NCA I-RER-04066 / 2004. 12

150

유비쿼터스 사회의 역기능에 관한 법제도적 기초연구

A Study on the Legal & Institutional Framework with Regard to Ubiquitous Society' Dysfunction

2004. 12

수탁기관: 정보통신정책연구원

한국전산원
National Computerization Agency

제 출 문

한국전산원장 귀하

본 보고서를 “유비쿼터스 사회의 역기능에 관한 법제도적 기초연구”의 최종연구개발결과보고서로 제출합니다.

2004년 12월

수탁연구기관: 정보통신정책연구원
연 구 책 임 자: 강 홍 렬 (정보통신정책연구원 디지털미래연구실 실장)
참 여 연 구 원: 양 인 애 (정보통신정책연구원 디지털미래연구실 연구원)
김 지 수 (정보통신정책연구원 디지털미래연구실 연구원)
참 여 전 문 가: 박 훤 일 (경희대학교 법과대학 교수)
강 달 천 (한국정보보호진흥원 선임연구원)
권 건 보 (명지대학교 법학과 교수)
조 규 범 (한국정보보호진흥원 선임연구원)
길 준 규 (호남대학교 법학과 교수)
강 현 구 (전자거래진흥원 정책기획팀 팀장)
윤 훈 주 (LG 전자기술원 Mobile Multimedia연구소 주임연구원)
이 홍 주 (단국대학교 교양학부 교수)
과 제 관 리 자: 황 종 성 (한국전산원 정보화기획단장)
이 규 정 (한국전산원 정보화기획단 정책개발분석팀장)
류 영 달 (한국전산원 정보화기획단 수석연구원)

요 약 문

1. 제 목

유비쿼터스 사회의 역기능에 관한 법제도적 기초연구

2. 연구의 목적 및 필요성

본 연구과제는 건강하고 안전한 유비쿼터스 사회가 구현될 수 있도록 정보화 역기능에 대한 정책적 대안을 법제도 측면에서 거시적인 마스터플랜과 세부적인 정비방안을 도출하는데 그 목표를 두고 있다.

또한 정보화 역기능의 문제를 유비쿼터스와 연계하여, 현 IT 법제도의 미진한 사항을 보완하고, 장기적인 유비쿼터스 법제도에 관한 비전을 제시하고자 한다.

유비쿼터스와 관련된 상기의 목표는 향후 유비쿼터스의 진입에 따른 법제도측면의 장애물을 제거함과 동시에 새롭게 요구되는 제도적 시스템을 구축하는데 제도적 발판을 마련하여 줄 것이다. 또한 개별적이고 산발적으로 제안된 법제도들의 기능적 효과를 극대화하기 위하여 이들 법제도들의 상호 연동성을 검토하면서, 유비쿼터스 환경하에서의 역기능에 관한 법제도 현안을 분류하고, 이에 관한 대응방안을 체계적 도출함으로써 향후 U-Korea 비젼 수립에 정책적 기여를 할 것이다.

3. 연구개발의 내용 및 범위

위의 목적을 달성하기 위하여 우선 제1장에서는 연구의 방법론적 기초로 산학연간의 능동적인 연구 교류를 통하여, 유비쿼터스 환경하에서의 역기능에 관한 법제도 현안을 분류하였다. 본 연구는 유비쿼터스의 핵심 기술과 패러다임에 대한 선행

연구를 마친 후, 공공 부문에서 필요한 유비쿼터스의 제도화와 민간 부문에서 제기되는 유비쿼터스의 쟁점을 구별하여 연구를 진행하였다.

제2장에서는 유비쿼터스 제도화 구현의 개념을 정의하고 그에 따른 패러다임의 변화 양상을 고찰하였다. 유비쿼터스 IT의 핵심 기술 내용은 크게 4가지로 나눠볼 수 있는데 RFID로 대표되는 센서, 태그 기술과 Ad-hoc 네트워크, IPv6 등의 네트워크 커뮤니케이션 기술, 사용자 인터페이스 기술, 정보보안 기술 등이다.

제3장에서는 유비쿼터스 환경에서 본격적으로 문제시되는 공공 부문의 법적 고려사항을 4가지 이슈로 나누어 고찰하였다. 첫째, 유비쿼터스 도입을 위한 IT법률의 정비방안, 둘째, 유비쿼터스 환경에서의 개인정보보호 법제 검토, 셋째, 전자감시사회에 대한 헌법적 고찰 및 관련 사례, 넷째, RFID에 관한 외국 입법 사례 조사 및 국내법과의 조화등이다.

제4장에서는 기업이나 일반 소비자의 이용 측면에서 유비쿼터스의 확산을 고려하여 민간 부문에서의 제도화와 역기능 대비에 대한 연구를 진행하였다. 첫째, U-Commerce 확산 및 안정성에 관한 IT법률의 정비방안, 둘째, RFID 활성화를 위한 제도적 기반으로 나누어 연구를 진행하였다.

그리고 마지막으로 제5장에서는 상기의 분야별로 진행된 연구 성과를 바탕으로, 유비쿼터스 환경하에서 구현될 수 있는 미래 사회의 이슈와 법제도적 구현 방향을 제시하였다.

4. 연구 결과

가. 제1장 서론

본 연구는 U-KOREA 환경의 신뢰성을 확보하여 그 효율성과 안정성을 법적으로 체계화하여, 유비쿼터스 사회의 진입을 거시적, 미시적으로 고찰하는 데 초점을 두고 있으며, 유비쿼터스의 법적 환경에서 예상될 수 있는 문제점을 적극적으로 조망함으로써 사회 각 부문에 긍정적 파급효과를 유도할 것으로 기대한다.

산학연간의 능동적인 연구 교류를 위하여, 본 연구는 전문가 체제의 유비쿼터스 전문가 pool을 구성하여, 유비쿼터스 환경하에서의 역기능에 관한 법제도 현안을 분류하여 이에 관한 대응방안을 체계적 도출하였다.

본 연구는 유비쿼터스의 핵심 기술과 패러다임에 대한 선행 연구를 마친 후, 공공 부문에서 필요한 유비쿼터스의 제도화와 민간 부문에서 제기되는 유비쿼터스의 쟁점을 구별하여 연구를 진행하였다.

그리고 유비쿼터스 환경에서 본격적으로 문제시되는 공공 부문의 법적 고려사항을 4가지 이슈로 나누어 고찰하였다.

- 유비쿼터스 도입을 위한 IT법률의 정비방안
- 유비쿼터스 환경에서의 개인정보보호 법제 검토
- 전자감시사회에 대한 헌법적 고찰 및 관련 사례
- RFID에 관한 외국 입법 사례 조사 및 국내법과의 조화

또한 기업이나 일반 소비자의 이용 측면에서 유비쿼터스의 확산을 고려하여 민간 부문에서의 제도화와 역기능 대비에 대한 연구를 진행하였다.

- U-Commerce 확산 및 안정성에 관한 IT법률의 정비방안
- RFID 활성화를 위한 제도적 기반

나. 제2장 유비쿼터스 제도화 구현의 개념과 패러다임의 변화

유비쿼터스 IT는 사용자의 상황에 맞게 언제 어디서나 연결된 컴퓨팅(computing) 기술을 통해 원하는 정보를 얻게 되는 기술이다. 기술의 발전에 따라 컴퓨팅 기술은 기존의 단말기는 물론 일상적인 사물, 건물, 상품 등에도 내재화 되며, 이들이 서로 네트워크화 되기 때문에 사람, 사물, 공간의 네트워크화가 실현된다. 유비쿼터스 IT의 핵심 기술 내용은 크게 4가지로 나눠볼 수 있는데 RFID로 대표되는 센서, 태그 기술과 Ad-hoc 네트워크, IPv6 등의 네트워크 커뮤니케이션 기술, 사용자 인터페이스 기술, 정보보안 기술 등이다. RFID의 경우에는 소형화, 내재화가 가능하고 기존 바코드에 비해 정보에 대한 입출력 등 정보처리를 할 수 있게 됨에 따라 기업의 입장에서는 보다 효율적인 물류관리가 가능해 질 것이며 생활편의 서비스에 있어서

도 획기적인 변화를 미치게 될 것으로 예상된다. 또 이동 단말만으로 구성된 자율적이고 독립적인 네트워크 역할을 하는 Ad-hoc 네트워크 기술이나 각 컴퓨팅에 고유 주소를 할당할 수 있는 IPv6 역시 유비쿼터스 컴퓨팅 파워를 더욱 증가시켜줄 것으로 예상된다. 이러한 유비쿼터스 컴퓨팅은 모두 사용자들로 하여금 편리한 생활을 영위하게 하는데 있기 때문에 보다 사용자 중심적인 인터페이스 기술, 이를테면 정보의 비선형 시스템 방식과 같은 유연한 정보처리 시스템이 가능한 기술이 등장할 것이다. 또한 센싱과 태그, 이동 단말기의 사용 등으로 인해 사용자의 정보가 쉽게 노출될 수 있기 때문에 정보보안 기술 역시 발전할 것으로 보인다.

이렇게 유비쿼터스 환경은 우리가 깨닫지 못하지만 생활 속에서 수많은 컴퓨터와 기술들을 사용하게 되는 환경을 말하며, 컴퓨터들은 좀더 자연스러운 존재, 일상화된 존재로 다가올 것이다. 따라서 유비쿼터스 기술은 단순한 기술 도입보다는 우리 생활과 밀접하게 연관되어져서 생활과 더불어 사용되어지고, 우리의 가정문화, 사무실 문화, 청소년 문화, 자동차 문화 등 사회문화 전 영역에 걸쳐 큰 영향을 미칠 것이다. 따라서 본 보고서에서는 유비쿼터스 기술들이 사회문화와 엮어져서 발생할 수 있는 법제도적 기반을 마련하고 지속적인 IT 성장, 경제발전, 기업의 경영효율화를 위해 유비쿼터스 기술을 활용시킬 방안들을 마련하였다.

다. 제3장 공공 부문에서의 유비쿼터스 제도화 구현 및 역기능 대비

(1) 제1절 유비쿼터스 도입을 위한 IT법률의 정비방안

현행 정보통신법이 유비쿼터스 IT기술을 포괄하고 있는지에 대한 검토가 선행되어야 한다. 정보화촉진기본법은 제2조 제1호상의 “정보”개념을 처리정보(data)로만 한정하고 있어서, 유비쿼터스 IT기술이라는 제2의 정보혁명의 사회에서는 적절하지 않다. 따라서 온라인과 오프라인을 망라할 수 있는 정보(Infomation)으로 규정되어야 한다.

또한 유비쿼터스 하에서는 정보의 개념이란 단순히 처리형태가 중요한 것이 아니고, 아울러 자료나 지식이 아닌 것도 정보일 수 있다. 결론적으로 종래의 개념정의가 아닌 “기록 또는 전자적 방식에 의하여 처리된 사항”으로 포괄적으로 규정함으

로서 수동정보인 기록과 자동정보인 처리정보를 포괄하는 개념으로 규정되어야 한다. 유비쿼터스 IT기술은 기존의 정촉법상의 “정보화 촉진”이라기 기반시설적인 측면의 소극적인 측면이 아닌 능동적으로 실시간으로 정보활용이 가능한 환경을 제공해주는 시스템이므로, 종래의 정보화촉진법으로서는 포괄하기 어려우므로 이에 대한 개념 정립과 제도적인 규율 범위에 대한 근거가 마련되어야 한다.

(2) 제2절 유비쿼터스 환경에서의 개인정보보호 법제 검토

기존의 정보통신환경을 중심으로 한 현행 개인정보보호법제는 정보통신기술의 비약적인 발전을 포괄하기에는 역부족이다. 즉 유비쿼터스 컴퓨팅의 발전으로 인한 새로운 정보통신기기 및 매체의 정보유통에 의한 개인정보 침해 유형을 규제하기에는 현행 법제로는 그 규제의 사각지대가 존재할 수 밖에 없다.

현행의 법제상의 개인정보의 범위에 새로운 유형의 개인정보를 추가하여야 할 것인가의 의문이 있을 수 있다. 시대가 변하고 정보기술이 발전하여도 “개인을 식별할 수 있는 일체의 정보”라는 개인정보의 기본적인 개념은 변하는 것이 아니다. 정보통신기술의 발전에 따라 생성되는 위치정보, 생체정보, RFID에 포함된 개인정보, 텔레메틱스 서비스를 위한 개인정보 등은 어떠한 정보통신 매체를 통해 유통되는 개인정보라도 역시 개인정보임에 변함이 없기 때문이다. 결국, 문제는 개인정보의 보호 범위가 아니라 다양한 네트워크를 통해 유통되는 개인정보를 어떻게 보호할 것인지의 여부이다. 즉, 급변하는 정보유통 환경으로 인한 현행 법제도의 개인정보보호 일반원칙(수집제한의 원칙 등) 적용의 곤란함을 어떻게 해결할 것인지의 여부가 관건이 된다.

지금의 시점에서는 현존의 법제도를 개선・보완함으로써 유비쿼터스 환경에서의 개인정보 보호가 충분히 이루어질 수 있도록 하는 방안을 고려하는 것이 차선책이 될 수 있을 것이다. 즉, 중장기적으로는 유비쿼터스 환경을 모두 포괄할 수 있는 보편적 입법모델을 모색해 가면서, 단기적으로 필요한 분야에서부터 가이드라인・지침・기준 등을 수립하는 방안을 고려할 수 있다.

(3) 제3절 전자감시사회에 대한 헌법적 고찰 및 관련 사례

과거와 달리 오늘날 국가는 첨단 정보통신기술을 이용하여 과거보다 훨씬 용이하고 교묘한 방식으로 국민에 대한 관리와 통제를 실시하고 있다. 특히 유비쿼터스 시대에서 개인은 어느 곳에 머물든 고성능 CCTV, GPS, 무선전화위치 감응기, 스마트차량 등과 같은 첨단장치를 통해 자신의 모든 행적이 기록되고 분석됨으로써 완벽한 감시의 대상이 될 있다. 따라서 전자감시사회에 있어서 개인의 일상에 대한 무차별적 감시는 막강한 정보권력의 남용에 따른 개인의 비인격화 내지 소외화를 초래하게 되는바, 이에 대처해야 하는 국가의 과제는 대체로 기본권보장이라는 헌법적 요청에 토대를 두고서 다각도로 검토되어야 할 것이다.

그럼에도 몇몇 외국의 경우와 달리 우리나라에서는 현재 전자적 감시를 직접 규율하는 법률이 제정되어 있지 않다. 향후 전자감시방비의 설치・운영에 관한 법제의 정비과정에서는 무엇보다도 인권보호의 요청과 그 효율적 활용의 측면을 적절하게 조화시킬 수 있는 방안을 모색하는 것이 중요하다. 그 구체적인 내용은 기본권 제한의 일반원칙과 개인정보보호에 관한 특수원칙 등에서 찾을 수 있으며, 개별분야에 있어서는 해당 기술의 특수성과 그에 대한 수요 등을 충분히 고려하여 그 법적 규율의 형태나 정도가 결정되어야 할 것이다.

먼저, CCTV의 설치・운영과 관련하여 주체, 설치장소, 장비의 종류, 그 운영방법과 절차, 본인에 의한 통제방법, 감독기관의 감독 등을 포괄적으로 규정하는 특별법을 제정할 필요가 있다.

다음으로, 카메라폰의 사용과 관련하여서는 카메라폰에서 특별히 문제가 되고 있는 것은 통화기능이 아니라 촬영기능에 있다는 점을 고려하여 통화기능까지 전면 차단하기보다는 촬영기능만 규제하는 방식을 취하는 것이 바람직할 것이다. 그리고 무단촬영에 대한 행위규제라는 법적 방안과 더불어 일정한 지역에서의 촬영기능을 중단하거나 촬영사실을 표시하도록 하는 기술적 방안도 고려될 수 있다.

마지막으로, 위치추적시스템의 활용과 관련하여 실효성의 측면에서 법적 규제의 수단을 강구하지 않을 수 없다. 이 문제에 대처하기 위한 우리의 법제정비에 있어서는 위치확인정보의 수집과 이용은 원칙적으로 사전설명에 기초한 당사자의 동의

를 얻도록 하고, 그 처리는 부가서비스 제공에 필요한 한도와 기간 내에서 그리고 익명화에 의해서 이루어지도록 하여야 할 것이다. 또한 위치기반서비스에 의한 불필요한 상호접속은 법으로 금지하거나 제한하고, 위치확인정보를 불필요하게 수집하는 것은 법적으로 제한하여야 한다. 그리고 위치기반시스템에 내재된 취약성은 수정되거나 제거될 수 있도록 조직적·절차적적 조치가 강구되어야 한다. 나아가 수집한 위치확인정보를 심각하게 남용할 경우 형사처벌을 할 수 있도록 하여야 할 것이다.

(4) 제4절 RFID에 관한 외국 입법 사례 조사 및 국내법과의 조화

RFID는 그 특성상 반도체 칩에 기록된 정보를 제3자가 손쉽고 은밀하게 판독할 수 있고, 장기적으로 태그 정보와 연동된 데이터베이스를 축적·이용할 수 있다는 점에서 개인정보의 침해 가능성이 제기되고 있다. 특히 RFID 태그를 탑재 또는 부착하여 언제 어디서나 RFID 태그에서 전송되는 정보를 이용할 수 있고, 실시간으로 물건, 사람 혹은 동물의 움직임을 파악하여 상황정보를 분석할 수 있다는 점에서 그 침해 가능성은 가히 놀랄만한 것이라 할 것이다. 또한 RFID의 무절제한 사용으로 고객정보가 무작위로 유출된다면 이 역시 개인정보 보호에 대한 큰 위협이 될 것이다.

정보주체의 개인정보자기결정권이 자의적으로 침해되지 않기 위해서는 정보주체에게 통상 익명권, 정보처리금지청구권, 열람 및 갱신청구권, 정보분리청구권이 보장되어야 한다. 이러한 권리의 행사는 네트워크이용관계에 있어 경제적으로나 지적인 면에서 약자인 정보주체에 대해 충분한 설명 내지 위험에 대한 설득을 전제하여야 하며(소위 Informed Consent), 이를 전제하지 아니한 정보제공 동의나 이용관계의 설정은 정보주체의 정보자기결정권에 대한 침해로 새겨야 할 것이다. RFID 시스템에 대해서도 이러한 익명권, 정보처리금지청구권(수집제한의 원칙, 목적구속의 원칙, 시스템공개의 원칙), 정보열람권과 정보갱신청구권, 정보분리청구권은 동일하게 적용될 것이다.

라. 제4장 민간 부문에서의 유비쿼터스 제도화 구현 및 역기능 대비

(1) 제1절 U-Commerce 확산 및 안정성에 관한 IT법률의 정비방안

이와 같이 유비쿼터스 환경에서 나타날 수 있는 역기능에 대한 법제도적 기반이 필요한 반면, 유비쿼터스 IT를 활성화 시킬 수 있는 기반 역시 중요하다. 유비쿼터스 IT가 우선적으로 도입되서 활용될 수 있는 분야는 바로 기업 비즈니스 분야이다. 인터넷 기반의 전자상거래(e-business)를 넘어서서 사용자들이 이동 단말기를 통해 언제 어디서든 원하는 상품정보를 얻고, 구매할 수 있는u-Commerce 분야가 바로 그것이다. 이러한 u-Commerce가 활성화 되기 위해서는 사업자나 중개업자, 소비자 모두가 안심하고 거래할 수 있는 법적 환경을 조성하는 것이 중요한데 본 보고서에서는 u-Commerce에서 상품이나 소비자 정보 등 정보유통을 담당하는 중개자책임법제, 글로벌한 상거래 환경에서의 국제재판관할 및 준거법 마련 등 민사법령의 정비를 제안하였다. 또한 양질의 정보들이 유통되기 위해 지적재산보호에 관한 법령을 정비하는 것 또한 필요한데 이를 위해서는 상품정보, 식별정보의 저작권 보호, 콘텐츠와 같은 소프트웨어 상품을 개발, 이용할 수 있는 법적 보호 근거를 마련하여 물질적 상거래뿐만 아니라 지식기반 사회에 대비하여 콘텐츠 거래에 있어서도 법적 보호 토대 마련이 시급함을 지적하였다.

