 스팸 메일의 비중이 갈수록 높아지는데다 스팸의 대부분이 음란물 광고라는 판단 때문에 정보통신부는 옵인 제도의 도입을 긍정적으로 검토하고 있는 중이다⁽⁵⁾.

3. 사회적 신뢰의 제고

현 시점에서 정부가 국민에게 자신을 전폭적으로 믿어달라고 주문하거나 기업이 소비자에게 그렇게 요구하는 것은 우리나라에서는 어쩌면 시기상조이다. 정부는 아직까지도 권위주의적 행태를 완전히 벗어나지 못하고 있으며, 끝없는 부정부패의 스캔들에 휩싸여 있고, 조령모개의 정책 집행으로 국민의 불신을 자초해 왔다. 그런 정부를 정권이 몇 번 바뀌었다고 국민들이 갑자기 신뢰해주리라 기대하는 것은 매우 비현실적이다. 기업의 형편도 대동소이하다. 과거에 비하면 기업들의 행태가 많이 나아졌지만, 기업의 이윤과 기업가의 이익을 위해서라면 환경파괴, 불량식품제조, 분식회계, 뇌물수수 등을 서슴지 않아 왔던 기업들을 소비자가 하루아침에 신뢰하게 되리라 기대하는 어렵다.

신뢰의 회복에는 노력과 시간이 필요하다. 공직자는 국민과의 약속을 지키기 위해 최선을 다하고, 자신이

나 자신이 속한 기관보다 국민의 이익을 우선시하는 행정문화가 들어서고, 기업에는 소비자를 두려워하고 소비자와 약속을 지키기 위해 최선을 다하는 기업문화가 정착할 때야 비로소 국민과 소비자는 정부와 기업을 신뢰할 수 있을 것이다. 그러한 문화가 형성되기까지는 공직자와 기업가의 많은 노력이 요구되며 상당한 시간도 필요할 것이다. 개인 사이에서도 깨어진 신뢰를 회복하려면 많은 노력과 시간이 필요한데, 하물며 국가와 기업의 경우는 어떠하겠는가.

사회적 신뢰가 빈약한 상태에서 추진되는 정보화는 그렇지 않은 경우보다 훨씬 많은 비용이 소요된다. 사실 어떤 부분의 정보화는 아주 불가능하기조차 하다. NEIS는 정부에 대한 국민의 신뢰가 낮기 때문에 엄청난 추가적 비용이 투입되지 않을 수 없는 상황에 처해 있으며, 전자주민카드나 전자건강보험증과 같은 스마트카드 도입 정책은 아예 좌절되고 말았다.

NEIS의 경우 그것의 운영을 독립적인 프라이버시 보호기구의 엄격한 감독아래 두기로 교육인적자원부와 여러 이해 관련 단체들이 합의하였다. 객관적으로 볼 때 그것은 NEIS 운영에 관련된 문제들을 대부분 해결할 수 있는 강력한 제도적 처방이었지만, 그 기구가 제대로 운영될 것이라고 믿는 이해관련 당사자들은 많지 않았다. 그렇기 때문에 일부 단체들은 서버를 물리적으로 분산시켜 학교별로 두어야 한다는 주장을 끝까지 포기하지 않았다. 결국 그와 같은 불신은 NEIS 운영을 위해 최소한 수백억 원의 추가 지출을 불가피하게 만들었다.

1997년부터 약 3년 동안이나 지속된 전자주민카드 도입 논쟁도 사회적 불신의 비용이 얼마나 큰 지를 보여주었다⁽¹⁾. 당시 내무부(현재의 행정자치부)는 국민적 논쟁을 거치면서 원래 전자주민카드에 담기로 했던 주민등록증, 운전면허증, 의료보험증, 국민연금증서, 지문, 주민등록등·초본 등 7개 정보를 대폭 축소하여 그중 주민등록자료와 인감만을 수록하기로 하였으며, 주민카드 정보의 오·남용을 방지하기 위해 민간인도 참여하는 '주민카드정보보호위원회'를 설치하기로 하였다.

그러나 그 대체 방안마저도 결국 폐기되고 말았다. 국민들은 전자주민카드가 일단 도입되고 나면 정부가 틀림없이 거기에 다른 정보들을 추가하려고 할 것이라고 예상하였으며, '주민카드정보보호위원회'가 개인정보보호를 위해 실질적인 역할을 수행할 수 있을 것으로 믿지 않았다. 2001년에 전자건강보험증 도입을 추진할 때도 정부는 제한된 정보만을 수록하겠다고 거듭

밝혔지만 국민들은 정부의 약속을 믿지 않았다.