(2) 제2절 RFID 활성화를 위한 제도적 기반

유비쿼터스 기술에 있어서 복잡한 정보를 취급하고 이력정보를 관리할 수 있는 RFID의 경우에도 활용분야가 무궁무진하다고 할 수 있다. 본 보고서에서는 금융기관에서 기업의 담보를 관리하기 위해 RFID를 활용하는 방안과 이를 효율적으로 처리하기 위한 법제도 정비방안을 제시하였다. RFID를 이용하여 기업의 담보물을 관리하기 위해서는 위・변조가 불가능한 RFID의 개발 및 여러 재료들에 부착 가능한 소재의 개발, 판독상의 인식률 제고, 위・변조 및 오류 방지, 해킹 방지 등 다양한 기술적 보완이 필요하다. 아울러 표준화, 주파수대역 할당 관리 등에 있어서도 정부의 주도적인 관리 노력이 요망된다. 또한 RFID를 활용한 기업동산의 담보관리를 위해서는 전자적 장치를 이용한 공시방법을 법률상으로 인정하고, RFID를 통한 담보

권 설정자 및 담보권자의 권리와 의무를 규정할 필요가 있다. 무엇보다 RFID가 부착된 담보물건에 대해서는 리더기와 인터넷을 통해 법원의 법인등기부 시스템에 접속하여 담보권의 존재와 담보물건의 일치 여부를 확인하고, 담보권의 취득・실행・소멸을 가능하게 하는 절차법상의 제도가 마련되어야 한다. 이렇게 RFID를 통해 담보관리를 하게 될 경우 대기업은 물론 중소기업들도 고가의 동산을 담보로 활용할 수 있게 되어 기업의 자금조달이 크게 늘어나고 담보활용의 사각지대가 해소됨으로써 기업의 경제적 활동이 획기적으로 확대되고, 설비투자가 확대되는 효과가 기대된다. 또한 RFID를 통한 담보관리의 안전 및 신뢰성 제고를 위한 관련 산업이 발전하여 정보보안 및 서비스 개발, 담보물 DB 관리 대행업체 등 관련된 전문업체의 고용도 촉진될 것으로 예상된다.

마. 제5장 결론: 정책적 제언

본 보고서는 “유비쿼터스(ubiquitous)"라는 세계적인 IT 기술 방향의 흐름에 맞춰 유비쿼터스 환경의 핵심개념과 핵심 기술을 파악하여 미래 한국사회를 보다 풍요롭고, 안전하게 만들기 위한 법제도적 기반을 마련하는 것이 목적이다. 물론 법제도라는 것이 현 상황에 맞춰 적절한 대안을 찾고, 마련하는 것이 되어야 하겠으나 급속도로 IT의 기술혁신이 진행되는 현시점에서는 다가오는 미래상에 대한 정확한 개념파악을 통해 IT기반의 미래사회를 활성화시키고, 발생가능한 역기능을 최소화할 수 있는 법제도적 기반을 제시하는 것이 적절한 것으로 판단된다. 따라서 본 본고서에서는 우선적으로 유비쿼터스 개념을 파악하고, 유비쿼터스 IT로 구현된 사회환경의 모습을 그려보고 유비쿼터스 IT가 어떠한 핵심 기술들로 이루어지는지를 살펴보았다. 이를 통해 다음과 같은 5가지의 미래사회의 이슈와 법제도적 구현방향을 제시할 수 있다. 첫 번째는 미래사회 이슈는 디지털 디바이드와 사회적 불평등의 확산 가능성이다. 두 번째 이슈는 시스템 리스크(system risk)의 발생 가능성이다. 세 번째 유비쿼터스 IT로 인한 미래사회 이슈는 센싱이나 태그 확대로 인한 개인정보보호 및 프라이버시(privacy) 문제이다. 네 번째 유비쿼터스 사회 이슈는 컴퓨팅(computing)이 서로 네트워크화 되어 컴퓨팅 파워의 폭발 시대가 올 것이라는 것이다. 다섯

번째는 유비쿼터스 IT로 인해 자본이나 기계 등의 생산과정이 전개됨에 따라 노동의 사회적, 제도적 역할 변화가 불가피 할 것이라는 점이다.

5. 활용에 대한 건의

초고속정보통신기반이 구축됨으로 인해서 제개정된 IT법률을 유비쿼터스 시스템과 연계하여 포괄적, 세부적으로 검토할 수 있으며, 이는 향후 관련 법률의 입법적 요청 및 외국의 선진 사례가 될 수 있다.

또한 유비쿼터스의 역기능에 대한 법제도 현안을 전체적으로 고찰할 수 있는 연구협력 체제를 구축함으로써, 정보통신 분야와 연계된 기업, 관련 기관, 이용자에게 단기적인 개선 방안을 제공하고 더불어 장기적인 유비쿼터스의 비전을 제시할 수 있다.

6. 기대 효과

본 연구는 U-KOREA 환경의 신뢰성을 확보하여 그 효율성과 안정성을 법적으로 체계화하여, 유비쿼터스 사회의 진입을 거시적, 미시적으로 고찰할 수 있는 역할을 할 것으로 기대한다. 또한 공공부문의 책무와 역할을 선결조건으로 하는 정보사회의 순기능 조장 및 역기능 해소에 대한 구체적 방안을 법제도적으로 정비할 것으로 기대한다.

Summary

1. Title

A Study on the Legal & Institutional Framework with Regard to Ubiquitous Society' Dysfunction

2. Purpose and Significance of the Study

The purpose of this research report is to investigate into the legal foundation of the ubiquitous society and possible effects that ubiquitous IT has on the society. For the effective study, a research team has conducted a project of school-work links about what dysfunctions arise from the ubiquitous society and how they can be solved. Before discussing the ubiquitous society in depth, this report first looks into core technology and paradigm of ubiquitous IT.

3. Contents and Scope of the Study

The First Chapter emphasizes the legal foundation of the ubiquitous society and possible effects that ubiquitous IT has on the society. The Second Chapter analyzes the critical technology of u-IT which is divided into four categories; sensor/tag (RFID), network communication technology such as Ad-hoc network and IPv6, user interface technology and information security technology. The Third Chapter analyzes the legal frame and public policy for privacy with respect to public sector. The Fourth Chapter analyzes the use of ubiquitous technology in private area such as business and corporate sector

and legal policy useful U-commerce. Finally, the Fifth Chapter lay the legal and institutional foundation with the advent of the ubiquitous society.

4. Results of the Study

(1) Chapter I Introduction

The purpose of this research report is to investigate into the legal foundation of the ubiquitous society and possible effects that ubiquitous IT has on the society. For the effective study, a research team has conducted a project of school-work links about what dysfunctions arise from the ubiquitous society and how they can be solved. Before discussing the ubiquitous society in depth, this report first looks into core technology and paradigm of ubiquitous IT.

(2) Chapter 2 critical technology of u-IT and paradigm

Ubiquitous Information Technology(u-IT) means literally IT everywhere so that users are allowed to access context-aware information anywhere and whenever. Thanks to technology development, computing could be embedded in pre-existing equipments, some kind of items, buildings and products and these are networked with one another enabling the network of people, things and space. The critical technology of u-IT is divided into four categories; sensor/tag (RFID), network communication technology such as Ad-hoc network and IPv6, user interface technology and information security technology. Of these, RFID that can be miniaturized and embedded in some items and products, will serve as a more effective and convenient commercial vehicle operation system compared to the existing Bar-code technology. In addition, network communication system only run by mobile equipments will play a role in giving more empowerment to ubiquitous computing. Since this ubiquitous computing is designed to make users' lives more convenient,

user-centered interface such as non-liner information processing system is inevitably needed. And information security technology is also required because sensing, tag and mobile device raise concerns over security and privacy of users' information.

(3) Chapter 3 legal frame and public policy in public sector

In a ubiquitous environment, people unconsciously use numerous computers and technologies in their lives and computers will become more ordinary than ever. Accordingly ubiquitous technology will have an important effect upon the way we live, work and even drive. This report aims to lay a legal and institutional foundation of the ubiquitous society and to make proposals to utilizes ubiquitous technology in order for continuous IT development and effective business management.

With regard to utilization of ubiquitous IT, the concept of ‘information’ in the ubiquitous society should be properly defined. We argue that Telecommunication law should reflect ubiquitous IT as the concept of active system rather than that of passive system. To than end, we need to formulate a clear definition of ubiquitous IT and regulation boundary. In addition, vital information processed by RFID or telematics becomes more important but at the same time more diffusive than ever so we should now focus on how to protect personal information. In the short run, the existing privacy law could be revised or complemented; however, in the long run, we should pursue a universal ubiquitous law model and consider setting up guidelines and norms for the ubiquitous society.

In particular, ubiquitous IT could put people under constant supervision with high-powered CCTV(closed-circuit television), GPS(Global Positioning System) and RFID(Radio Frequency Identification System) that can lead to information power abuse so that we should take into consideration diverse aspects of the existing privacy law. Above all, we need to foster the ubiquitous society that guarantee and do not interrupt deliberately information subjectivity such as the right of anonymity, anti-information processing and

claims of renew information.

(4) Chapter 4 use of ubiquitous technology in private area and legal policy

Corporate business is one of the areas where ubiquitous IT can be best utilized. First of all, compared to Internet-based e-business, u-Commerce enables people to get product information and to buy them using their mobile devices. For activation of u-Commerce environment, it is important to lay a legal foundation which is an essential part for safe bargaining among businessmen, agents and consumers. Therefore, this report proposes to put the civil law in place such as agent responsibility law which is in charge of product and consumer's information. In addition, the intellectual property law is prerequisite for better quality information so this report proposes to build a legal foundation for the software industry, for instance, product information, copyright of identification information and contents which will become all the more important in the ubiquitous society.

The application of RFID that can mange diverse information and product history is quite extensive in the ubiquitous society so this report suggests using RFID for management of business mortgage and establishing appropriate legal institutions to handle related issues. For RFID-based mortgage management, RFID needs to include such features as counterfeit prevention, easiness to be attached to diverse materials, easy readout and anti-error etc. The government should play its part in standardization of RFID system and frequency assignment. Moreover, electronic posting system should be legally allowed and the responsibility and right of mortgagor and mortgagee should be stipulated. And RFID-attached collateral should be able to be read and confirmed via the Internet or reader devices in the court registration system; and institutional foundation for dealing with its procedures should be set up to make it possible to exercise security right and to bargain, acquire or cease mortgage. The utilization of RFID to manage business mortgage will contribute to transparent corporate fundraising, active optimization of it and amplification of facility investment due to high-priced chattel real. Related industries

involved in safety and reliability of mortgage management will be developed and job creation in such areas as information security, service development and data base management agency is also expected.

(5) Chapter 5 legal and institutional foundation in ubiquitous society

This report will be used to lay the legal and institutional foundation with the advent of the ubiquitous society.

5. Practical Usages of the Study

The results of the study are expected to be useful reference materials for analyzing and developing legal foundation of the ubiquitous society and possible effects that ubiquitous IT has on the society. They also will be useful for protection of privacy in ubiquitous society.

6. Expected Benefits

This research is beneficial to foster the ubiquitous society that guarantee and do not interrupt deliberately information subjectivity such as the right of anonymity, anti-information processing and claims of renew information. Also, they are so valuable to use guide line in both public sector and private sector in utilizing ubiquitous technology.

Contents

목 차

표 목 차

그 림 목 차

제 1 장 서 론

유비쿼터스 기술은 정보통신시스템에 새로운 패러다임을 제기하고 있으며, 그로 인하여 사회 각 분야에 획기적인 영향을 미치고 있다. 새로운 패러다임의 등장으로 인하여 기업의 입장에서는 기술적 이슈들이 주요 관심이 되며, 일반인들에게는 이러한 기술의 보급으로 인하여 생활 속에서 어떠한 변화가 있을 것인지가 관심이 되고 있다.

유비쿼터스로 인하여 지능형사회로 접어들면서 생활의 편리성을 보장받는 장점이 있으나, 한편 이로 인해 노출되는 각종 개인정보의 노출 피해에 따른 부작용도 각종 연구를 통하여 예측되고 있다. 역기능의 사례들은 현재보다 다양하고 복잡한 형태로 나타날 것이고, 미연에 이를 방지하기 위한 제도적 보호 장치가 절실히 요구되고 있으므로 단순히 세부적인 역기능 사례를 방지하는 차원이 아닌, 유비쿼터스 제도 전반에 대한 능동적 검토가 선행되어야 할 것이다.이는 동시에 유비쿼터스 기술을 보급하고 확산시킬 수 있는 제도적 여건도 고려해야 할 것이다. 즉, 개인의 권리 보호를 전제로 하여 새로운 신기술의 대국민서비스를 극대화할 수 있는 정책적 방안이 마련되어야 한다.

본 연구는 u-Korea 환경의 신뢰성을 확보하여 그 효율성과 안정성을 법적으로 체계화하여, 유비쿼터스 사회의 진입을 거시적, 미시적으로 고찰하는 데 초점을 두고 있으며, 유비쿼터스의 법적 환경에서 예상될 수 있는 문제점을 적극적으로 조망함으로써 사회 각 부문에 긍정적 파급효과를 유도할 것으로 기대한다.

산학연간의 능동적인 연구 교류를 위하여, 본 연구는 전문가 체제의 유비쿼터스 pool을 구성하여, 유비쿼터스 환경하에서의 역기능에 관한 법제도 현안을 분류하여 이에 관한 대응방안을 체계적 도출하였다. 전문가 인력 중심의 체제는 그간 연구 중심의 과제를 실무적 차원에서 고찰하는 통로가 되므로, 유비쿼터스의 제도화 및 역기능의 핵심 쟁점을 실무적으로 파악하여 궁극적으로 IT 미래를 예측하고 준비할 수 있는 연구 수행 방법의 일환으로 활용되었다.

본 연구는 유비쿼터스의 핵심 기술과 패러다임에 대한 선행 연구를 마친 후, 공공 부문에서 필요한 유비쿼터스의 제도화와 민간 부문에서 제기되는 유비쿼터스의 쟁점을 구별하여 연구를 진행하였다. 유비쿼터스의 기술의 제도화하여 고찰하기 위해서 제2장은 유비쿼터스 기술의 핵심 개념과 패러다임을 분석하였다.

유비쿼터스 시스템은 정보기기가 사용자의 행동에 따라 필요한 솔루션을 제공한다는 개념으로 이해될 수 있다. 이와 같이 유비쿼터스는 IT 전반의 모든 기술 내용을 포함하고 있기 때문에 각 기술들이 가지는 특징과 사용될 수 있는 서비스 분야를 파악하여 이들이 사회 전반에 어떠한 영향을 미칠 것인가를 살펴보는 것이 바람직하다. 이에 본 연구에서는 유비쿼터스 시스템을 구성하는 분야를 분석하여 각 분야에서의 기술적 속성 및 특성을 파악하고자 한다. 이에 유비쿼터스 시스템을 구성하는 분야를 센서/태그 기술, 네트워크 커뮤니케이션 기술, 사용자 인터페이스 기술, 정보보안 기술 등 크게 4가지 분야로 분류하여 연구를 진행하였다. 그리고 유비쿼터스 환경에서 본격적으로 문제시되는 공공 부문의 법적 고려사항을 다음과 같이 4가지 이슈로 나누어 고찰하였다.

- 유비쿼터스 도입을 위한 IT법률의 정비방안
- 유비쿼터스 환경에서의 개인정보보호 법제 검토
- 전자감시사회에 대한 헌법적 고찰 및 관련 사례
- RFID에 관한 외국 입법 사례 조사 및 국내법과의 조화

기존의 정보통신환경을 중심으로 한 현행 개인정보보호법제는 정보통신기술의 비약적인 발전을 포괄하기에는 역부족이다. 즉 유비쿼터스 컴퓨팅의 발전으로 인한 새로운 정보통신기기 및 매체의 정보유통에 의한 개인정보 침해 유형을 규제하기에는 현행 법제로는 그 규제의 사각지대가 존재할 수 밖에 없다. 이는 즉, 급변하는 정보유통 환경으로 인한 현행 법제도의 개인정보보호 일반원칙(수집제한의 원칙 등) 적용의 곤란함을 어떻게 해결할 것인지의 여부가 관건이 된다.

지금의 시점에서는 현존의 법제도를 개선・보완함으로써 유비쿼터스 환경에서의 개인정보 보호가 충분히 이루어질 수 있도록 하는 방안을 고려하는 것이 차선책이 될 수 있을 것이다. 즉, 중장기적으로는 유비쿼터스 환경을 모두 포괄할 수 있는 보

편적 입법모델을 모색해 가면서, 단기적으로 필요한 분야에서부터 가이드라인・지침・기준 등을 수립하는 방안을 고려할 수 있다. 또한 기업이나 일반 소비자의 이용 측면에서 유비쿼터스의 확산을 고려하여 민간 부문에서의 제도화와 역기능 대비에 대한 연구를 진행하였다.

- U-Commerce 확산 및 안정성에 관한 IT법률의 정비방안
- RFID 활성화를 위한 제도적 기반

유비쿼터스 컴퓨팅과 네트워크를 기반으로 등장할 수 있는 비즈니스 사업은 인터넷을 이용한 e-commerce를 발전시킨 u-commerce이다. u-commerce는 유비쿼터스 컴퓨팅과 네트워크를 기반으로 하여 일상생활 속에서 고객의 소비활동을 촉진시키고, 고객이 구매하려는 상품이나 기업의 생산, 마케팅, 물류 판매나 고객관리 등의 비즈니스 프로세스를 도와준다. 즉, 모든 상품과 소비자, 기업이 항상 연결되어 있으며(always connected), 또한 항상 연결되어 있다는 것을 인식하고 있으며(always aware), 모든 상품이나 프로세스가 지능화 되어(always smart), 생산성과 소비를 촉진시키는 방향(always active)으로 가는 것이다.

이를 위해서는 유비쿼터스 환경에서 경제활동을 하는 각 주체가 현실공간과 똑같이 안심하고 거래를 할 수 있는 법적 환경을 정비할 필요가 있다. 우선 유비쿼터스 환경에서의 거래와 같은 경제 활동을 안심하고 수행하는데 있어서 기본이 되는 민사법령이 필요하며, 그런 다음에 사업자가 갖는 불안에 대응하여 지적재산보호 법령을, 소비자의 불안에 대응하여 소비자의 신뢰를 확보할 수 있는 법령을 각각 정비할 필요가 있다. 마지막으로 유비쿼터스 환경에서의 활동을 안전하게 수행 할 수 있는 보안의 확보도 필요 불가결하다.

마지막으로 본 연구에서는 RFID가 활용분야 중에서 아직 본격적으로 활용되고 있지는 않으나 발전 가능성이 큰 금융기관의 담보관리에 RFID를 활용하는 방안을 살펴보고자 한다. 종래 기계・기구, 재고자산 등 기업동산은 그 가액에도 불구하고 담보 제공하는 방법이 제한되어 있어 금융기관으로부터 자금을 차입할 때 제대로 이용되지 못하였다. 이하에서는 금융기관의 RFID 이용 사례를 알아보고 해결해야 할 과제와 활용방안, 법제화 방안 등에 대하여 검토해보기로 한다.

제 2 장 유비쿼터스 제도화 구현의 개념과 패러다임의 변화

제 1 절 유비쿼터스 환경의 핵심 개념

유비쿼터스(ubiquitous)란 단어의 어원을 라틴어에서 찾아보면 “언제, 어디서나, 도처에 존재한다”라는 뜻을 가지고 있다. 일반적으로 도처에 편재(偏在)해 있는 물과 공기와 같이 자연물을 말할 때 사용되고, 종교적으로는 언제, 어디서나 시간과 공간을 초월하여 존재한다는 무소부재(無所不在)를 의미할 때 사용되는 말이다(최남희, 2002; 권수갑, 2003; 김재윤, 2003). 유비쿼터스란 용어를 컴퓨터 분야에서 처음 사용한 사람은 미국 제록스(Xerox)사 PARC(Palo Alto Research Center)의 마크 와이저(Mark Weiser) 박사로서[1], 마크 와이저와 그의 동료들은 “우리가 사용하는 컴퓨터가 왜 이리 사용하기도 힘들고 어려운가”라는 의문에서 출발하여 유비쿼터스 컴퓨팅의 개념을 정립하기 시작했다.

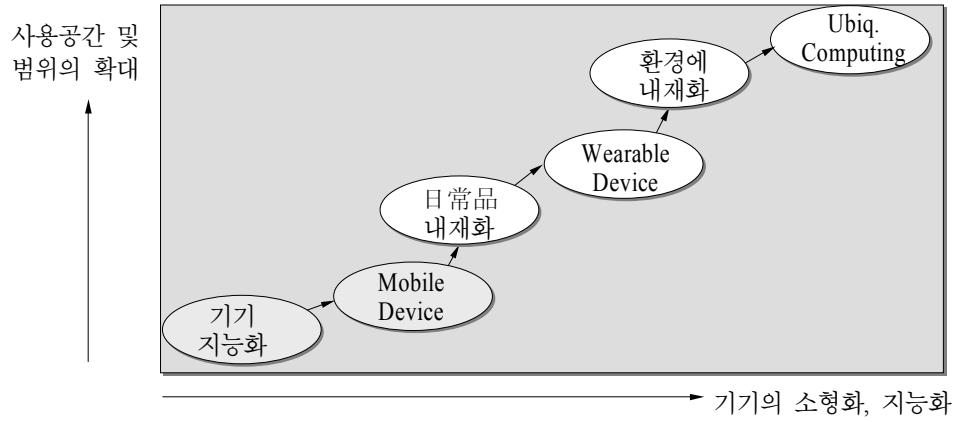
논문에서 우리의 눈엔 보이지 않지만 분산되어 있는 수많은 컴퓨터들이 서로 연결되어 사람이 컴퓨터들을 의식하지 않고도 자연스럽게 컴퓨팅 기술을 이용할 수 있는 환경이 도래한다고 주장하면서 이러한 환경을 ‘ubiquitous computing’ 혹은 ‘calm technology’로 부르면서 컴퓨팅의 ‘제3의 물결’이라고 보았다.[2] 유비쿼터스는 기기의 소형화, 지능화와 사용공간의 범위가 확대되는 과정을 거쳐서 발전된다.

---

1) 그는 유비쿼터스 컴퓨팅의 원전이라고 불리는 「21세기를 위한 컴퓨터(The Computer for the 21st Century)」라는 논문을 미국의 대표적 과학저널의 하나인 ‘Scientific American’ 1991년 9월호에 게재했다.

2) Apple사의 Alan Kay는 이것을 ‘제3의 컴퓨팅 패러다임’이라고 부르고 있다.

〔그림 2－1〕 유비쿼터스 컴퓨팅의 진화

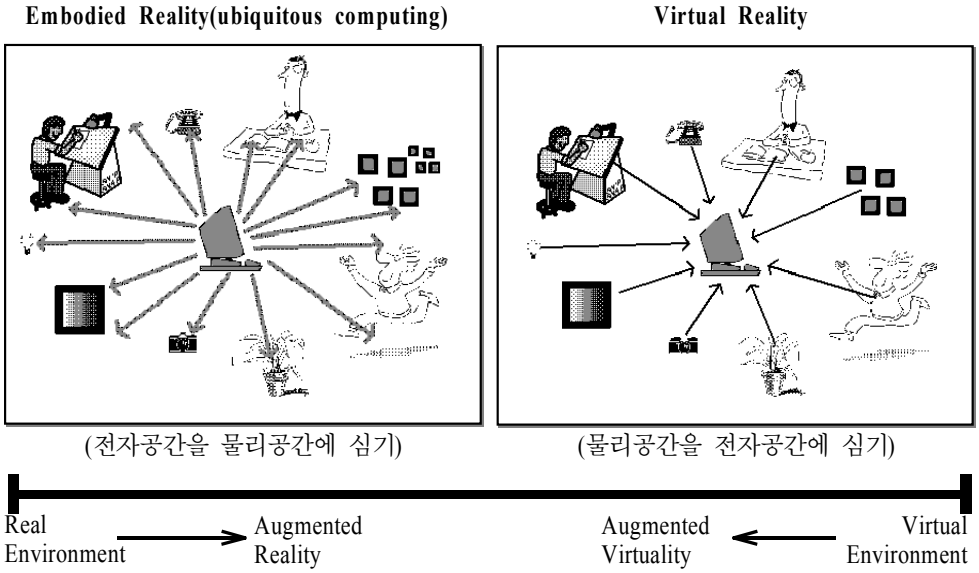


자료: 김재윤, 2003. “유비쿼터스 컴퓨팅 : 비즈니스 모델과 전망”, 삼성경제연구소. 2003. 12. 6.

마크 와이저는 많은 사람이 한 대의 대형 컴퓨터를 공유하던 메인 프레임 시대에서, 1980년대부터 시작된 퍼스널 컴퓨터 시대와 광역 분산 컴퓨팅을 제공하는 인터넷 시대를 거쳐 개개인이 주변에 편재되어 있는 여러 컴퓨터를 사용하는 유비쿼터스 컴퓨팅 시대가 도래하고 있으며, 2005년에서 2020년 사이에 일반화 될 것이라고 예측하고 있다. 마크 와이저가 지적하고 있는 유비쿼터스 컴퓨팅의 가장 기본적인 개념은 컴퓨터 파워의 내재화(embodied)이다. 분산되어 있거나 가상 공간 중심이던 컴퓨팅 환경을 실재 생활에 내재화 시켜서 보다 실재화되고 생활과 밀착된 컴퓨팅 환경을 구현하는 것이다.

이러한 유비쿼터스 컴퓨팅의 기본개념이 오늘날에 와서는 차세대 IT 혁명의 핵심 동인으로서 사회, 경제적으로 커다란 변화를 가져올 것으로 예견되고 있다. 따라서, 그 개념도 ‘유비쿼터스 컴퓨팅 및 네트워킹 기술’을 활용하여 보이지 않는 마이크로 컴퓨터를 주택, 시설, 상품, 기계 등등의 모든 장소와 사물에 심어 모든 사람, 사물, 컴퓨터가 언제, 어디서나, 유선/무선 초고속정보통신망을 통해 연결되도록 함으로써, 국가를 구성하는 모든 국민, 기업, 정부의 기능과 역할을 지능화시켜 국가 경쟁력을 향상시키고, 나아가서는 국민의 삶의 질을 혁신적으로 개선시킬 수 있는 비전을 담는 새로운 국가, 기업의 경영 정책과 전략으로까지 확대되고 있는 것이다.

〔그림 4－2〕 마크 와이저의 유비쿼터스 컴퓨팅 이미지



자료: 최남희, 2002, “유비퀴터스 혁명이란 무엇인가?”, 2002년 8월 u-Korea 포럼 준비반 워크샵 발표자료

하지만 유비쿼터스라는 단어를 국가전략과 경영 정책 전략으로 확대되기 위해서는 보다 전략적 의미 선택이 요구된다. 최근 유비쿼터스가 일상적인 용어로 사용되기 시작하면서 기업과 국가 단위에서도 “유비쿼터스” 단어를 사업과 정책의 영역으로 끌어들이고 있지만 실상 유비쿼터스가 IT의 전영역을 망라하고 있어 특정의미를 지니기 어렵기 때문에 보다 전략적인 의미사용이 제안되기도 하였다(강홍렬, 2004).

따라서 현재 경영전략이나 국가전략으로 상정되어 있는 유비쿼터스의 의미에 대해 살펴보면, 유비쿼터스란 기술이 생활 속에 스며들어 사용자는 그 기술의 존재를 깨닫지 못하는 상황을 의미하며, 또한 언제 어디서나 네트워크에 접속되어 정보 서비스를 제공받을 수 있는 것을 말한다. 즉, 유비쿼터스는 우리가 깨닫지는 못하지만 생활 속에서 수많은 컴퓨터와 기술을 사용하게 되는 환경인 것이다. 그만큼 컴퓨터는 우리에게 자연스러운 존재이어야 하며, 주변 사물 및 생활과 자연스럽게 어울러져야 한다. 때문에 유비쿼터스 기술은 단순한 기술 도입에서 그치는 것이 아니라 우리의 생활과 밀접하게 관련되어져 사용되는 생활과 ‘함께’ 사용되어지는 기술이며, 생활은 물론 사회, 문화 전반에 걸쳐 널리 영향을 미칠 것이다.

제 2 절 유비쿼터스 IT의 핵심 기술 내용

유비쿼터스 시스템은 다양한 종류의 컴퓨터가 사람, 사물, 환경 속에 내재되어 있어 이들이 서로 연결되어, 필요한 곳에서 컴퓨팅을 구현할 수 있는 환경을 지칭한다. 따라서 유비쿼터스 시스템이 지향하는 궁극적인 모습은 컴퓨팅의 유틸리티화(computing utility)이다. 따라서 유비쿼터스 환경에서는 네트워크에 접속되는 기기의 증대로 인해 다양한 새로운 기술 발전이 이루어지게 되며, 상태 감지, 위치추적 능력의 확대가 일어나게 된다. 이를 통해 커뮤니티(community)의 파워가 증대하게 되어 형태지의 교환 및 공유가 가능해진다(강홍렬, 2004). 궁극적으로 유비쿼터스 시스템은 정보기기가 사용자의 행동에 따라 필요한 솔루션을 제공한다는 개념으로 이해될 수 있다. 이와 같이 유비쿼터스는 IT 전반의 모든 기술 내용을 포함하고 있기 때문에 각 기술들이 가지는 특징과 사용될 수 있는 서비스 분야를 파악하여 이들이 사회 전반에 어떠한 영향을 미칠 것인가를 살펴보는 것이 바람직하다. 이에 본 연구에서는 유비쿼터스 시스템을 구성하는 분야를 분석하여 각 분야에서의 기술적 속성 및 특성을 파악하고자 한다. 이에 유비쿼터스 시스템을 구성하는 분야를 센서/태그 기술, 네트워크 커뮤니케이션 기술, 사용자 인터페이스 기술, 정보보안 기술 등 크게 4가지 분야로 분류될 수 있다.

1. 센서/태그 기술

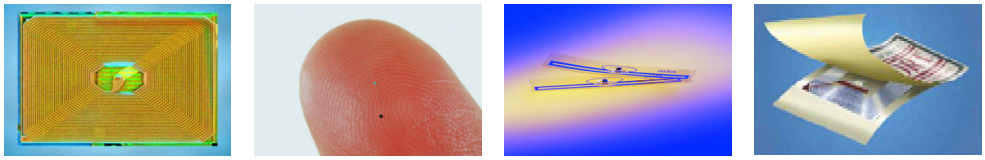
센서(sensor)는 외부의 변화를 감지하는 정보기기의 소자로 유비쿼터스 정보기술의 입력장치에 해당 되며, 사물감지 능력에 따라 수동형(passive)과 능동형(active)으로 나뉘어 진다. 일반적으로 센서는 청각 정보는 물론 빛, 온도, 냄새, 전파 등 물리적 화학적 에너지를 감지하여 그 정보 수집 시스템의 입력신호로 변환하는 장치이며, 최근 자동인식(Auto-ID)는 서비스 산업, 구매 및 유통・재고관리 산업분야, 제조사 및 자재 유통 등 다양한 분야에서 보편화 되고 있는 추세이다. 이러한 센서/태그 기술을 활용하여 기업의 물류비용을 획기적으로 절감할 수 있고, 보다 정밀하면서 손쉽게 소비자의 요구사항 등을 파악할 수 있어, 기업의 경쟁력을 제고시킬 수 있

는 장점이 있다. 무엇보다 기업의 입장에서는 물류 흐름의 투명화 등으로 인한 한결 빠른 Business Process를 구축할 수 있다는 장점이 있다. 센서와 비슷한 개념으로 볼 수 있는 기존의 바코드(Barcode) 라벨은 자동인식 시스템의 혁명을 일으키는 촉매가 되었으나, 저장능력이 낮고 다시 프로그래밍 할 수 없다는 단점을 가지고 있다. 따라서 최근 RFID(Radio Frequency ID)가 유비쿼터스 환경의 새로운 센서/태그 기술로 급부상하고 있다.

가. RFID의 특성 및 활용 분야

RFID란 초소형 마이크로칩과 안테나를 내장한 태그로서 물품 등에 부착되어 전자 방식으로 당해 물품 등에 관한 정보를 표시하고, 감지기(reader, sensor)를 이용하여 정보를 읽고 쓰고 지울 수 있는 것을 말한다. 부착하는 물건의 성상에 따라 원판형, 원통형, 라벨형, 카드형, 상자형 등 여러 형태를 취할 수 있다. 그 안에 개별 식별정보를 수록하고, 전파를 이용하여 감지기에 접촉하지 않고, 또 한 번에 여러 개 태그 안의 정보를 읽고 쓰고 할 수 있으므로 '자동인식 시스템'으로 많이 이용되고 있다. 따라서 RFID 시스템은 개인 생활은 물론 산업 전반에 다양한 응용 서비스가 가능하게 하는 무선감지 장치이다.

〔그림 2－3〕 RFID



자료: 윤훈주, 2004, 유비쿼터스 컴퓨팅 & 네트워크, 2004년 7월 22일 KISDI 발표자료

RFID의 특징을 정리하면 다음과 같다.

- 데이터의 송・수신이 가능하다.
- 비활동성(수동형, passive) 태그는 전지(battery)가 없어도 작동한다.
- 전원이 내장된 경우에는 스스로 전파를 발생시키는 활동성(능동형, active) 태그가 된다.

- 얇고 작게 만들어 물건 속에 집어넣는 것도 가능하다.
- ID정보를 읽기만 할 수 있는 저가형에서부터 각종 데이터를 읽고 쓸 수도 있는 고기능 제품까지 다양하게 나와 있다.

현재 자동인식 시스템으로는 RFID 외에 '바코드', '광학문자판독'(OCR) 장치가 있다. 가장 널리 쓰이고 있는 바코드와 RFID를 비교해보면 RFID가 바코드에 비해 가격을 제외하고는 성능이 뛰어남을 알 수 있다. 따라서 RFID는 기술 및 인프라 측면에서 무선정보처리의 대량 공급이 가능한 새로운 기술이라는 특성이 있으며, RFID의 비접촉식 인식방법, 인식거리, 인식속도 및 데이터 저장 능력은 고객 정보 수집 및 분석에 있어 의미있는 정보를 보다 빠르고 편리하게 기업에게 전달할 수 있다. 이러한 RFID의 특징을 살리고 유기 반도체와 인쇄기술을 적용한다면 얼마든지 새로운 어플리케이션 서비스도 가능할 것이다.

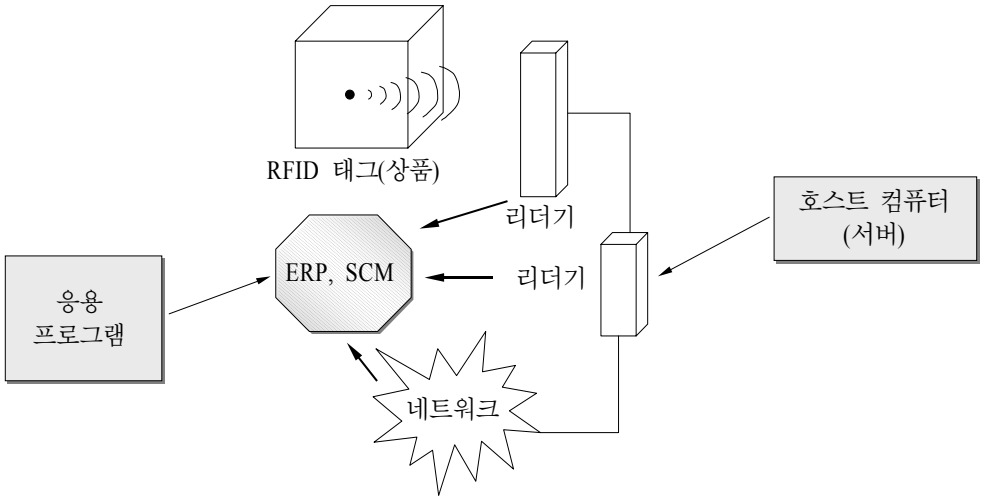
〈표 2－0〉 RFID와 바코드의 비교

	RFID	바코드	2차원 바코드
유니크 ID	칩에 식별자 부여	개별 물품에 부여	개별 물품에 부여
판독거리	수m	수십cm	수십cm
복수 판독능력	○	×	×
피복(被覆) 가능	○	×	×
이동중 판독능력	○	×	×
차폐물 극복능력	○	×	×
기록능력	○(高기능형)	×	×
내 구 성	좋음	매우 취약함	매우 취약함
가 격	상당히 고가. 기술발전에 따라 가격인하의 여지 많음	매우 저렴	저렴

예를 들면, RFID를 생활속의 여러 형태를 고정과 이동 관계로 구분하여 적용할 수 있다. 태그(tag)가 움직이고 리더기(reader)가 고정되어 있다면, 유통, 물류, 교통요금 징수와 같은 분야에서 상품이나 물건이 여러 경로를 통해 이동을 하고 리더기

는 주요지점에 설치가 되는 형태로 적용될 수 있을 것이며, 태그가 고정되어 있고 리더기가 움직인다면, 휴대폰이나 PDA에 리더기가 장착이 되고, 그 리더기를 사용자가 가지고 다니면서 고정된 장소의 정보를 획득하는 형태로 적용될 수 있을 것이다. 또한 태그와 리더기가 모두 움직이는 경우에는 미아찾기와 같은 경우처럼 어린이에 태그를 부착해놓고 미아를 찾아다니는 형태로 적용이 될 수 있으며, 수많은 물건중에서 원하는 물건을 임의로 찾고자 할 때도 적용이 될 수 있을 것이다.

〔그림 2-4〕 RFID 시스템 구성도



자료: 이근호, “무선식별(RFID)기술”, TTA 저널, 제89호.

이렇게 RFID와 같은 유비쿼터스 센서/태그 기술이 적용되는 초기 시장은 기업중심의 산업 및 물류분야가 주도할 것으로 보인다. 무엇보다 RFID 태그 및 리더기 보급 등으로 인해 초기 비용이 많이 들기 때문에 기존의 비용을 절감하고자 하는 기업비즈니스분야에서 사업적 필요에 의해 도입될 가능성이 크다. 후발 시장은 칩 가격의 하락과 많은 제품에 RFID가 적용이 되면 이를 이용한 응용서비스가 많이 파생될 것인데, 개인을 위한 교육 및 사물인식서비스분야로 센서/태그 기술이 확산될 것으로 예상된다. 이외에도 자동정보획득을 통한 각종 생활 편의 서비스나 시각적으로 눈에 보이지는 않으나 감각을 통해 정보를 표시하는 등 정보 교환 수단으로

활용될 수도 있으며, 지능화 시스템을 운용할 수도 있다. 예컨대 개인이 RFID를 활용하기 위해서는 개인휴대형 기기에 내장된 RFID 리더기를 활용하여 상품정보를 얻거나, 마트나 백화점에서 이용이 될 때는 쇼핑을 위한 리더기를 카트에 부착된 상태로 상품정보를 제공할 수도 있다. 또한 초단거리 통신 수단으로 활용될 수도 있는데 주파수특성 및 안테나에 따라 동작거리가 몇 Cm 이내로 제한될 수 있으며, 이러한 짧은 인식거리를 이용하여 개인 인증 및 사용자 의도를 반영한 근거리 통신으로 이용될 수 있다.

나. RFID의 문제점

앞서 제시한 바와 같이 RFID는 소형화, 내재화, 자동 인식 기술 등 편리한 기능이 많지만 데이터의 저장용량이 낮고, OTP(One Time programming)로 태그를 프로그램하여 데이터의 수정이 불가능 하다는 단점을 가지고 있다. 또한 현재 RFID를 이용한 시스템을 운영하는 부분 내에서만 활용되는 폐쇄형 시스템으로, 타 시스템과 호환되는 개방형 시스템이 되기 위해서는 까다로운 보안요구 사항을 만족시켜야 한다.

물리적 충격에 의해 칩이 파괴될 수 있는 가능성이 있으며, RFID의 재활용을 위해 RFID가 부착되어 있는 사물들로부터 칩을 제거하는데 따른 재활용처리기술이 복잡해지고 비싸질 수 있다는 것 역시 기업들이 상업적 목적으로 RFID를 활용하는데 제약점으로 작용한다. 덧붙여 칩의 오동작에 의해 발생되는 손해배상 문제 이슈가 제기될 수 있으며, 칩을 바꿔치기 하거나 복제를 통한 사기문제가 발생할 가능성이 있다.

무엇보다 상업적으로 활용되는 RFID에 관해서 문제시 될 수 있는 것은 개인 프라이버시 침해에 관한 사항이다. 물건 등에 부착된 RFID가 원하지 않는 제 3자가 본인 소유의 물건 실체를 파악할 수 있다는 것에 대한 불안한 심리가 발생할 수 있다. 따라서 물건을 판매할 때 칩의 동작을 정지시키거나 침을 떼어내거나 하는 방안이 마련되어야 하며, 사용자 중심의 대책 이외에 허가받지 않는 정보의 수집을 법적으로 규제할 필요가 있다.[3] 개인과 관련되어서 발생할 수 있는 또 하나의 문제가 RFID

3) RFID에 의한 프라이버시 침해 문제에 관한 사항은 차후 다른 장에서 좀더 심도 깊게 다룰 것이다.

를 통해 지속적으로 교환되는 전파가 인체에 유해하다는 논란이다. 전파의 인체 유해 논란을 방지하게 위해서 전파를 차단할 수 있는 재질을 이용한 전파차단 상품이 등장하여 가방이나 의류 등에 적용하여 프라이버시 침해를 해결하고 몸에 해로운 전자파 차단을 하려는 관심이 더욱 커질 것으로 보여진다. 덧붙여 RFID의 전자파는 전파의 특성상 금속물질, 일부 액체 및 물체 표면의 성격에 따라 인식률의 차이를 보일 수 있어서 정보의 왜곡이 가능하다. 주위에 금속 등 전파반사물이 존재하는 경우, 또는 형광등이나 네온 등 노이즈 발생원이 있는 경우, 또한 부착물의 재질 등으로 인해 주파수 인식률 수준이 달라질 수 있다는 것도 문제점으로 지적된다.

이와 같은 RFID 기술과 관련된 여러 문제점을 해결하기 위해서 제도적 적용방안이나 장치들이 고려될 수도 있을 것이며, RFID 기술 표준에 대한 논의, 복제방지 기술(Blocker tag), 동작주파수 및 인식거리에 대한 시스템 연구들도 진행되어야 할 필요가 있다. RFID와 관련된 보다 자세한 법제도적 기반 마련에 관한 논의들은 후술하도록 하겠다.