V. 결론

이상에서 살펴본 것처럼 최근 프라이버시 보호에 있어 여러 가지 진전이 이루어졌다. 몇 가지 주목할만한 법제도가 마련되었고, 국민들의 프라이버시보호의식이 크게 제고되었다.

그러나 엄격하게 볼 때, 우리사회는 아직 프라이버시 보호에 관한 법제도적 장치를 제대로 갖추지 못하고 있고, 법제도와 기술의 운영을 뒷받침할 사회적 신뢰 수준도 크게 낮다. 또한 이 글에서 프라이버시 침해에 관한 기술적 해법에 대한 논의는 하지 않았지만, 국내에서 PETs(Privacy Enhancing Technologies)는 저개발 상태이고 정책당국은 그것의 개발을 위한 투자의 필요성조차 크게 느끼지 못하고 있는 실정이다. 2002년 7월에 발표한 "중장기 정보보호 기본계획"에는 PETs의 활용을 강화하는 내용이 포함되어 있었지만 현재까지 실천에 옮겨진 정책은 눈에 띄지 않는다.

한마디로 정보주체의 자기정보관리의 시대가 요구하는 문화, 법제도, 기술 등 어느 것도 제대로 갖추어져 있지 못하다.

때문에 아직 우리 사회는 전(前)유비쿼터스(pre-ubiquitous) 컴퓨팅 환경이 지배적인데도, 앞에서 살펴본 것처럼 프라이버시 침해가 광범위하게 발생하고 그에 대한 국민과 소비자의 우려와 반발이 NEIS의 경우처럼 사안에 따라서는 국가행정을 마비시킬 정도로 심각하게 노정되고 있다.

그런데 지금과 같이 어정쩡한 법제도 그리고 취약한 기술적 환경에서 유비쿼터스 컴퓨팅이 도입된다면 과연 어떤 일이 벌어질까? 아마도 프라이버시 침해로 인한 엄청난 사회경제적 손실, 그에 따른 국민과 소비자의 우려와 저항으로 우리사회는 심각한 혼란에 빠지고 정보화는 더 이상 진행되기 어려울 것이다.

우리가 유비쿼터스 컴퓨팅 시대를 다른 나라보다 먼저 열어가겠다면 무엇보다도 프라이버시 보호에 대한 획기적인 대책이 필요하다. 넓게는 정부, 업계, 학계, 언론 등 우리 사회의 선도적 집단들이 우리 사회의 신뢰 수준을 높이는데 노력해야 할 것이며, 좁게는 프라이버시 보호를 위한 법제도를 시급히 정비하고 PETs의 개발에도 적극 나서야 할 것이다.

그렇지 않을 경우 우리사회는 네트워크 시대를 목전에 두고도 진입하지 못하는 역사적 좌절을 경험하게 될 지도 모른다.

참고문헌

- [1] 고영삼. 전자감시사회와 프라이버시. 한울아카데미. 1998
- [2] 이근호. "유비쿼터스 컴퓨팅 환경에서의 정보보호", 제8회 정보보호심포지움. pp. 627-651. 2003
- [3] 정보통신부. 2003정보통신백서. 2003
- [4] 조동기·김성우. 인터넷의 일상화와 개인정보보호. KISDI 이슈리포트 03-11. 2003
- [5] 네이버 뉴스(news.naver.com)의 각종 신문기사
- [6] Aberdeen Group. "Identity Theft: A \$2 Trillion Criminal Industry in 2005." 2003. www.aberdeen.com/2001/research/05030013.asp
- [7] Castells, Manuel. The Rise of the Network Society. Malden, Mass.: Blackwell Publishers. 1996
- [8] Giddens, Anthony. The Consequences of Modernity. Stanford, CA.: Stanford University Press. 1990
- [9] Penders, Jacques. "Telecommunication Privacy and Ubiquitous Computing." 2002. guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/soc%20designPenders.doc
- [10] UNCTAD. E-Commerce and Development Report 2003. 2003.

〈著者紹介〉

윤영민 (Yun, Young-Min)



1983년 2월 : 서강대학교 정치외교학과 졸업

1988년 8월 : University of South Carolina, Columbia 사회학 MA

1994년 5월 : University of California, Berkeley 사회학 Ph.D

1997년 3월~현재 : 한양대학교 정보사회학전공 교수

2001년 2월~현재 : 전자정부특별위원회 및 전자정부전문위원회 위원

〈관심분야〉 사회조사방법, 정보보호, 전자정부, 정보문화