2. 네트워크 커뮤니케이션 기술

유비쿼터스 IT에서 언급하는 네트워크 커뮤니케이션 기솔이라고 하는 것은 사물간의 원활한 의사소통을 위해 필요한 기술 분야로 사물과 사물, 사물과 인간을 무선으로 연결하는 WPAN(Wireless Personal Area Network) 기술, 시시각각 위치가 변하는 사물들을 동적으로 연결하기 위한 Ad-hoc 네트워크 기술이 필요하다. 또한 모든 사물에 주소를 할당하기 위한 IPv6(Internet Protocol Version 6) 연구가 활발하게 진행 중이다. 따라서 유비쿼터스 네트워크란－소형 컴퓨터 칩을 가진 사물들이 도처에 편재하여, 이들 간의 상호 연결에 의해 구성된 네트워크를 지칭하며, 유비쿼터스 네트워크 환경이란 사용자가 컴퓨터나 네트워크를 의식하지 않으면서 장소에 구애 받지 않고 자유롭게 네트워크에 접속할 수 있는 환경을 일컫는다. 이에 본 연구에서는 네트워크 커뮤니케이션을 Ad-hoc과 IPv6를 대표적인 유비쿼터스 네트워크 커뮤니케이션으로 살펴보도록 하겠다.

가. Ad-hoc 네트워크 개념과 필요성

Ad-hoc 네트워크는 고정된 기반망의 도움 없이 이동 단말만으로 구성된 자율적이고 독립적인 네트워크로서 통신 기기간의 능동적인 연결 설정이 가능하며, 기기의 자유로운 네트워크의 참여와 이탈을 보장하고 임시적이고, 즉흥적인 네트워크 구성이 용이하다는 장점을 가지고 있다. 또한 고정된 기반망의 도움없이 이동 단말만으로 구성된 자율적이고 독립적인 네트워크로서 통신 기기간의 능동적인 연결 설정이 가능하다. 무엇보다. 언제 어디서나 이용할 수 있는 인간, 사물, 정보간의 최적 컴퓨팅 환경으로 정의되는 유비쿼터스 컴퓨팅에서도 개인과 개인뿐만 아니라 개인과 사물, 사물과 사물간의 직접적인 통신을 위한 이동 Ad-hoc 네트워크의 개념 도입이 요구되고 있다.

특히 유비쿼터스 환경에서 다양한 통신 단말기가 등장하게 되면 이들과 자율적인 네트워크를 구성해야하기 때문에 Ad-hoc 네트워크 구성 필요성이 증대된다. 개인 영역 네트워크(PAN: Personal Area Network)로의 응용 및 네트워크 구성의 용이성 등에 의해 다양한 분야에서의 이동 Ad-hoc 네트워크의 실현이 기대되며, 네트워크의 구성에 필수적인 통신단말기는 과거의 고정 단말기에서 휴대 단말기, 이동단말기, 정보 단말기 그리고 유비쿼터스 단말기로 점차 진화하면서 다양한 형태와 복잡한 개념을 가진 지능화된 단말기 들이 등장할 것으로 예상된다.

이와 같은 Ad-hoc 네트워크는 자기 조직화(Self-organizing) 기능과 자동 인(Auto-recognition) 기능을 이용하여 지능화된 위치 기반 서비스가 가능하기 때문에 언제 어디서든 자신이 위치한 장소 또는 상황에 맞게 적절하게 동작함으로써 특정 지역이나 시점에서 제공하는 서비스를 받을 수 있음을 의미한다. 예를 들면, 대형 쇼핑몰에 이동형 단말기를 들고 가면 현재 진열된 제품에 대한 가격 및 작동법등이 보여주는 동영상이 디스플레이 되며, 현재 제고 물량 등에 대한 상세 정보들을 단말기를 통해 볼 수 있다.

나. IPv6 개념과 필요성

현재 전 세계적으로 정보기기 수요가 기하급수적으로 늘어나고 있어서, 사용자 수요를 감안할 때, 32 비트의 IPv4(Internet Protocol version 4) 인터넷 주소 체계로는

계속적으로 늘고 있는 주소 요구를 충족시킬 수 없다. IETF(Internet Engineering Task Force)에서는 2013경 IPv4 주소가 고갈될 것이라고 예측하고 있다. 따라서 새로운 IP 기술이 필요하지만, 기존의 IPv4에서는 패킷 헤더의 구조상 어려운 면이 많다. 이러한 작업의 일환으로 ITEF에서는 새로운 작업그룹을 결성하여, 1994년도부터 표준화 작업을 진행하였으며, IPv6 프로토콜이 개발되었다. IPv6는 주소의 개수가 많은 것뿐만 아니라 기존 인터넷 보다 보안성(Security)이 뛰어나며, 이동성(Mobility)을 지원하며 품질(QoS)에 대한 고려가 가능하다. 기존의 IPv4와 IPv6의 주요한 특징들을 바탕으로 비교해보면 다음과 같다.

〈표 2－1〉 IPv4와 IPv6의 비교

구분	IPv4	IPv6
주소갯수	약 43억개	약 3.4 X 1038 개
품질제어	품질 보장이 곤란 (QoS 일부지원)	등급별, 서비스별로 패킷을 구분 할 수 있어 품질 보장이 용이
보안기능	IPsec 프로토콜 별도 설치	확장기능에서 기본으로 제공
자동네트워킹	곤란	있음 (Auto configuration 기능)
이동성지원	곤란(비효율적)	용이(효율적)

3. 사용자 인터페이스 기술

앞서 언급한 바대로, 유비쿼터스 환경은 공간적 위치와 사용자 식별이 동시에 가능한 이동 네트워크(Mobile IPv6) 체계를 사용함으로써 정보기기를 직접 제어하는 환경에서 벗어나, 일상환경 속에 기기가 내재화 되게 된다. 따라서 유비쿼터스 환경에서 는 정보기기가 소형화, 지능화에 따른 인터페이스 변화가 요구된다. 무엇보다 개인 정보 처리 효율성을 위한 개인용 정보기기 필요성이 증대되기 때문에 인간 친화적이고 지능화된 사용자 인터페이스 설계가 필수 조건이라 할 수 있겠다. 예를 들면, 키보드, 마우스, 화면 중심에서 음성(억양 등), 동작(제스처 등), 문자, 표정 등

다양한 경로를 통해 정보 수집이 가능하도록 하는 것이다.

따라서 사용자 중심적인 인터페이스 기술을 개발하는 것이 유비쿼터스 환경에 적합한 기술이다. 사용자 중심적인 인터페이스라는 것은 사용자의 성향과 사용범이 제품 기능 결정에 핵심적인 조건이 된다(박세진, 2003). 따라서 유비쿼터스 기술의 인터페이스를 개발하는데 있어 가장 우선시 되는 것은 사용자 분석이 될 것이며, 인간에 대한 일반적인 연구부터 시작해서 누가 주된 사용자가 될 것이며, 그들의 성향은 무엇인지 파악해야 할 것이다. 또한 사용자가 제품이나 서비스를 통해 하려는 작업은 무엇인지를 파악하고 인간의 장단점과 제품의 장단점을 분석하여 담당할 기능을 적절하게 분배함으로써 유비쿼터스 기술 생산품(product)은 최고의 효과를 거둘 수 있게 된다(박세진, 2003).

이와 같이 유비쿼터스 환경에서 인터페이스는 사용자 스스로 정보를 취하고 재배열하도록 하는 시스템이어야 하기 때문에 비선형 시스템(Non-linear System) 방식으로 적용될 필요가 있다. 이러한 비선형 시스템은 사용자와 환경에 유동적으로 대처함으로써 보다 다양한 결과의 가능성, 즉 여러 가지 진행형 상태의 결과들을 제시하는 특성이 있다. 그렇다면, 사용자들은 다양한 결과들 중에서 정보를 선택, 취할 수 있게 되어 사용자가 선택하나 정보에 따라 다시 정보들이 재배열되는 유연한 정보제공 및 선택의 가능성이 증가하게 되는 것이다.

4. 정보보안 기술

유비쿼터스 환경에서는 활용되는 RFID 등은 사용자의 정보를 쉽게 얻을 수 있을 수 있으므로 개인의 정보보안 및 프라이버시가 이슈로 부각되고 있다. 따라서 보안의 취약성을 극복하기 위해 생체정보, 행동특징 등에 대한 정보 활용을 극대화 할 필요가 있다. 특히 RFID 기술은 사람, 제품, 현금의 추적에 사용되어 개인의 프라이버시 침해 위험이 매우 높다. 미국 시민 단체인 전자프라이버시정보센터(EPIC: Electronic Privacy Information Center)는 RFID를 이용하는 환경에서의 프라이버시 위험요인을 다음과 같이 분석하고 있다.

〈표 2－3〉 EPC의 RFID 프라이버시 위험 요인

구 분	설 명
숨겨진 태그 장소	RFID 태그들이 소유주인 개인들이 알지 못한 상황에서 사물들과 문서에 내장되어질 수 있음. －무선전파는 섬유, 플라스틱, 다른 물질들을 쉽게 조용하게 통과할 수 있기 때문에 지갑, 쇼핑 백, 옷가방 등에 들어 있는 사물 또는 옷에 부착된 RFID 태그들을 읽을 수 있음.
전세계 모든 사물들을 위한 유일한 식별자	전자제품코드(EPC)는 지구상에 있는 모든 사물에 유일한 ID를 가지게 할 수 있음. －유일한 ID 번호의 사용으로 개별 물리적인 사물이 판매 또는 이전 시점에서 신원이 확인되고 구매자 또는 소유자와 연결될 수 있는 전세계적인 사물 등록 시스템의 창조가 가능.
대규모 데이터 통합	RFID 배치는 유일한 태그 데이터를 포함하고 있는 대량 데이터베이스의 개발을 요구. －이들 기록들은, 특히 컴퓨터 메모리와 프로세스 능력이 확장되면서, 개인 신원확인 데이터와 연결될 수 있음.
숨어있는 리더	－인간 또는 사물이 모여져 있는 어떤 환경에서도 보이지 않게 섞여질 수 있는 리더들에 의해 태그들은 시야의 제한없이 멀리서 읽혀질 수 있음. －RFID 리더들은 이미 실제로 바닥 타일들에 내재되어 소비자들이 언제 또는 ‘스캔’되고 있는지 없는지에 대한 인식을 불가능하게 하고 있음.
개인추적과 개인정보프로파일	－개인적 신원이 유일한 RFID 태그 넘버와 연결되어 있다면, 개인들이 인식하지 못하는 사이에, 프로파일(profile)되고 추적 당할 수 있음.

따라서 유비쿼터스 환경에서는 정보보안 기술이 요구되는데, 위에서 언급한 RFID 시스템의 보안 및 프라이버시 노출 위험에 대한 안전성을 높이기 위해서는 태그가 태그 소유자의 프라이버시를 노출시키지 않아야 하고, 태그에 저장된 정보가 허가되지 않은 리더기에 노출되지 않는 기술적 솔루션이 필요하다. 또한 태그와 태그 소유자 사이 장기간 유지되는 추적 관련 정보를 만드는 것이 가능하지 않아야 하며, 추적을 방지하기 위해 태그 소유자는 작동되는 태그를 탐지할 수 있어야 하고, 원하는 경우 태그를 작동되지 않도록 하는 기술이 필요하다. 무엇보다 공개적으로 이용 가능한 태그는 태그와 소유자간의 장기간 연결을 피하기 위해 랜덤화가 가능해

야 하고, 쉽게 변결될 수 있어야 하며, 개인 태그에 저장된 데이터는 접근권한에 의해 보호되어야 하고, 안전하지 않은 채널이 가정되어 있다면 암호화 기법으로 보호되어야 한다. 덧붙여 접근제어 메커니즘을 제공하는 것 이외에 태그와 리더사이의 상호인증이 가능하도록 하여 태그와 리더 사이에 신뢰할 수 있는 기술적 기반을 마련해야 하며, 리더와 리더기 사이의 세션 가로채기(Hijacking)과 재생(Replay) 공격, 중간자 공격(Man In the Middle Attack)에 대해 안전해야 한다.

제 3 절 유비쿼터스의 사회・문화적 특징 및 의미

유비쿼터스 기술의 등장은 보다 편리한 기술을 제공해 줄 것이다. 또한 유비쿼터스 기술이 널리 사용되기 시작하면서 우리 사회의 생활 모습에 변화를 가져올 것임에 분명하다. 따라서 유비쿼터스 IT 기술이 가져온 사회적 패러다임의 확대로 인하여 유비쿼터스 사회, 유비쿼터스 문화 형성에 대한 연구에 대한 필요성이 제기되고 있다. 새로운 패러다임의 등장으로 인하여 기업의 입장에서는 기술적 이슈들이 주요 관심이 되며, 일반인들에게는 이러한 기술의 보급으로 인하여 생활 속에서 어떠한 변화가 있을 것인지가 관심이 된다. 또한, 기업에게는 이러한 기술을 활용하여 어떠한 서비스를 제공할 것인지도 중요한 관심 분야가 된다. 일반적으로 유비쿼터스 기술 도입으로 인해 나타날 수 있는 문화를 크게 2가지 관점에서 이해할 수 있다.

첫 번째는 생활속에 기술이 스며들어 컴퓨터의 존재를 의식하지 않게 됨으로써 발생되는 문화이다. 유비쿼터스 기술의 확산으로 인해 컴퓨터는 생활의 배경으로써 사람의 눈에 거슬리지 않는 자연스런 존재가 된다. 이럴 경우 생활의 일부로서 존재하는 컴퓨터를 사용자가 의식하지 않고 사용함으로써 삶이 편리해지며, 사용자에게 있어서는 인터페이스, 디자인같은 측면이 더욱 중요해지게 된다. 두 번째는 언제, 어디서나 네트워크에 접속되고 정보서비스를 이용하는 환경에서 비롯되는 문화이다. 이는 주로 모바일 단말기를 이용하게 됨으로써 형성되는 문화로 현재 휴대폰 단말기를 통해서도 초기 문화가 형성되고 있지만 유비쿼터스 기술의 본격적인 도입으로 인해 더욱 활성화 될 것으로 보인다. 이에 따라 개인은 생활 속의 라이프 스타

일과 관련된 관심을 보이고 있으며, 이러한 라이프 스타일이 여러 사람들과 공유가 되면 새로운 문화가 형성되는 것이다.

그렇다면, 유비쿼터스의 사회·문화적 접근은 무엇보다 인간 중심적이며, 여러 학문이 접목되어 바라보는 것이 중요하다. 인간중심적 관점으로 기존의 기술들을 바라보게 됨으로써 일상생활을 기반으로 하는 새로운 활용분야를 개척하고, 기존 기술들을 새로운 관점으로 해석할 필요가 있다. 또한 유비쿼터스 환경에서는 기존의 기술이나 신기술을 활용하여 생활 속에서 필요로 하는 기능을 가진 다양한 형태의 제품을 개발하여 일상생활의 흐름에 방해되지 않고, 자연스러운 생활의 일부가 되는 제품들이 더욱 필요해 질 것이다. 무엇보다 이러한 유비쿼터스 환경에서는 다양한 컴퓨터 환경, 다양한 단말기가 등장하기 때문에 복잡한 인공지능이 아닌 일상생활의 상식적인 수준 판단을 할 수 있는 컴퓨터가 필요해지며, 누구나 사용하기 쉬운 컴퓨터, 주변 환경에 구애받지 않고 언제든지 사용이 가능한 컴퓨터가 필요해진다. 따라서 공학 분야 내에서 정보기술, 나노기술, 바이오기술, 콘텐츠기술, 환경기술, 로봇기술 등 다양한 공학 분야 내 기술접목이 이루어지게 되며, 사회, 문화, 심리, 인류학, 디자인, 도시, 법제도 등 타 학문 간의 접목이 이루어져서 연구되어야 하는 분야이기도 하다.

따라서 본 연구에서는 유비쿼터스 기술의 도입으로 나타날 수 있는 사회문화 현상을 각 분야별과 기술적 단위에 근거하여 문화 형성을 예측하여 보았다.

1. 분류별 유비쿼터스 문화

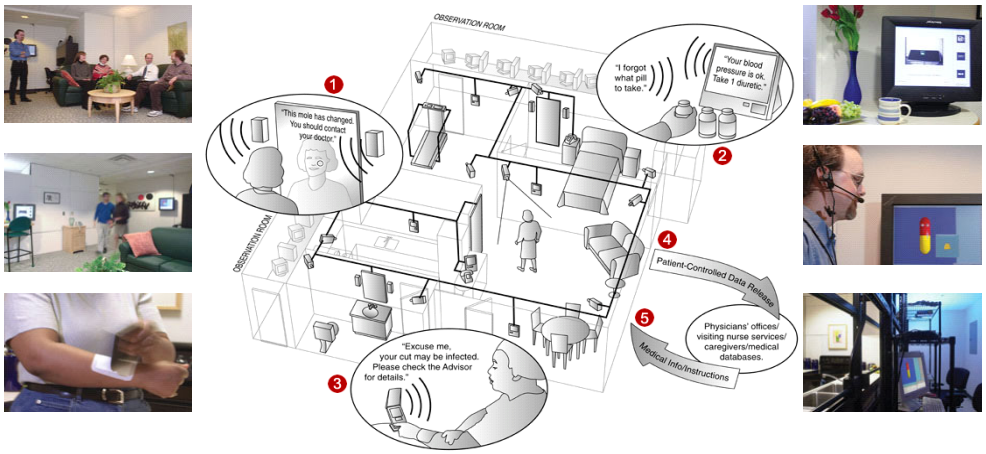
가. 가정 문화

모든 가전 기기들이 홈 네트워크(home network)로 연결되어 있어서 거실이나 안방에서도 집안의 여러 기기들을 제어할 수 있다. 코쿤족과 같은 문화가 더욱 심화될 것으로 보인다. 즉, 소파나 침대에서 일어나지 않고 가정내의 대부분의 일을 처리할 수가 있다. 이러한 홈 네트워크 문화에 따라 가정내 가전기기를 별도의 리모컨이 아닌 개인이 휴대하는 휴대폰으로 제어함으로써, 휴대폰 중심의 가정문화가 형성이 된다. 즉, 집에서 시청하는 텔레비전의 채널을 휴대폰의 버튼을 눌러서 컨트

롤하게 되어 가정내의 개인문화가 발전하게 될 것으로 보인다.

또한 가정 내 침대 및 소파에 각종센서가 달려있어 사용자의 활동을 인식하게 된다. 몸무게를 단다거나 움직임 감지를 통해 거실내 가전기기를 켜거나 끌 수 있다. 전기를 일일이 신경쓰며 끌 필요없이 자동으로 감지하여 제어를 하게 되어 전기절감효과를 가져온다. 또한 가정 내에서 원격으로 건강검진이나 진료를 할 수 있게 되어 노약자의 건강은 물론 수시로 건강을 체크할 수 있어 훨씬 풍요로운 생활을 즐길 수 있게 된다.

〔그림 2－5〕 Smart medical home 구축 예시



자료: 윤훈주, 2004, 유비쿼터스 컴퓨팅 & 네트워크, 2004년 7월 22일 KISDI 발표자료

유비쿼터스 기술이 가정생활 속으로 스며들어 발생하는 효용성을 김선경(2003)은 연결 용이성, 정보 획득의 용이성, 커뮤니케이션 용이성, 제품구매 용이성, 주거 생활의 편리성 등으로 나누고 있다. 즉, 가정 내 모든 전자 제품과 기기들이 지능화되어 연결되어 있기 때문에 사용자 입장에서는 언제 어디서든지 하나의 단말기로 가정내 기기들과 연결하여 작동하거나 기기들에 대한 정보를 파악할 수 있으며, 커뮤니케이션 할 수 있다. 또 가정 내 필요한 물건들을 자동적으로 파악하여 제품을 구매하거나 가정 구성원들에게 현재 필요한 제품만을 선택적으로 주문할 수도 있을 것이다. 이를 통해 더욱 편리하고 건강한 가정생활을 영위할 수 있게 된다.

나. 사무실 문화

유비쿼터스 기술은 일하는 환경에도 많은 변화를 가져올 것이다. 고정된 사무실이 아닌 휴대기기 및 전국적으로 네트워크화 된 오피스 서비스로 인하여 전국 어디서나 고정사무실처럼 각종 작업 및 정보 서비스를 받을 수 있다. u-프린팅 서비스, 전자 카달로그, 전자칠판, 전자책이 기반이 된다. 이렇게 이동형 근무 환경 조성으로 인해 원격지에 떨어진 구성원끼리 실시간 화상시스템을 이용하여 생생한 회의를 진행할 수 있다. 마치 한 장소에 있는 것처럼 느낌을 갖게 되며, 사무실 책상에서도 이러한 회의가 가능하다. 벽면에 내장된 디스플레이를 통하여 상대방을 보면서 자연스레 대화가 가능하다. 장소의 구분이 없게 된다.

또한 일에 따라서 웨어러블 디스플레이를 이용하여 야외에서 이동을 하면서도 각종 컴퓨터 작업이 가능하다. 도면과 같은 정보를 디스플레이를 통해 보면서 작업이 가능하다. 건설현장이나 복잡한 기계수리 작업이 가능하다. 컴퓨터는 음성인식, 장갑, 손동작 인식, 휴대형 입력장치를 통해서 쉽게 컴퓨터 제어가 가능하다. 인간 친화적 인터페이스 등장이 예상된다.

다. 청소년 놀이 문화

유비쿼터스 기술은 가정과 사무실 뿐만 아니라 대인관계에도 상당한 영향을 미치게 되는데 현재 휴대폰과 같은 이동형 단말기를 통해 친구들과 문자를 보내는 것은 단순한 놀이가 아니라 교우 관계를 형성하고, 또래 문화를 형성하고 있다. 휴대폰을 자꾸 만지작 거리는 느낌은 심리적 안정감을 부여하게 되며 이는 중, 고등학생과 같은 젊은층에게 많이 나타나는 증상이다. 따라서 휴대폰에 기반한 또래문화가 발전하게 되는데 이는 “철저하게 개인 기기인 휴대폰이 개인적이고 자기표현 욕구가 강한 디지털 세대와 만났기 때문”이라고 설명할 수 있다. 즉 때와 장소에 구애받지 않고 쓸 수 있는데다 상대의 즉각적인 반응을 얻을 수 있기 때문이다. 특히 유비쿼터스 시대에는 휴대폰 단말기를 통해 많은 서비스를 주고 받고, 커뮤니케이션이 일어나기 때문에 휴대폰을 통한 청소년 문화 형성은 더욱 주목을 받을 것으로 예상된다.

라. 사회문화

언제, 어디서나 다른 이들과 접속이 가능한 유비쿼터스 시스템의 발전은 현재 인터넷이나 휴대폰으로 연결된 집단보다 훨씬 발전된 자발적 네트워크 집단 결성하여 사회에 긍정적인 힘을 발휘할 수 있을 것으로 예상된다. 예를 들면, 경찰의 휴대전화를 범죄신고망으로 활용하다던지, 개인의 휴대폰에 위험요소 탐지 기능을 추가시켜 자율방범대원으로 활동할 수도 있게 된다. 이러한 자발적인 사회참여 및 사회감시 역할로 인해 커뮤니티 파워가 증대되어 사회적 투명성이 향상되고, 사라져 가던 사회적 신뢰(social trust)가 회복될 수 있다.

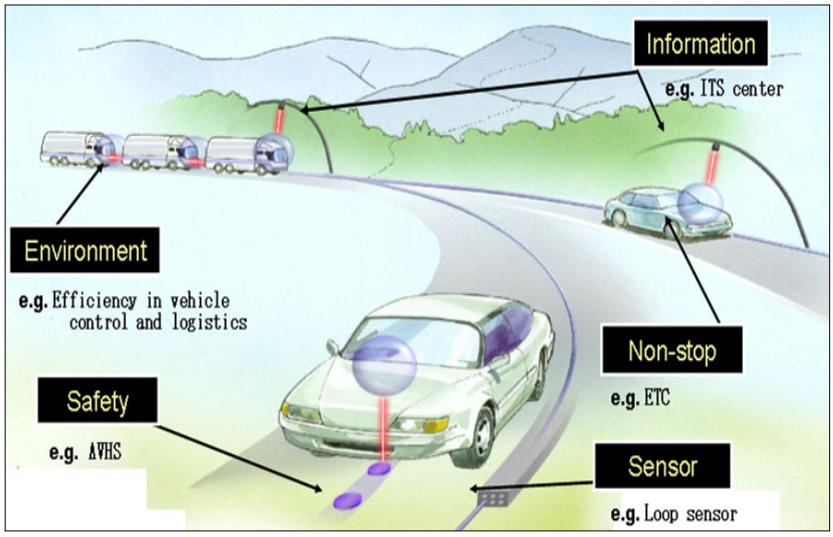
마. 자동차문화

앞으로는 자동차안에서 보내는 시간이 많아지면서 다양한 차량문화가 형성이 된다. 자동차를 개성에 따라 꾸미려는 카데코 문화에서부터 자동차를 여가활동의 수단으로 이용하는 사람이 많다. 특히 유비쿼터스 기술이 자동차에 적용되기 시작하면서 운전습관도 변화가 예상된다. 예를 들면, 스마트 자동차(smart car)의 경우에는 네비게이션을 활용해 도로 안내, 자동 요금 징수, 주차장, 주유소 내 자금 결제 등을 할 수 있게 되고, 차간거리 및 차선 위치 등을 자동 측정해서 사고를 방지하는 첨단 안전기능을 수행할 수 있게 된다. 여기서 ITS(Intelligent Transport System)의 진보로 운전자는 실시간으로 도로정보를 얻을 수 있어서 쾌적하고 안전한 운전을 할 수 있게 된다.[4] 자동차에 타면 휴대하고 있는 휴대폰을 자동차 거치대에 올려놓는 패턴이 형성되며, 다양한 악세사리가 제품이 등장하게 될 것이다. 휴대폰을 통한 자동차 원격제어를 하는 사람도 등장하게 되며, 자동차운전을 위한 인증수단도 휴대폰이 하게 될 것으로 보인다. 이는 자동차 도난방지를 위한 것이다. 또한, 교통사고시 휴대폰을 통한 사진촬영이 필수적인 생활습관이 될 것이다. 이러한 사진은 보험회사 직원과 실시간 전송이 되어 적절한 사고처리가 빠른 시간에 가능하다.

---

4) 스마트 카의 단계는 일반적으로 1단계 네비게이션 시스템 개시, 2단계 ETC(Electronic Toll Collection System), 3단계는 VICS(Vehicle Information and Communication System)으로 교통정보, 소요시간, 주차장 정보 등 자동차와 도로가 대화하는 수준으로까지 이끌어내겠다는 계획을 세우고 있다.

〔그림 2－6〕 유비쿼터스 기술을 이용한 교통 환경 예시



2. 기술적 단위에 근거한 문화형성 예측

가. 카메라기반 생활문화

디지털 카메라가 개인 중심으로 보급, 사용되기 시작하면서 음식, 풍경, 이벤트 등등의 각종 생활속의 모습을 카메라로 찍어 실시간으로 인터넷에 올리는 1인 미디어 문화가 더욱 활발해진다. 또한 블루투스와 같은 개인 근거리통신망의 보급이나 휴대인터넷이 보급되면서 같은 장소에 있는 사람들끼리 사진을 나눠갖거나 시공간의 제약없이 서로간의 일상생활을 공유하는 문화가 활성화 될 것으로 예측된다.

또한 바코드의 진화된 형태인 컬러코드를 이용한 정보수집 및 연결문화가 형성될 것으로 보인다. 책을 보면서 마음에 드는 내용이 있으면 컬러코드를 찍어 더욱 자세한 정보를 얻게 된다.

나. 위치 기반 생활문화

GPS 및 휴대폰 위치인식 기술에 의해 사용자의 위치정보를 이용한 LBS가 활성화 될것이다. 여행지에서의 관광정보, 시내중심지에서의 식당이나 가게 찾기, 각종 쿠폰 서비스, 근거리 친구찾기 등등의 서비스를 통해 자신이 있는 지점을 통해 즉시

무언가를 찾고자 하는 문화가 형성될 것으로 보인다.

〔그림 2－7〕 휴대폰을 통한 위치 기반 생활 문화

자료: 윤훈주, 2004, 유비쿼터스 컴퓨팅 & 네트워크, 2004년 7월 22일 KISDI 발표자료

이러한 장소관련 정보나 위치기반 서비스의 활용은 처음와 본 곳이라도 익숙하게 길이나 가게를 찾게 됨으로써 편안한 생활을 영위할 수 있게 된다. 앞서 설명한 바와 같이 휴대폰이 가장 대표적인 위치 기반 서비스 단말기로 활용될 것이지만, 스마트 인공물을 통해 새로운 공간에 대한 정보를 제공할 수도 있다.

다. 커뮤니케이션 생활문화

지하철, 버스, 집, 학교에서 항상 누군가와 대화하고 연결하는 문화가 형성된다. SMS와 같은 저렴한 서비스를 이용할 수 있고, MMS(multi-message service)와 같은 서비스를 이용할 수도 있다. 블루투스와 같은 개인근거리 통신망을 이용하여 비용을 들이지 않고 주변의 사람들과 커뮤니케이션을 이룬다. 이는 Ad-hoc시스템의 개념을 기반으로 할 수도 있다.

제 3 장 공공부문에서의 유비쿼터스 제도화 구현 및 역기능 대비 요약

제 1 절 유비쿼터스 도입을 위한 IT법률의 정비방안

1. 유비쿼터스 IT 기술과 현행 정보통신법제와의 양립 가능성

현행 정보통신법이 유비쿼터스 IT기술을 포괄하고 있는지에 대한 검토가 선행되어야 한다. 정보화촉진기본법은 제2조 제1호상의 “정보”개념을 처리정보(data)로만 한정하고 있어서, 유비쿼터스 IT기술이라는 제2의 정보혁명의 사회에서는 적절하지 않다. 따라서 온라인과 오프라인을 망라할 수 있는 정보(Infomation)으로 규정되어야 한다.

※ 정보화촉진법 제2조제1호 정보: 자연인 또는 법인이 특정목적을 위하여 광 또는 전자적 방식으로 처리하여 부호・문자・음성・음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식.

※ 정보공개법 제2조제1호 정보: 공공기관이 직무상 작성 또는 취득하여 관리하고 있는 문서・도면・사진・필름・테이프・슬라이드 및 컴퓨터에 의하여 처리되는 매체 등에 기록된 사항.

또한 유비쿼터스 하에서는 정보의 개념이란 단순히 처리형태가 중요한 것이 아니고, 아울러 자료나 지식이 아닌 것도 정보일 수 있다. 결론적으로 종래의 개념정의가 아닌 “기록 또는 전자적 방식에 의하여 처리된 사항”으로 포괄적으로 규정함으로서 수동정보인 기록과 자동정보인 처리정보를 포괄하는 개념으로 규정되어야 한다. 유비쿼터스 IT기술은 기존의 정촉법상의 “정보화 촉진”이라기 기반시설적인 측면의 소극적인 측면이 아닌 능동적으로 실시간으로 정보활용이 가능한 환경을 제공해주는 시스템이므로, 종래의 정보화촉진법으로서는 포괄하기 어려우므로 이에 대

한 개념 정립과 제도적인 규율 범위에 대한 근거가 마련되어야 한다.

광대역통합망의 경우에 현행 망법 제2조 제1호의 정보통신망의 개념으로 포괄하기 어려우며, 특히 전기통신기본법 제2조 제6호의 전기통신역무(전화 역무, 통신회선임대 역무, 주파수제공 역무, 인터넷 접속 역무 등)와 관련한 사업을 규제하는 데에 적절치 않다.

2. 현행법하에서의 유비쿼터스 IT기술을 포함하는 방법

유비쿼터스 기술을 현행 정보통신망 관련 법제와 조화시키는 방으로 우선 정보화촉진기본법을 활용하여 동법 제2조 제7호로서 유비쿼터스 IT기술의 정의규정과 기본 원칙을 명시할 수 있다. 개별법상의 개정이 아닌, 새로운 법률을 제정하여 유비쿼터스 IT 법으로서의 새로운 구조적인 전환도 고려할 수 있다. 유비쿼터스를 포괄하는 새로운 정보통신 기본법은 유비쿼터스 뿐만이 아니라, 기존의 통신법, 정보법 등과의 연동성을 확보할 수 있어야 할 것이다. 세부적인 사항은 다음과 같다.

○ 정보화촉진법상의 근거조항 확보

– 정보화촉진기본법상의 유비쿼터스 IT 기술 관련 규정의 삽입을 통하여 기존의 정보통신기술을 뛰어 넘는 유비쿼터스 IT 기술에 대한 지원규정을 기본법상에서 확보함.

– 정보화촉진기본법상의 개정사항

- 법 제2조제7호에 유비쿼터스IT 기술에 관한 정의 삽입
- 법 제2조제1호의 정보개념의 개정
- 법 제2조제4호의 정보보호 대신에 “정보보안”의 개정

– 정보통신망이용촉진및정보보호등에관한 법률의 개정사항

- 법 제2조제1항상의 정보통신망 개념 개정
- 법 제2조제2항상의 정보통신서비스 개념 개정
- 법 제2조제3항상의 정보통신망서비스제공자 개념 개정
- 법 제2조제6항상의 개인정보 개념 개정
- 법 제3조상의 정보통신서비스제공자의 책무 강화

－ 전기통신기본법의 개정사항

• 법 제2조 제1호의 전기통신 개념 개정

• 법 제2조 제7호의 전기통신역무 개념 개정

• 법 제7조의 전기통신사업자의 구분 개정

－ 전기통신사업법의 개정사항

• 법 제2조 제1호의 전기통신 개념 개정

• 법 제4조 제1호의 전기통신사업의 종류 개정

또한 유비쿼터스 IT기술 개발과정에서 연구개발기관간의 정보교류 및 정부의 개입을 통하여 연구개발을 효율화 할 필요가 있으므로, 정보통신기술의 연구・개발체계를 효율화할 의무를 부과하기 위한 규정이 필요하다.

제 2 절　유비쿼터스(Ubiquitous) 환경에서의 개인정보보호법제

1. 서　론

정보사회에서는 어디에서든지 존재하고 있는 것이 컴퓨터이며 이 안에는 Bit(이진수 단위)와 byte(8bit) 단위로 이루어진 헤아릴 수 없을 정도의 개인정보가 저장되어 있다. 국가의 컴퓨터 안에는 국민의 가족사항, 재산상태 등에 관한 기록이 담겨있으며, 또한 국민이 어디에 주거하던지 그의 이동경로가 담겨있기도 하다. 그리고 민간부문에서도 많은 개인정보가 유통되고 있다. 이제는 누구라도 슈퍼마켓, 약국, 각종 웹사이트 등 개인이 접촉하는 곳이면 어디에서나 개인정보를 수집할 수 있게 되었다. 그러나 우리는 급변하는 환경 속에서 날마다 누군가에 의해서 엄청난 양의 디지털 정보가 수집・사용・가공 및 공유되고 있다는 사실을 인식하고 있음에도, 거기에 정확하게 어떠한 해악이 있을 것인지 예측하지 못하고 있는 것이 현실이다.

더구나, 정보통신기술의 비약적인 발전으로 인간의 주변에 있는 모든 사물 안에 컴퓨터 기능을 탑재하거나, 또는 인간이 소지하고 다니는 소형 단말기에 컴퓨터 기능을 부착하여 “언제, 어디서나” 인간 삶의 모든 것을 관리하고 감독할 수 있는 시대(유비쿼터스 시대)가 도래하였다. 이에 따라 새로운 정보통신환경에서는 언제 어

디서나 다양한 정보를 수집・가공・처리할 수 있게 되었고, 개인정보 침해 위험성은 더욱 커졌다. 예들 들어, 차세대 PC는 개인신상명세, 서비스사용 종류, 위치정보, 생체정보를 비롯한 사용자에 대한 다양한 개인정보를 수집하고 저장하며, 이를 바탕으로 각 사용자에게 특화된 서비스를 제공하기도 한다. 이러한 특성은 사용자의 편리성을 증대시키는 반면, 차세태 PC는 네트워크 기반으로 무선통신을 이용하여 주변의 장비들과 정보를 빈번하게 교환하기 때문에 자신도 모르는 사이에 정보가 제3자에게 노출될 위험성도 더욱 증대시킨다.

아직은 우리가 이러한 유비쿼터스 환경을 피부로 느낄 만큼 일상화되어 있지는 않은 것 같지만, 유비쿼터스 컴퓨팅 환경은 이미 그 징후를 보이고 있고, 이로 인한 프라이버시 보호 문제는 조속히 해결하여야 할 커다란 사회적 이슈로 대두되고 있다. 어디에서든지 네트워크에 접근할 수 있다는 말을 뒤집어 보면, 어디에서든지 정보가 누출되고 왜곡될 위험성이 있다는 것을 의미하기도 한다. 어디에서든지 컴퓨터를 사용할 수 있는 “유비쿼터스”이기 때문에 어디에서든지 ‘안심하고’ 사용할 수 있는 제도적, 기술적 장치를 마련하지 않는다면, 유비쿼터스 환경에서 발생할 수 있는 개인정보침해 현상을 통제할 수 없을 것이다.

본 논문에서는 유비쿼터스 시대의 도래로 인한 정보통신환경 패러다임의 변화를 간단히 살펴보고, 개인정보 보호를 위한 법제도 측면에서의 현황과 전망을 살펴보고자 한다.

2. 유비쿼터스 환경과 개인정보보호법제 현황

가. 유비쿼터스 환경과 역기능의 문제

유비쿼터스 환경에서는 홈네트워크의 보편화, 24시간 맞춤형 행정서비스제공, 교육・보건・환경・교통 등 사회인프라의 지능화, 소외계층의 사회활동 참여확대 등 편리하고, 안전하고, 윤택한 삶을 누릴 수 있게 된다. 그러나 반면, 주변의 모든 사물 안에 컴퓨터 기능을 부착하여 언제, 어디서나 인간의 모든 것을 관리하고 감독할 수 있는 유비쿼터스 시대가 도래함에 따라 개인정보 침해의 위험성이 커지고 있다. 차세대 PC는 개인신상명세, 서비스사용 종류, 위치정보, 생체정보를 비롯한 사

용자에 대한 다양한 개인정보를 수집·저장하며, 이를 토대로 각 사용자에게 특화된 서비스를 제공할 수 있고, 그 결과 사용자의 편리성은 증대되지만, 무선네트워크 기반으로 주변의 장비들과 빈번히 정보를 교환하기 때문에 자신도 모르는 사이에 정보가 누출될 위험성도 크게 증대된다.

예를 들면, RFID 사용으로 인한 프라이버시 침해는 매우 다양할 것이며, RFID 서비스 자체에 대한 이해가 부족할 경우 정보처리자에 의한 개인정보의 오남용 행위를 방지하기 매우 어렵다. RFID를 부착함으로써 어떤 개인의 의류에서 신체정보를, 지갑에서 현금 및 카드정보 등 신용정보를, 가방 안의 의약품, 서적, 기타 소지품 등에서는 개인의 의료정보, 사상정보, 취미정보, 위치정보 등을 용이하게 파악할 수 있다. 또한 RFID의 ID가 유일하기 때문에 개인의 위치정보가 직접적으로 누출될 우려가 있으며, RFID와 연계된 텔레메틱스 서비스를 통하여 개인의 위치정보 뿐만 아니라 소비, 취미 등 상황정보까지도 누출될 수 있다.

이러한 환경에서는 기존의 컴퓨터에 저장되어 있는 이름이나 연락처 등 단순한 개인 신상정보 누출의 수준에 그치지 않고, 개인의 이동경로에 따라 위치정보, 소비정보, 의료정보 등 '실시간으로 예민한 정보'가 누출딘다는 점에서 그 위험성이 더욱 심각하다. 이용자 입장에서도 프라이버시 또는 개인정보의 보호문제가 중대한 관심사로 떠오르게 될 것이다. 결국 유비쿼터스 환경의 안전성과 신뢰성이 보장되지 않는다면 이용자는 IT 관련 서비스제공을 외면하게 될 것이다. 결국 안전성이 확보되지 않는 IT산업의 기반형성은 사상누각이 될 것이다.

나. 현행 개인정보보호법제의 문제점

1) 기술중립적 입법의 부존재

기존의 정보통신환경을 중심으로 한 현행 개인정보보호법제는 정보통신기술의 비약적인 발전을 포괄하기에는 역부족이다. 즉 유비쿼터스 컴퓨팅의 발전으로 인한 새로운 정보통신기기 및 매체의 정보유통에 의한 개인정보 침해 유형을 규제하기에는 현행 법제로는 그 규제의 사각지대가 존재할 수 밖에 없다.

현행 정보통신망법은 법 적용대상 사업자의 범위를 정보통신서비스제공자 및 정보통신서비스제공자 이외의 자로서 학원, 여행사, 항공사 등 일부 off-line 사업자에

한정하고 있고, 기타 규제대상에 대하여는 각 주무부처에서 개별법에 의해 규제하고 있기 때문에 개인정보를 취급하는 모든 자에 대하여 적용할 수 없는 사각지대가 잔존하고 있다. 이러한 사각지대로 인하여 보호되는 개인정보의 범위가 그 만큼 제한된다는 약점을 가질 수 밖에 없다. 예컨대, 정보통신망법은 그 규제대상을 정보통신서비스제공자등이 수집하는 개인정보와 전기통신 역무를 기준으로 규정하고 있기 때문에 개인용 컴퓨터 등 독립형(stand-alone) 정보처리장치를 통해 수집되는 개인정보를 포괄하지 못하고 있다. 또한 신용정보 등 개인정보와 연계된 RFID에 탑재된 정보의 유출로 인한 개인정보침해 및 개인의 사물에 부착된 센서로 인한 개인정보침해 등의 문제를 규제할 방법이 없다.

EU는 기술적 입법원칙을 고수하기 위하여, 2002년 7월 「정보통신분야에서의 개인정보처리 및 프라이버시보호에 관한 지침」(Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector)을 개정하였다. 이 개정의 목적은 이전의 지침(97/66/EC)의 내용을 전면적으로 변경하여 새로 제정하고자 하는 것이 아니라, 새롭게 등장하는 예측 가능한 통신기술의 발전을 수용하고 이를 적용할 수 있도록 하자는 것이었다. 개정 지침은 이전 지침의 "통신서비스와 통신망(communication service ,communications network)"이라는 용어를 "전자통신서비스와 전자통신망(electronic communications service, electronic communications network)"으로 대체함으로써, 공적인 정보통신망 서비스 이용자에게 동일한 수준의 개인정보 및 프라이버시 보호를 제공할 수 있도록 정보통신 서비스 시장과 기술의 발전사항을 반영하였다.[5] 이 지침 제3조 제1호는 "본 지침은 EU 공동

---

5) 기존의 지침(97/66/EC)은 "통신서비스(telecommunications service)"를 "라디오와 TV 방송을 제외한 통신망에서 전체적 또는 부분적으로 신호의 전송 또는 경로를 구성하는 서비스를 말한다"고 정의하고 있는데, 유럽위원회는 기존의 지침으로는 새롭게 등장하는 통신기술에 대하여 대처할 수 없음을 인식하게 되었다. 예컨대 위치정보 등 그 규제의 범위를 넘어선 분야에 대해서는 기존의 지침을 적용할 수 없다는 문제점을 인식한 것이다. 이러한 이유로 적용범위를 확대할 필요를 느끼고, "통신서비스"라는 용어를 "정보통신서비스(electronic communications service)"라고 확대 변경하고, 그 정의를 "라디오와 방송망에서의 전송서비스를 포함한 정보통신망에서의 신호의 전송을 주

체 내의 공중통신망에서의 정보통신서비스 제공과 관련한 개인정보의 처리에 적용된다"고 규정[6]하여 기술중립적 입법임을 명확히 하고 있다.

2) 개인정보의 정의

"개인정보"란 "본인의 의사에 반하거나 본인이 알지 못하는 상태에서 이용될 경우 정보 주체(혹은 당사자)의 안녕과 이해관계에 영향을 미칠 수 있는 개인과 관련된 모든 정보"로 폭 넓게 해석되어야 한다. 개인정보는 인격을 이루는 요소이면서 표현의 자유 등 헌법상 인정되는 다양한 기본권과 밀접한 관련이 있는 정보로서 오·남용될 경우 개인의 인격적·재산적 권익을 손상시킬 우려가 있으므로 모든 개인정보는 개인의 인격 존중 이념에 따라 신중히 취급되어야 하기 때문이다. 이러한 면에서 "개인정보 침해"라 함은 "당해 정보주체와 관련된 제반의 정보가 오·남용(도용, 변경, 유출, 훼손 등)됨으로써 정보 주체의 자기정보통제권이 침해되는 것"을 의미한다고 정의할 수 있다. 여기에서 "자기정보통제권"이라 함은 "자신에 관한 정보의 수집·이용·공개·제공 등을 본인이 통제할 수 있는 권리"를 의미한다.

현행 정보통신망이용촉진및정보보호등에관한법률(이하 '정보통신망법'이라 한다) 제2조는 "개인정보라 함은 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다"고 규정하고 있다. 그리고 공공기관의개인정보보호에관한법률은 "개인정보라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다"고 규정하고 있다.

로 구성하는 서비스를 말한다"고 정의하고 있다. 결국 이렇게 용어의 정의를 새롭게 한 것은, 개정 지침(2002/58/EC)을 사용되는 통신기술에 관계없이 정보통신을 위한 다양한 모든 종류의 전송서비스에 적용할 필요가 있기 때문이다.

6) Directive(2002/58?EC) Article 3: 1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

이러한 법률상 정의에 의하면, 개인정보라 함은 “신원을 확인할 수 있는 개인에 관한 일체의 정보”를 의미하며, 따라서 신원을 확인할 수 없는 형태로 수집·처리되는 어떤 개인에 관한 여기의 개인정보에 해당하지 않는다. 다만, 신원을 확인할 수 없는 정보라도 그 속에 개인의 신상정보가 포함되어 있고, 다른 개인정보들과 결합하여 쉽게 신원확인이 가능한 개인정보는 보호의 대상에 포함된다.[7)]

그러나 기존의 정보통신 환경에서 수집되는 개인정보와 유비쿼터스 환경에서의 개인정보는 그 내용 및 중요성 면에서 근본적인 차이가 있다. 기존의 정보통신 환경에서 유통되는 개인정보는 주로 개인의 신상정보 또는 신용정보가 주류를 이루었고, 따라서 개인을 식별하고 확인하는데 그치는 경우가 많았다. 더구나 이들 정보는 정보시스템에 저장되어 있는 것이어서 참신하고 새로운 것이 아닌 정보도 적지 않았다. 반면에 유비쿼터스 환경에서 유통되는 개인정보는 단순한 신상정보 이상의 것이 대부분을 이루게 된다. U-Commerce 등 신유형 산업의 등장은 개인이 지니는 컴퓨터 및 내장된 기기를 통해서, 그리고 각종 사물에 내장된 보이지 않는 컴퓨터 단말기를 통해서 언제 어디서나 실시간·연속적으로 추적하며 정보수집과 마케팅 활동을 가능하도록 하였다. 이러한 활동은 유비쿼터스 환경에서는 온라인과 오프라인을 가리지 않고 모든 분야에서 통합된 상거래의 형태로 이루어지기도 한다. 이렇게 수집되는 개인정보의 내용은 단순한 신상정보나 소비정보 이상의 것이다. 컴퓨터 센서와 칩 등을 통하여 추적되는 위치정보, 이동정보, 대금결제 정보, 소비정보, 건강정보 등 개인의 생활이 낱낱이 공개되는 민감한 정보가 대부분이다.

또한 유비쿼터스 환경은 전술한 바와 같이 저장이나 전송이 어려웠던 개인이 보유한 고유한 지식이나 기술의 노하우를 쉽게 저장하고 전달할 수 있는 네트워크를 갖추고 있다. 이는 민감한 개인정보라는 의미 이상의 중요한 인격권과 재산권의 총합체를 수집하고 제공할 수 있음을 의미하는 것이다.

그렇다면, 정보통신환경의 변화에 따라 개인정보의 보호범위는 달라질 것인가?

---

7) 주요 각국의 개인정보보호법에서 “개인정보”에 관한 정의는 거의 유사하게 규정되어 있다. 다만, 개인정보를 정의함에 있어 “표현상 차이”는 있으나, 일반적으로 “식별가능한 개인(identified or identifiable individual)에 관한 모든 정보”를 의미한다.

즉, 현행의 법제상의 개인정보의 범위에 새로운 유형의 개인정보를 추가하여야 할 것인가의 의문이 있을 수 있다. 시대가 변하고 정보기술이 발전하여도 “개인을 식별할 수 있는 일체의 정보”라는 개인정보의 기본적인 개념은 변하는 것이 아니다. 정보통신기술의 발전에 따라 생성되는 위치정보, 생체정보, RFID에 포함된 개인정보, 텔레메틱스 서비스를 위한 개인정보 등은 어떠한 정보통신 매체를 통해 유통되는 개인정보라도 역시 개인정보임에 변함이 없기 때문이다. 결국, 문제는 개인정보의 보호 범위가 아니라 다양한 네트워크를 통해 유통되는 개인정보를 어떻게 보호할 것인지의 여부이다. 즉, 급변하는 정보유통 환경으로 인한 현행 법제도의 개인정보보호 일반원칙(수집제한의 원칙 등) 적용의 곤란함을 어떻게 해결할 것인지의 여부가 관건이 된다.

다. 유비쿼터스 환경에의 개인정보보호 일반원칙의 적용 여부

개인정보보호와 관련한 법을 가지고 있는 주요 국가들은 예외 없이 정보주체로부터 정보를 수집하는 경우에는 명시적 동의를 얻어야 한다는 원칙 및 정보수집 및 사용에 대한 고지 및 공정(Notice and Fairness)의 원칙들을 적용하고 있다. 고지원칙은 정보수집자들이 정보주체에게 그들의 개인정보제공에 대한 건전한 판단을 할 수 있도록 충분한 정보를 제공하는 것을 요구하는 것이다. 또한 공정원칙은 정보사용자들이 어떻게 정보가 사용될 것인지에 관한 개인의 이해에 불합치한 방법으로 개인정보를 사용하지 말 것을 요구하는 것이다. 이러한 원칙들은 자기정보통제권을 보호하기 위한 최소한의 원칙들이다.[8] 그러나 유비쿼터스 환경에서의 정보유통은

8) 개인정보보호 원칙 중 대표적인 것이 1980년의 OECD의 「프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인」(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)의 개인정보보호 8원칙이다. 이 지침은 세계 각국의 개인정보보호법의 준거가 되었다. 그 핵심 내용 중의 하나가 개인정보의 수집은 원칙적으로 제한되어야 하고, 합법적이고 공정한 절차에 의해 정보주체의 인식 하에 또는 동의를 얻은 후에 수집되어야 한다는 것이다(수집제한의 원칙). 그리고, 1995년에 EU는 OECD 가이드라인의 8원칙을 기본 내용으로 하는 「개인정보의 처리 및 자유로운 전송에 관한 개인정보보호 지침」(Directive on the protection of individuals with regards to the processing of personal data and the free movement of such data; 95/46/EC)을 제정하여 유럽

현행 개인정보보호 정책 또는 관련 법령 등으로는 정보주체의 권리를 보장하기 어렵다는 이슈를 제기하고 있다.

라. 정보수집 방법・경로의 상이함 및 동의획득의 곤란함

유비쿼터스 환경에서는 실시간・연속적으로 어디에서라도 개인과 관련된 환경에서의 컴퓨터, 휴대전화, 사물에 내장된 칩 등으로부터 자동적으로 수집된다. 이러한 정보 수집은 정보주체가 인식한 상태에서 이루어지는 경우도 있겠지만, 일반적으로는 정보주체가 인식하지 못한 상태에서 이루어진다. 유비쿼터스 컴퓨팅의 대표적 특성 중의 하나가 아무런 의식 없이 컴퓨터를 사용하는 것(invisible)임을 고려할 때, 대부분의 정보주체는 자신의 정보가 누군가로부터 수집되고 있다는 사실을 인식하지 못할 것이다.

한 개인이 기존의 회원가입신청서에 기입하는 행위나, 웹사이트에 가입하기 위하여 키보드를 이용하여 자신의 신상정보를 입력하고 “동의”란에 마우스를 클릭하는 시스템은, 휴대전화를 갖다대면 자동으로 결제되는 시스템 또는 RFID가 부착된 의류를 구입함과 동시에 정보가 입력되는 이른바 유비쿼터스 시스템과는 기본적으로 다르다. 예컨대, A라는 사람이 자동자 운전 중 톨게이트를 지나며 행한 요금결제로 인한 무의식적인 위치정보 및 소비정보의 등록과 단순히 웹사이트에서의 결제를 위해 “동의”란에 클릭하는 의식적인 행위는 커다란 차이를 나타낼 수 밖에 없다. 이것은 이미 사회현상으로 나타나기 시작하였으나, 이에 대한 아무런 대책이 없는 것도 현실이다. 예를 들면, 최근에 급속히 사회적 이슈로 대두되고 있는 RFID 활용서비스를 현행의 법률에 적용하기에는 매우 곤란하다. 현행법은 RFID 활용에 대한 아무런 규제조항을 마련하고 있지 않기 때문이다. 그렇다고 무조건 이것의 사용을 금지하는 법률을 규정하면 유비쿼터스 환경의 실현 및 정보통신산업의 발전에 치명적인 걸림돌이 될 뿐이다.

연합 회원국에 대하여 동 지침의 내용에 근거하여 개인정보보호법률을 제정 또는 개정하도록 강제하였다.

마. 정보주체에 대한 고지의 어려움

정보수집자가 개인정보를 수집하는 때에는 그 수집에 대하여 해당 정보주체로부터 동의를 얻어야 할 뿐 아니라, 자신의 연락처, 정보수집의 목적, 누구에게 개인정보를 제공할 것인지 등에 대한 고지 또는 통지가 이루어져야 한다. 이것은 개인의 자기정보통제권을 실현하기 위한 가장 기본적인 개인정보보호 원칙이다.[9)]

그러나 유비쿼터스 환경의 시스템은 정보주체에게 정보 이용에 대한 고지 절차를 거치지 않게 되는 경우가 많다. 유비쿼터스 컴퓨팅의 특성은 개인과 개인, 개인과 사물, 사물과 사물을 직접 연결하여 줌으로써 공간－사물－사람－정보(web presence)의 기능적 일체화가 이루어진다는 것에 있고, 이는 네트워크를 기반으로 하여 어떠한 장치에서도 접근이 가능한 분산환경의 구축을 의미한다. 이러한 환경에서 정보주체에게 정보의 흐름을 일일이 고지하는 것 자체가 매우 어렵고 불필요한 것으로 여겨질 수 있다. 즉, 정보주체의 단독적 행위, 또는 로 거래행위가 완성되는 경우가 많기 때문에, 정보주체가 상대방으로부터 고지를 받는 아무런 절차가 존재하지 않는다. 예를 들면, 어떤 사람이 휴대전화의 결제기능을 이용하여 자동판매기의 음료수를 구매하는 경우에, 자동판매기에 특정한 고지가 되어 있지 않은 한, 그는 자동판매기를 설치한 회사로부터 자신의 정보제공에 따른 타당한 고지를 받지 못한다. 또한 텔레메틱스 서비스[10)]의 경우에도 통신, 도로, 방송 등의 인프라와 통신사업

---

9) 정보통신망이용촉진및정보보호등에관한법률 제22조 (개인정보의 수집)
②정보통신서비스제공자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 각호의 사항을 이용자에게 고지하거나 정보통신서비스이용약관에 명시하여야 한다.
1. 개인정보관리책임자의 성명・소속부서・직위 및 전화번호 기타 연락처
2. 개인정보의 수집목적 및 이용목적
3. 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용
4. 제30조제1항・제2항 및 제31조제2항의 규정에 의한 이용자 및 법정대리인의 권리 및 그 행사방법
5. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치・운영 및 그 거부에 관한 사항
6. 그 밖에 개인정보 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항

10) 텔레메틱스는 Telecommunication와 Informatics의 합성어로 위치정보와 무선통신망을

자, 자동차업체, 전자기기업체, 보험회사 등 사업자주체 간 상호연계 관계가 분산되어 있어, 정보주체의 정보유통에 대한 체계적 규제수단이 존재하지 않는 한 정보주체가 자신의 정보이동에 대한 사항을 고지받기는 쉬운 일이 아니다.

더구나 분산형 네트워크가 특징인 유비쿼터스 환경에서는 개인과 개인간의 정보유통 또한 자유롭게 이루어질 수 있으므로, 사업자와 개인간의 정보유통보다도 더욱 정보수집에 대한 고지가 어렵게 된다.

3. 유비쿼터스 환경에서의 개인정보보호법제의 당면 과제

가. 개인정보보호법제의 정비방향

나. 기존 법제의 정비

유비쿼터스 환경의 급속한 발전은 현행의 법률과 정책 등으로는 감당할 수 없는 문제들을 제기하고 있다. 유비쿼터스 컴퓨팅의 발전은 전술한 바와 같이 다양한 종류의 컴퓨터가 사람, 사물, 환경 속으로 내재화되고 이들이 지능화됨과 동시에 네트워크로 연결되어 인간을 도와주는 신개념 환경을 의미한다. 현행의 개인정보보호 법제는 퍼스널 컴퓨터가 주로 사용되면서 유선인터넷이 주된 통신수단으로 사용되는 세대에 통용되는 법제라 할 수 있다. 그러나 네트워크의 본질적 변화와 다양한 통신기기의 발전, 그리고 이를 기반으로 한 새로운 정보통신산업 및 서비스(u-Commerce 등)의 등장은 다양하고 새로운 개인정보침해 유형을 현행의 법제에 적용하기 어렵게 만들었다.

유비쿼터스 환경에 있어 개인정보보호를 위한 법정책적 대안은 기본적으로 통상적인 개인정보보호를 위한 기존의 법제도를 새로운 유비쿼터스 환경에 적용할 수 있도록 개혁하는 데에서 출발하여야 한다. 이를 위해서는 기존의 법제의 개선 등을 모색하면서, 이러한 법정책적 대안들이 유비쿼터스 환경에서의 개인정보침해 문제를 충분히 해결할 수 있는지, 아니면 유비쿼터스 환경에 타당한 새로운 입법을 추

이용하여 운전자와 탑승자에게 교통안내, 긴급구난, 원격차량진단, 인터넷(금융, 뉴스, 이메일, 메신저 등) Mobile Office 환경을 제공하는 서비스를 말한다.

구할 필요가 있는지를 검토할 필요가 있다.[11]

우선, 유비쿼터스 환경에 타당한 입법모델을 정립하는 방안을 고려해 볼 수 있으나, 이 방안을 채택하기에는 아직은 다소 무리가 있어 보인다. 그 이유는 유비쿼터스 컴퓨팅 기술이나 사회의 변화에 대한 전반적 문제점들을 예측할 수 있으나, 실제로 아직은 차세대 정보통신 환경에서의 기술개발이 어떻게 진화해갈지, 이로 인한 정보침해의 유형이 어떠할지에 대한 예측이 명확하지 못한 것 또한 사실이기 때문이다. 결국, 어떠한 사회현상에 대한 단순한 유추나 가정만으로 법적 규제를 마련한다는 것은 자칫하면 지나친 규제가 수반되어 위헌적 요소를 배제할 수 없다는 사실을 충분히 고려하여야 한다.

그렇다면, 지금의 시점에서는 현존의 법제도를 개선·보완함으로써 유비쿼터스 환경에서의 개인정보 보호가 충분히 이루어질 수 있도록 하는 방안을 고려하는 것이 차선책이 될 수 있을 것이다. 즉, 중장기적으로는 유비쿼터스 환경을 모두 포괄할 수 있는 보편적 입법모델을 모색해 가면서, 단기적으로 필요한 분야에서부터 가이드라인·지침·기준 등을 수립하는 방안을 고려할 수 있다.

다. 유비쿼터스 환경에의 개인정보보호원칙 적용 방안 마련

"현재의 개인정보보호 원칙을 유비쿼터스 환경에 적용할 수 없는 것인가?"라는 질문에 대한 답을 얻기 위해서는, 먼저 "프라이버시와 관련된 분야에 있어서, 일반적 컴퓨터 공학과 유비쿼터스 컴퓨팅 간의 차이점은 무엇인가?"에 대한 답이 선행되어야 할 것이다.

유비쿼터스 컴퓨팅은 언제, 어디에서나 존재한다. 뿐만 아니라, 유비쿼터스 컴퓨팅은 우리가 느끼지 못하는 사이에 이루어진다. 이는 타인에 의한 감시에 하에 있으면서도 유비쿼터스 컴퓨팅과 통신장치와의 상호작용이 언제 이루어지는지 인식하기 더욱 어려워짐을 의미한다. 그리고 센서의 식재 및 탑재 기술과 적용 능력은 더욱 증가할 것이며, 이러한 컴퓨터 기술은 단순히 온도나 빛의 밝기를 측정하는

11) 홍준형, 유비쿼터스환경에서의 개인정보보호－법정책적고찰－, 한국공법학회 제117회 국제학술발표회 발표논문, 2004, 6., 53면.

수준을 넘어서 단추크기보다 작은 카메라와 소형전화기 등으로 뛰어난 질의 소리와 화면을 제공할 것이다. 또한 센서 기술과 더불어 우리생활의 모든 언동을 기억할 수 있는 방대한 메모리 저장능력이 향상될 것이다.

이와 같은 이유로, 유비쿼터스 환경에서는 기존의 정보환경과는 달리, 정보주체로부터 동의를 획득하거나 정보주체에게 특정사항을 고지한다는 것은 거의 불가능해질 수 있으며, 어쩌면 이러한 절차가 불필요한 것일 수도 있다. 이러한 면에서 동의와 고지수단이 불가능한 사회에서 개인의 자기정보통제권은 어떻게 보장되어야 할 것인가라는 풀기 어려운 문제가 제기된다.

정보처리자가 개인정보수집시 정보주체에게 동의를 획득하고, 정보의 수집목적 등 일정한 사항을 고지하는 절차는 개인의 자기정보통제권을 보호하기 위한 최소한의 원칙이다. 유비쿼터스 환경이라는 새로운 정보통신사회에서도 이 원칙은 고수되어야 하며, 이것이 지켜지지 못한다면, 유비쿼터스 환경에서 얻는 문명의 이익보다 회복 불가능한 기본권 침해라는 손실이 더욱 클 수 밖에 없다. 따라서, 기존의 개인정보보호 원칙은 유비쿼터스 환경에서도 유지되어야 한다.

그러나 개인정보보호 원칙의 일방적 강제는 유비쿼터스 컴퓨팅의 발전을 저해하는 요인으로 작용할 수 있다. 따라서 유비쿼터스 컴퓨팅 특성에 타당한 별도의 동의획득 및 고지절차를 마련하여 개인정보를 보호하는 방안의 모색을 고려하여야 한다. 예컨대, 특정 분야에서의 기술적 요소 및 정보의 수집·사용 유형 등을 고려하여, 이 분야에서 정보보호 일반원칙을 적용할 수 있는 가이드라인 또는 지침 등을 제시함으로써 할 수 있을 것이다.[12] 이러한 조치를 통하여, RFID 기술 등 유비쿼터스 컴퓨팅 기술이 특별한 충격없이 사회에 원활히 수용될 수 있도록 하고, 프라이버시의 문제를 해소할 수 있을 것이다.

아직 세계적으로 유비쿼터스 환경에 대비한 보편적 법모델은 제시되고 있지 않

12) 홍준형 교수는, RFID 기술처럼 한창 발전도상에 있는 기술과 서비스에 관한 법모델을 모색함에 있어서는, 국제동향이나 주요 선진국들의 입법례들을 예의 주시하면서 일단은 지침이나 권고 등을 통한 일종의 연성법적 접근(soft law approach)을 시도해 볼 필요가 있다고 한다(홍준형, 전게논문, 60면).

다. 한편, 일부 국가에서는 최근 커다란 사회적 이슈로 떠오르고 있는 RFID 서비스와 관련한 가이드라인 또는 법안을 제시함으로써, 장래의 정보통신환경에서 발생할 수 있는 개인정보침해에 대한 대비책에 대한 관심을 기울이고 있다. 그 예로서, 미국, 유럽 및 일본 등 일부 국가에서는 RFID 및 텔레메틱스 서비스와 관련한 법안 및 가이드라인 등을 제시하고 있다.[13] 미국의 소비자감시단체인 CASPIAN 등 각국의 시민단체에서도 RFID의 사용제한을 주장함으로써 유비쿼터스 사회에서의 프라이버시 및 개인정보 보호 중요성의 인식을 새롭게 하고 있다.[14]

정보통신기술이 아무리 발전하더라도 개인의 자기정보통제권을 보호하기 위한 개인정보보호의 보편적 원칙이 변화할 수는 없는 것이다. 정보수집 및 사용에 대한 고지, 동의 및 공정의 원칙은 준수되어야 하며, 기술의 발전에 따른 정보주체의 권

---

13) 미국의 시민단체인 '수퍼마켓의 프라이버시 침해에 대한 소비자 단체'(CASPIAN)은 2003년 6월 11일 '2003년RFID알권리법안'을 제안하였고, 동년 8월에는 캘리포니아주 의원 등에 RFID의 프라이버시 침해 위협 가능성 및 이슈에 대한 설명회를 개최하였다. 캘리포니아주 상원의원 데브라 보웬(Debra Bowen)은 2004년 2월 20일 RFID 상용화와 관련한 소비자 사생활보호 등을 주장한 법안 SB 1834를 제안하였다. 이후 법안은 4월 1일, 6월14일 두차례 수정되어 주상원에 계류중이다. 유타주에서도 하원의원 호이그(Hogue)의 제안 하에 'RFID알권리법안'이 하원의회를 통과하였다. 일본은 경제산업성이 주도하여 2003년 12월 22일에 "RFID 기술에 관한 프라이버시 보호 가이드라인(안)"을 정리하였고, 2004년 1월 21일에 이를 발표한 바 있다(이에 관한 자세한 내용은, 조규범, RFID의 발전에 따른 정보 프라이버시 보호에 관한 법적 연구, 기술보고서, 한국정보보호진흥원, 2004, 6. 참조)

14) 의류업체인 베네통(Benetton)은 자사의 제품에 RFID를 부착하여 고객의 소비정보를 수집하기로 하였으나 심각한 개인정보 침해의 우려가 있다는 이유로 CASPIAN(수퍼마켓의 프라이버시보호소비자단체) 등의 강력한 반대에 부딪쳐 그 부착을 유보한 바 있다. 또한 질레트(Gillette)는 제품의 도난방지 및 실시간 재고관리를 위해 월마트(Wall-Mart)에서 시험운영하고자 하였으나 이 역시 프라이버시 침해의 강한 우려를 표명한 소비자단체들의 반대로 중단되었다. 미셸린(Michellin)은 타이어에 고유식별 번호를 저장한 RFID를 삽입하여 추적장치 시험운영을 시도하였으나, 위치추적의 우려로 인해 문제점이 지적되고 있다. 또한 유럽중앙은행은 지폐위조방지, 거래정보의 저장 등을 위해 유로화지폐에 RFID를 삽입하려는 계획을 가지고 있으나, 현금거래의 익명성 저해 우려 등 소비자 단체의 지적을 받고 있다.

리확보 방안을 위한 지침 및 가이드라인을 마련하여 기술의 발전과 정보보호의 조화를 모색하여야 한다. 결국은 유비쿼터스 환경의 어떠한 분야에 있어서도, 정보주체의 권리 행사는 어떠한 방식으로 이루어질 것인지, 그리고 유비쿼터스 환경을 지향한 사업자들의 활동에 어떠한 법적 권리와 의무를 부과할 것인지의 여부 등에 대한 기초적 연구분석이 선행되어야 할 것이다. 이렇게 마련된 지침 또는 가이드라인은 유비쿼터스 환경에서의 보편적 입법을 제정하는데 기초자료로서의 역할을 할 수 있다.

라. 정보유통과 개인정보보호와의 조화 모색

유비쿼터스 환경에서는 홈네트워크의 보편화, 24시간 맞춤형 행정서비스제공, 교육・보건・환경・교통 등 사회인프라의 지능화, 소외계층의 사회활동 참여확대 등을 통하여 헤아릴 수 없을만큼 편리하고, 안전하고, 윤택한 삶을 누릴 수 있게 된다. 반면에 개인정보침해의 위험성은 현저히 증대한다. 이러한 유비쿼터스 환경의 동전의 양면과 같은 상충관계의 한계를 현명하게 극복하기 위한 방안을 모색하는 것이 무엇보다도 중요하다.

개인정보의 보호라는 요청과 공익의 이익 또는 영업의 자유 등 기타의 기본권과 조화를 이루는 원칙들은, 전술한 바와 같이 유비쿼터스 환경의 특수성을 고려한 법적 규제의 방법이나 정도에 대한 기준을 마련함으로써 정립될 수 있을 것이다.

마. 기술중립적 입법의 준비

유비쿼터스 환경에 대비한 입법에서 가장 중요한 것은 새롭게 등장하는 예측 가능한 통신기술의 발전을 수용하고 이를 적용할 수 있는 기술중립적 입법 모델을 마련하는 것이다. 이는 유비쿼터스 네트워크의 이용자에게 동일한 수준의 개인정보 및 프라이버시 보호를 보장할 수 있도록 정보통신 서비스 시장과 기술의 발전사항을 반영하는 것이어야 한다. 새로운 기술이 등장할 때마다, 새로운 유형의 개인정보침해 문제가 제기될 때마다 법제도를 제・개정하는 것만으로 유비쿼터스 컴퓨팅 환경에서의 개인정보보호가 충분히 이루어질 수는 없다. 따라서 중장기적인 계획을 통해 유비쿼터스 환경에 적합한 보편적 모델을 제시할 수 있어야 한다. 그래야만

유비쿼터스 네트워크에서 발생하는 개인정보 처리에 관한 모든 사항에 대하여 통일적고 체계적으로 적용할 수 있는 법제가 완비될 수 있다고 생각된다.

4. 사업자의 자율규제 강화

이미 전세계의 많은 기업들이 유비쿼터스 컴퓨팅을 이용한 새로운 정보통신산업을 개발하고 있다. 유비쿼터스 네트워크를 활용한 상황인식 마케팅 산업 등 U-commerce를 필두로 하여, 전자인식카드(RFID Tag)·스마트카드 설계 및 식재 산업, 센서산업, 광역계측사업 등 지금의 정보통신 산업과는 차원을 달리하는 산업이 양산될 것으로 전망된다. 이러한 산업들은 한편으로 불가피하게 많은 개인정보를 요구하게 된다.

이러한 U-Commerce 환경 하에서는 개인정보에 관한 사업자의 인식변화와 개인정보 보호를 최우선으로 배려하고 있다는 안전성과 신뢰성이 최우선적으로 고려되어야 한다. 이에 따라 사업자들은 유비쿼터스 환경에 적합한 스스로의 개인정보보호 정책의 수립이 필요하다. MicroSoft사 등 외국 기업의 경우에는 이미 개인정보 보호가 자사에 대한 고객의 신뢰성 구축과 고객만족도 향상을 위한 최선의 마케팅기법임을 인식하고 이 분야에서 스스로 많은 노력을 기울이고 있다. 마이크로소프트,[15] IBM, AT&T 같은 Foutune지 선정 500대 기업에도 CPO(Chief Privacy Office, 개인정보담당이사)라는 직함이 생겼다. CPO는 고객관리와 관련하여 도덕적·윤리적·마케팅 측면의 딜레마를 힘겹게 조정하는 중책을 맡는다. 그는 개인정보관리와 고객보호에 대한 사내 정책담당관으로서 회사의 기준을 설정하고 이 기준을 전 조직이 수행할 수 있도록 한다.

유비쿼터스 환경에서도 이용자로부터의 신뢰는 중요하다. 이용자의 정보를 어떻게 수집하여 어떠한 목적으로 사용할 것인지 이용자가 쉽게 이해할 수 있도록 제시

15) 2004년 6월 Micro Soft사의 Peter Cullen(개인정보호정책담당관)이 한국에 방문하여, MS사의 개인정보보호 정책, 프라이버시보호시스템구축, 프라이버시보안 등에 관한 세미나를 개최하여 자신의 회사에 정보보호에 허점이 없음을 강조한 바 있다(Asia Trustworthy Computing Council, MicroSoft, 2004. 6).

하여야 한다. 정보를 제3자와 공유하는 경우에는 먼저 해당 정보주체의 동의를 얻어야 한다. 그리고 그가 원하지 않는 경우에는 쉽게 탈퇴할 수 있어야 한다. 가까운 미래의 정보통신환경에서 기업은 기술과 윤리적 딜레마에서 항상 한발 앞선 위치를 보여주어야 한다.

사업자 자율규제의 한 방법으로, 각 업종별 사업자들이 대표단체 등을 통해서 업종별 "표준 개인정보보호 정책"을 마련하여 사업자간에 자율적으로 강제하는 방안을 모색할 수 있을 것이다. 또한 정보보호를 위한 표준을 만들어 이에 자발적 준수를 유도하는 방안도 있을 것이다.

5. 개인정보보호 기술의 강화

유비쿼터스 컴퓨팅 환경 하에서의 보안 문제는 더욱 절실하다. 어디에서나 컴퓨팅을 이용한다는 것은 곧 어디에서든지 정보가 누출되고 왜곡될 위험이 있다는 것을 의미한다. 무엇보다도 개인정보 침해의 위험성이 더욱 커졌음을 항상 인식하고 있어야 한다. 따라서 어디에서든지 안심하고 사용할 수 있도록 보장해 주는 개인정보 보호기술이 필요하다.

유비쿼터스 컴퓨팅에서의 정보보안의 취약성을 극복하기 위해서는 기밀성, 인증, 무결성이 요구된다. (1) 기밀성(Confidentiality)은 전달 내용을 제3자가 획득하지 못하도록 하는 것으로 암호화 기술로 해결 가능하게 한다(도청자가 비밀번호 등을 알아내더라도 이를 암호화하여 풀지 못하도록 하는 것), (2) 인증(Authentication)은 정보를 보내는 사람의 신원을 확인하는 것이다. 즉 사용자가 어떤 사용 권리를 가지고 있는 사람인지를 확인하는 것이다. 예컨대, 어떤 고객이 신용카드 번호를 보내왔을 때 그 고객이 신용카드의 실제 소유자인지 확인하는 것이다. 인증 수단으로는 센서, 생체정보, 행동특징 등을 들 수 있다. (3) 무결성(Integrity)은 정보전달 도중에 정보가 훼손되지 않았는지 확인하는 것으로 이 역시 암호화 기술로 해결이 가능하다.

이같은 3요소를 바탕으로 하여, RFID・센서 등 새로운 정보기기의 안전성 및 기술개발이 필요하다. 또한 Digital ID, Digital Right, Digital Evidence 등의 차세대 인증에 대비한 인프라 구축과 이에 대비한 관리체계가 확립되어야 한다. 필요하다면 유

비쿼터스 컴퓨팅과 관련한 시스템 구축에 대한 프라이버시 영향평가를 실시하는 것도 개인정보침해를 예방할 수 있는 방안으로 들 수 있다.

6. 결 론

언제 어디서나 컴퓨팅이 가능하다는 유비쿼터스 시대의 도래는, 정보통신 환경의 "제3의 물결" 또는 "유비쿼터스 혁명"으로 지칭될 만큼 이 사회의 모든 영역에서 지대한 영향을 미칠 것이다. 세계 각국의 "스마트 먼지", "사라지는 컴퓨팅", 그리고 "smart its" 등 유비쿼터스 센서에 대한 연구 프로젝트는 본격적인 유비쿼터스 시대의 정착이 멀지 않았다는 예측을 가능하게 한다. 그러나 유비쿼터스 컴퓨팅 환경에서는 "드러난 컴퓨팅에 의해 한정된 공간에서 일정한 명령행위에 의해 개인 행적을 어느 정도 분산·디지털화하는" 기존의 정보화 환경과는 달리, 숨겨진 컴퓨팅에 의해 일정한 명령행위 없이 언제 어디서나 개인의 행적을 집약적·전자적 기록으로 남기기 되며, 전자적인 측면에서는 일정한 목적 범위 내에서 개인을 완전히 발가벗긴다는 점에서 개인 프라이버시의 한계와 그 보호가 핵심과제로 대두된다.

이렇게 기본적으로 보안에 취약할 수 밖에 없는 유비쿼터스 컴퓨팅 환경에서의 개인정보 침해 문제는 이미 사회현상으로 나타나기 시작하였다. RFID 등의 상용화로 인한 개인정보침해의 우려가 그 좋은 예이다. 이러한 새로운 유형의 개인정보 관련 이슈는 현행의 개인정보보호 정책 또는 관련 법령 등으로는 해결하기 곤란한 과제로 남게 되고, 정보주체의 자기정보통제권을 보장하기 어렵다. 그러나 아직 우리나라는 유비쿼터스 환경에 대비한 법률이나 지침 등은 마련되고 있지 않은 실정이다. 지난 해 교육행정보시스템(NEIS) 사태는 국가 IT산업 발전의 성패를 좌우하는 핵심요인이 바로 개인정보 보호에 있다는 사실을 일깨워 주었다. IT 산업발전의 초석이 될 유비쿼터스 환경 구축과 관련하여 프라이버시 문제를 소홀하게 된다면 NEIS, 전자주민카드 도입 실패 등의 전철을 밟게 될 것이다.

이제 신중하게 유비쿼터스 환경에 적합한 프라이버시보호 가이드라인 또는 지침 등 기준을 마련하고, 장기적 측면에서의 "유비쿼터스 프라이버시보호법"의 입법준비 등 정보통신사회 패러다임의 변화에 능동적·효율적으로 대처하여야 할 때이다.

이를 통해서 유비쿼터스 사회의 본격적 확산을 위한 초석을 마련할 수 있을 것이다.

제 3 절 전자감시사회에 대한 국내외 입법례 및 관련 사례의 고찰

1. 전자감시사회의 도래

모든 정보가 빈틈없는 네트워크를 타고 공유되는 유비쿼터스의 시대에서는 개인이 집에 있거나 거리를 활보하거나 자동차를 타고 질주하거나 간에, 우리의 모든 일상이 기록되고 감시되고 분석될 수 있다. 예를 들어 외부로부터의 침입을 감시하기 위해 설치해 둔 무선카메라는 오히려 집 주인의 일거수일투족을 관찰하는 '감시의 눈'이 될 수 있다. 또한 얼굴과 음성을 인식하는 소프트웨어, 무선전화위치 감응기, 스마트 차량 등과 같은 첨단적 감시장비의 등장으로 모든 사람의 위치에 관한 정보는 전적으로 그리고 거의 실시간으로 수집되어 제공될 것이다. 직장에서는 근로자의 행동거지가 카메라에 의해 낱낱이 관찰될 수 있고, 컴퓨터 사용을 포함한 모든 것들이 상세한 모니터링의 대상이 될 것이다. 그리고 수집된 개개의 정보들은 단일한 데이터베이스에 통합되어 구축될 수 있고, 분산된 개별 데이터도 컴퓨터매칭과 같은 기법에 의해 상호 참조됨으로써 필요한 개인별 파일로 추출될 수 있게 될 것이다.

어쩌면 우리의 실제 생활에서 이와 같은 우려는 이미 현재화되고 있는지도 모른다. 가령 CCTV의 경우를 보면, 광학기술의 발전으로 카메라의 렌즈와 부품이 극소화되면서 그 존재의 인식이 거의 불가능해진 정도가 된 반면, 그 촬영의 범위는 크게 확대되었고 촬영된 기록을 저장하거나 전송하는 기능은 크게 향상되었다. 카메라가 360도 또는 540도까지 회전하거나 아래위로 움직일 수 있게 된 것은 물론이고, 거리의 조절도 가능하여 100여 미터 떨어진 곳의 자동차번호판도 줌인(zoom in)을 하면 뚜렷하게 볼 수 있을 정도의 정밀성을 갖췄다. 이 경우 마음만 먹으면 골목길의 행인뿐 아니라 커튼이 열린 창가나 아파트 베란다를 엿볼 수도 있다. 도로에 접한 공원에 모이는 사람들의 행색과 누가 누구를 만나는지도 확인할 수 있는 성능이다. 또한 종래 VCR에 테이프로 녹화하던 방식에서 디지털영상저장장치(DVR)로 전

환되면서 모니터를 CCTV 수만큼 분할해서 볼 수 있고, 카메라와 모니터간에 전용 통신링크가 내장되어 있어 카메라에 담긴 영상이 모니터에 실시간으로 전송될 수 있게 되었다. 더욱이 CCTV의 가격이 떨어지고 안전에 대한 현대인의 욕구는 커져 수요는 계속 늘고 있다.

미국 MIT대의 공학전문지 [Technology Review] 2003년 4월호의 보도에 의하면, 전 세계에 설치된 감시카메라는 2,600만대이며, 미국에만 1,100만대에 이른다고 한다. 뉴욕의 시민단체 '미국시민자유연합(ACLU)'은 1999년 뉴욕 맨해튼 지역의 감시카메라를 2,397대로 집계했지만, 9·11 테러가 발생한 이후 최근까지 3배(7,200대)나 증가한 것으로 추산하였다. 영국에서는 이미 아일랜드공화군(IRA)의 도심테러에 부심하던 1980년대 집중적으로 감시카메라가 설치돼 현재 150만대가 전국 곳곳에 숨어있는 것으로 추정되고 있다. 15만대의 감시카메라가 설치된 런던에서 시민들은 하루 평균 5분에 한번씩, 하루 300번 정도 감시카메라에 노출된다는 보고서도 나와 있다.[16)]

국내에도 서울과 부산, 인천 등 6개 광역시 경찰청이 운영하는 1,178대, 서울의 종로, 관악, 강남구청이 운영하는 107대의 CCTV가 있다고 한다. 대당 가격이 1,500만원에 이르는 강남구의 CCTV는 360도 회전이 가능하며, 12배 이상의 줌인 기능을 갖추고 있어 500 미터 앞까지 볼 수 있는 고성능의 장비로 알려지고 있다. 최근에도 강남구청은 구 전역에 방범 CCTV 300여대를 추가로 설치할 예정으로 있다. 공공기관이 설치한 감시카메라는 극히 일부이고, 가령 기업빌딩과 학교, 지하철, 찜질방, 편의점, 술집, 주택 등에 설치되어 운용되고 있는 민간부문의 감시카메라까지 감안하면 전체적으로 수십만 대에 이를 것으로 추산된다.[17)]

이러한 전자적 감시의 상황을 두고 Roger Clarke는 "데이터감시(dataveillance)"라고 명명한 적이 있다.[18)] 그리고 Paul Schwartz는 인터넷을 통한 사이버감시가 조지오

16) 국민일보 2004. 5. 10.

17) 동아일보 2004. 2. 19.

18) Roger Clarke, "Information Technology and Dataveillance," Version of November 1987, at. 3, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

웰의 telescreen보다 오히려 더 교묘하다고 하면서, 오늘날에는 공공부문과 민간부문에서 개인적 자료를 수집하는 다수의 “Big and Little Brothers”가 존재한다고 하였다.[19)]

2. 전자감시에 의한 기본권의 침해

가. 전자감시와 기본권침해

전자감시사회에서 개인이 자신의 일거수일투족이 감시되고 있다는 사실을 의식한다든가 혹은 감시될지도 모른다고 걱정하게 될 경우나 자신의 행동에 상당한 제약을 받게 될 수밖에 없을 것이다. Reg Whitaker도 『프라이버시의 종말(The End of Privacy)』이란 책에서 감시카메라의 설치는 지역주민들의 일상적인 생활은 물론이고 정치적인 반대자나 파업에 참가하는 노조원들의 활동까지 위축시키는 효과를 유발할 수 있음을 지적하고 있다.[20)]

또한 개인이 종종 그 흐름을 통제할 권리를 가지지 못함으로 말미암아 개인정보 수집의 결과로서 상당한 문제점들이 발생할 수 있다. 때때로 개인이 통제할 수 없어서 유포된 정보를 바로잡을 수 없기 때문에 그 정보는 자칫 그릇된 정보가 될 가능성도 있다. 나아가 왜곡되지 아니한 개인정보도 고도로 민감하고 사적인 성질을 가진 것이어서 잠재적으로 해악을 미치고 부주의하게 유포될 경우 난처한 것이 된다. 뿐만 아니라 자신에 관한 정보임에도 그 처리의 상황이나 내용에 대해 전혀 인식을 할 수 없거나 그 처리과정에 관여 내지 통제할 가능성이 전면 차단되어 있다면, 그 개인이 겪게 되는 심리적 무기력증과 자신의 정보에 대한 소외감은 막대할 것이다. 이렇게 될 경우 개인의 자유로운 인격의 발현이나 사생활의 형성은 기대하기 어렵게 될 것이고, 결국 개인은 정보의 주체가 아니라 ‘단순한 정보객체’(bloß Informationsobjekt)로 전락하게 되고 말 것이다.

다른 한편으로, 사이버스페이스에서 개인에 대해 형성되는 가상의 인격이 실존의

---

19) Paul M. Schwartz, “Privacy and Democracy in Cyberspace,” 52 *Vand. L. Rev.* 1609, (1999), p.1657, Fn. 294.

20) 렉 휘태커/이명균・노명현 역, 『개인의 죽음』, 생각의 나무, 2001, 151면 이하 참조.

인격을 규정짓게 될 경우 개인의 사회적 정체성은 디지털화된 개인정보에 의해 좌우되는 상황이 초래될 것이다. 이렇게 되면 가령 잘못된 개인정보에 의하여 개인의 사회적 정체성이 왜곡되는 경우 그 개인이 입게 되는 피해는 예측할 수 없을 정도로 그 파장이 클 수밖에 없다. 범죄자로 오인되어 체포된다거나 신용거래불량자명단에 이름이 잘못 기록된다거나 하는 경우 신체의 자유의 침해나 경제생활상의 피해는 말할 것도 없고 고용에 있어서의 차별, 복지수혜의 기회상실, 공동체생활에 있어서 명예의 손상 등 그 피해는 실로 막대하다 할 것이다.[21]

나. 침해되는 기본권

이처럼 오늘날 전자적 감시는 단순한 명예훼손이나 재산적 피해와 같은 법률상의 이익을 침해를 가져오는 정도에 그치지 아니하고, 인격권 내지 프라이버시권, 초상권, 재산권, 교육권, 사회보장수급권 등과 같은 기본권의 침해로까지 이어진다고 할 수 있다. 따라서 오늘날 전자감시에 의한 개인정보의 대량적 수집과 보유 및 용이한 결합을 적절하게 억제함으로써 막강한 정보권력의 남용에 따른 개인의 비인격화 내지 소외화를 막아야 한다는 데 그 어떤 이견도 있을 수 없다. 그리고 그러한 과제는 오늘날 대다수의 국가에서 기본적 인권의 보장이라는 관점에서 파악되고 있다.

이하에서는 전자감시로 인하여 침해될 수 있는 기본권 가운데, 특히 자기정보통제권과 초상권을 중심으로 그 의의와 근거, 내용, 제한 등에 대해 간단히 살펴본다.

다. 자기정보통제권

사생활정보는 개인의 인격의 외부적 측면에 포함되는 것이라 할 수 있다. 개인에 관한 정보의 공개는 사회가 개인을 어떻게 바라보는지에 직접적으로 영향을 미치며, 사회에서 개인이 역할을 수행하는 데 영향을 미칠 수 있다. 그것은 개인의 사회적 정체성(social identity)을 형성하며, 그 결과 개인의 현실적 정체성(actual identity)에 영향을 미치게 된다. 왜냐하면 사회 및 사회에서의 개인적 역할은 모두 정체성을 형성하기 때문이다. 따라서 비록 인격의 외부적 측면이 개인정보에 포섭된다 하더라도 내적인 요소 역시 개인정보에 대해 강력한 연관성을 가진다. 그러한 내적

21) 성낙인 외, 개인정보보호를 위한 정책방안 연구, 정보통신부, 1999, 27면 참조.

요소의 보호는 개인정보에서의 프라이버시권을 중요하게 만든다. 정당하지 아니한 부정적인 사회적 비난을 피하기 위해 자신에 대한 정보의 유통을 통제하는 권리는 현실적 정체성을 보호하는데 필수적이다.[22)]

자신에 관한 정보의 생성과 유통, 소멸 등에 주도적으로 관여할 각종의 권리는 우리 헌법상 자기정보통제권이라는 기본권에 의해 통일적으로 파악될 수 있다. 이른바 자기정보통제권은 소극적 측면뿐만 아니라 적극적 측면도 아울러 가지는데, 개인정보의 수집·축적·보관·제공 등을 거부한다든가 혹은 본인의 의사에 반하거나 잘못된 개인정보의 보유나 처리에 대하여 정정이나 폐기 또는 손해배상을 청구한다든가 하는 것은 자기정보통제권의 소극적 측면이라 할 수 있다. 반면에 자신에 관한 정보의 보유상황을 확인하기 위하여 자료의 열람이나 조사를 청구하거나 혹은 원하는 대상에게 그 정보를 스스로 공개하거나 제공한다든가 하는 것은 자기정보통제권의 적극적 측면이라 할 수 있다.

이러한 자기정보통제권은 기본적으로 사생활의 유지와 형성을 자율적으로 결정내지 통제할 수 있는 사생활의 자유에서 나온다고 할 수 있다. 설령 그것이 자신의 인격상의 형성에 이르게 되는 사항이라 하더라도 그 정보의 수집과 보유, 유통에 이르는 과정에 본인이 관여할 수 있는지 여부의 문제도 역시 정보주체에게 있어서 사생활의 유지와 형성에 관한 내용이라 할 수 있기 때문이다. 그리고 자신에 관한 정보가 모두 사적 영역에 속한다고 할 수는 없겠지만, 그러한 정보의 전파에 대해 스스로 통제하는 문제는 사생활의 자유에 포함되는 내용으로 이해될 수 있을 것이다. 다만 주거와 통화에 있어서의 사생활은 주거의 자유(제16조) 및 통신의 자유(제18조)를 통하여 보호를 받게 되며, 가령 양심, 신앙, 사상, 정치적 견해, 교육정보, 신용정보, 고용정보, 신체장애 등에 관한 정보의 보호는 양심의 자유(제19조), 종교의 자유(제20조), 선거권(제24조), 교육권(제31조), 재산권(제23조), 노동권(제32조, 제33조), 사회보장수급권(제34조) 등의 보장으로 나타날 수도 있다. 또한 언론매체에 대한 액세스권이나 행정기관이 보유하는 개인정보의 열람권은 표현의 자유(제21조)와

22) Francis S. Chlapowski, “The Constitutional Protection of Informational Privacy”, 71 *Boston University Law Review* 133 (1991), p.154.

알 권리(제1조, 제10조, 제21조 등)의 내용이 될 수 있다. 이러한 점에서 이들 개별적 기본권도 자기정보통제권과 일정한 관련을 가질 수 있다.

자기정보통제권의 제한은 정보주체의 동의를 얻지 아니하거나 그 동의를 초과하여 공권력이 개인정보의 수집, 축적, 보유, 이용, 제공 등의 조치를 취하는 경우로서 이해되어야 할 것이다. 헌법 제37조 제2항에 의할 때 정보조사 기타 정보처리는 관련자가 명시적으로 목적이 구체화된 정보처리에 동의하지 않는 이상 안전보장, 사회질서유지, 공공복리를 위하여 제정한 법률에 근거하여서만 자기정보통제권에 대한 제한이 이루어질 수 있다. 나아가 비례의 원칙도 준수되어야 하는데, 정보처리의 위험성에 따른 보호의 정도는 당해 개인정보의 성격뿐만 아니라 수집목적, 이용형태, 처리방식 등 구체적인 정보처리의 위험성을 고려하여 개별적으로 검토하는 것이 바람직하다. 일반적으로 개인정보의 수집목적이 광범하고 그 보유기간이 길 경우 자기정보통제권의 침해가능성은 크다고 할 수 있으며, 예정된 취급자나 이용자가 많을수록 그 침해의 위험성은 커진다고 할 수 있다. 또한 수기식의 파일보다는 컴퓨터파일의 형태로 처리되거나 보유되는 경우 그 침해의 위험성이 훨씬 증대된다고 할 수 있으며, 분산되어 보유되는 개인정보가 용이하게 검색될 수 있거나 하나의 데이터베이스로 통합되어 관리될 경우 자기정보통제권의 침해로 이어질 개연성이 아주 크다. 1980년 OECD의 「프라이버시 보호와 개인데이터의 국제적 유통에 관한 가이드라인」에서는 ① 수집제한의 원칙, ② 정확성의 원칙, ③ 목적명확화의 원칙, ④ 이용제한의 원칙, ⑤ 안전확보의 원칙, ⑥ 공개의 원칙, ⑦ 개인관여의 원칙, ⑧ 책임의 원칙 등 8원칙이 제시된 바 있다. 이러한 8원칙은 국제적으로 개인정보보호에 관한 일반원칙으로서 인정받고 있으며, 각국의 개인정보보호법제에 의해 전면적으로 혹은 부분적으로 수용되었다. 그런데 이러한 개인정보보호에 관한 원칙은 기본권보장의 체계에서 볼 때 비례원칙의 구체화 내지 비례원칙의 파생원칙으로 이해될 수 있다.

라. 초상권

초상권은 사람이 자신의 초상에 대하여 갖는 인격적·재산적 이익, 즉 사람이 자기의 얼굴 기타 사회 통념상 특정인임을 식별할 수 있는 신체적 특징에 관하여 함부

로 촬영되어 공표되지 아니하며 광고 등에 영리적으로 이용되지 아니하는 법적 보장이라고 할 수 있다.

우리 헌법상 국가가 보장하여야 할 인간으로서의 존엄과 가치는 생명권, 명예권, 성명권 등을 포괄하는 일반적 인격권을 의미하고, 이 일반적 인격권에는 개별적인 인격권으로서의 초상권이 포함되어 있는 것으로 파악된다.[23] 따라서 이러한 초상권은 초상의 인격적 가치를 보호하는 것을 내용으로 하는 인격권의 일부로서 이해할 수 있다.

따라서 초상권은 현행 헌법상 명문의 규정은 없지만, "모든 국민은 인간으로서의 존엄과 가치를 가지며 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다"고 규정하고 있는 헌법 제10조에서 그 법적 근거를 찾을 수 있다고 본다. 또한 민법 제750조 제1항은 "타인의 신체, 자유 또는 명예를 해하거나 기타 정신상의 고통을 가한 자는 재산 이외의 손해에 대하여도 배상할 책임이 있다"고 규정하고 있는데, 이 규정은 초상권 침해로 인한 손해배상청구의 민사법적 근거로서 이해될 수 있다.

일반적으로 초상권에는 ① 얼굴 기타 사회 통념상 특정인임을 알 수 있는 신체적 특징을 함부로 촬영 또는 작성되지 아니할 권리(촬영・작성 거절권), ② 촬영된 사진 또는 작성된 초상이 함부로 공표·복제되지 아니할 권리(공표거절권), ③ 초상이 함부로 영리목적에 이용되지 아니할 권리(초상영리권)가 포함되는 것으로 이해되고 있다.[24]

초상권의 제한은 일차적으로 본인의 동의를 얻지 않고 은밀하게 혹은 일방적으로 촬영・작성・공표・이용 등의 행위를 할 경우에 발생한다. 이 경우 본인의 동의는 사전에 충분한 설명이 이루어져 있을 것을 전제로 한다. 따라서 동의가 있었다고 하더라도 본인에게 고지된 내용과 다르게 혹은 그 범위를 넘어서서 촬영 기타의 행위가 이루어졌다면 당연히 초상권의 제한이 있다고 해야 할 것이다.

---

23) 김철수, 헌법학개론, 박영사, 2000, 364－365면 참조.

24) 서울민지 1997.8.7. 선고 97가합8022 판결, 손해배상(기) 하집 1997－2, 80.

가령 CCTV의 경우 사람은 무단으로 촬영되는 것을 아는 것만으로도 고통을 느끼는 경우가 있으므로 영상이 공표되지 아니하는 경우라도 초상을 촬영하는 자체만으로도 초상권의 제한에 해당할 수 있다. 또한 길거리나 광장 등 공공장소에 나왔다는 사실만으로 초상권을 포기한 것이라고는 볼 수 없고, 사회통념상 상당한 정도와 방법을 벗어난 촬영은 그들의 초상권을 제한하는 것이라고 해야 한다. 그리고 법적 근거가 있고 공익적 목적을 위해 설치되었다고 하더라도 촬영된 사진을 무한정 저장하거나 이용하는 행위, 당초의 목적과 다른 목적에 다시 사용하는 행위는 모두 초상권을 제한하는 것이 될 수 있다.

그런데 이러한 초상권도 역시 안전보장, 사회질서유지, 공공복리를 위하여 제한이 이루어질 수 있으나, 그 제한에는 형식적 의미의 법률에 근거할 것이 요구됨은 물론이다.

3. 전자감시와 관련된 국내외의 입법례

가. 미국의 경우

미국은 개인의 사생활보호를 위해 1974년 12월 31일에 이미 프라이버시법(The Privacy Act)을 제정하여 공포한 바 있다. 하지만 이것은 공공부문에서만 적용될 뿐이고, 민간부문에서의 사생활보호는 별도의 단행법에 의해 개별적으로 규율되고 있다. 그리고 컴퓨터연결프로그램(computer matching program)에 이용하기 위한 개인정보의 제공을 제한 1988년에 Computer Matching and Privacy Protection Act[25]이 제정되었다.

한편, 1984년의 Cable Communications Policy Act(CCPA)[26]는 케이블사업자들이 가입자의 개인정보를 이용하는 방법을 규제하고 있으며, 1986년의 Electronic Communications Privacy Act(ECPA)[27]는 전자통신의 차단, 이용, 공개, 불법적 접근, 저장된

---

25) Pub. L. No. 100－503.

26) 47 U.S.C § 551(2000). “Protection of subscriber privacy”. http://www4.law.cornell.edu/ uscode/ 47/551.html 참조.

통신내용의 검색 등을 제한하고 있다. 또한 1996년의 Telecommunications Act는 전화회사가 가입자의 정보를 이용하는 방식을 규제하고 있으며, 1998년의 Children's Online Privacy Protection Act(COPPA)[28]는 인터넷상에서 13세 미만의 아동의 개인정보를 수집하는 행위를 규율하고 있다.

하지만 공공장소에서의 전자감시를 규제하는 법률은 존재하지 않는다. 따라서 이 문제는 법원의 판단에 맡겨져 왔다. 그런데 미국의 판례는 대체로 공공장소나 대중에게 공개되어 있는 장소에서 이루어진 촬영에 대하여 프라이버시의 침해로 인정하는 것을 거부해 왔다.

예컨대, 피고가 일상적인 대중의 시선에 노출되어 있는 시내의 가로에서나,[29] "공공장소나 대중에게 노출되어 있는 장소"에서,[30] 혹은 "공개된 장소와 다수의 사람들이 모여 있는 일반 작업장에서"[31] 촬영된 경우에는 프라이버시의 침해가 아니라고 판시한 사례가 있다. 이러한 관점에서는 프라이버시의 침해가 되려면 그 침해의 대상은 일반 대중이 자유롭게 볼 수 없는 어떤 것이어야 한다.[32]

이는 일반적으로 공공연하게 노출되어 있는 사항은 누구나 거기에 대하여 글을 쓰거나 이야기할 수 있듯이, 공공장소나 대중의 시선에 노출되어 있는 장소에서 촬영하거나 비디오로 녹화하는 것도 수정헌법 제1조의 취지상 허용된다는 입장으로 이해된다.

최근 하원에서는 2003년 비디오감시방지법(안)(Video Voyeurism Prevention Act of 2003)을 발의한 바 있다. 이 법안에 의하면, 어떤 개인의 부정적 이미지(improper image)를 포착하기 위하여 의도적으로 그 개인의 프라이버시를 침해하는 행위를 할 경우 벌금 또는 1년 이하의 징역에 처할 수 있도록 되어 있다.[33]

---

27) 18 U.S.C. §§ 2510-2522, 2701-2709, 2711 (2000).

28) 15 U.S.C. §§ 6501-6506 (2000).

29) United States v. Vazquez, 31 F. Supp. 2d 85, 90 (D. Conn. 1998).

30) Jackson v. Playboy Enter., 574 F. Supp. 10, 13 (S.D. Ohio 1983); Fogel v. Forbes, Inc., 500 F. Supp. 1081, 1087 (E.D. Pa. 1980).

31) Cox v. Hatch, 761 P.2d 556, 564 (Utah 1988).

32) Vazquez, 31 F. Supp.2d at 90 (quoting Mark, 618 P.2d at 519).

이 밖에도 미국 보안산업협회(SIA)에서 공공안전을 위한 CCTV와 지역사회경찰 활동 가이드라인(CCTV for Public Safety and Community Policing Guideline)을 제정하여 업계 차원의 자율적 규제에 활용하고 있으나, 법적 구속력을 가지지는 못한다.

한편, 2000년 8월 무선통신과공중안전법(Wireless Communications and Public Safety Act)은 이동전화의 송수신지국의 위치를 알려줄 수 있는 대상을 응급의료, 공공안전, 소방 등의 서비스제공자나 법집행기관, 이용자가 죽음이나 심각한 신체상의 위험이 있는 응급상황에 처한 경우 그 법정대리인이나 직계가족에 한정하고 있다.[34)]

그리고 2001년 7월에 마련된 위치프라이버시보호법(안)(Location Privacy Protection Act)은 법원의 요청이 있거나 집합적 정보나 응급서비스를 위해 사용되는 정보에 해당하는 경우를 제외하고 위치정보의 수집・이용・보유・유포에 있어서 반드시 위치기반서비스제공자가 미리 정보주체에게 고지하여 그의 동의를 얻도록 하는 FCC의 규칙을 제정할 것을 규정하고 있다.[35)]

또한 미국의 의회는 2003년 9월 라커룸, 침실 등 사생활을 침해할 우려가 있는 곳에서 몰래 촬영하는 것을 처벌할 수 있도록 하는 비디오관음증방지법을 제정하였고, 나아가 누드나 속옷을 입은 사람을 비디오나 카메라폰으로 촬영・유포・방송하는 행위에 대해 벌금 및 1년 이하의 징역을 부과하는 규제법안도 2004년 8월까지 마련할 계획이다.[36)]

나. 영국의 경우

(1) 영국에서는 OECD “프라이버시보호와 개인데이터의 국제유통에 관한 가이드라인에 관한 이사회권고”(1980)를 받아들여 1984년에 데이터보호법(Data Protection Act 1984)을 제정하게 되었다. 그러나 이 법률은 이 개정법은 1995

---

33) http://www.theorator.com/bills108/hr2405.html 참조.

34) FCC, *Third Report and Order in the Matter of Communications Assistance for Law Enforcement Act*, CC Docket No. 97－213, ¶¶ 12, 21, 22, Aug. 26, 1999 http://www.fcc.gov/Bureaus/Engineering_Technoloy/Orders/1999/fcc99230.wp.

35) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_billf:s1164is.txt.pdf 참조

36) 전자신문 2004. 6. 8.; 연합인포맥스 2004. 5. 19. 참조.

넌 유럽공동체의 개인정보보호지침(Directive 95/46/EC)을 국내법적으로 구체화하기 위해 1998년 데이터보호법(Data Protection Act 1998)으로 대체되어 2000년 3월 1일부터 부분적으로 시행되고 있다.

1998년에 개정된 데이터보호법에서는 1994년 데이터보호법에서와 달리 대중이 자유롭게 접근할 수 있는 지역에서 행하는 감시의 기록도 보호의 대상이 되는 데이터에 포함시킴으로써(제1조 제1항 제4호; 제68조; 부칙 12) CCTV 시스템의 운영에 대해서도 동법이 적용될 수 있도록 하였다.

1998년 데이터보호법상 경찰이나 지방정부 등 적절한 주체에 의해 공공장소에 설치된 CCTV는 다음의 세 가지 요건을 갖출 경우에 한하여 적법하게 허용될 수 있다.

1) 정당한 근거: “범죄예방과 검거”와 “공중의 안전” 등 “공공의 이익”에 부합하는 경우여야 한다.
2) 정보감독관에의 통지: 모든 자동화된 디지털 녹화장치의 공공장소 설치 및 이용은 정보감독관에게 통지하여 등록되어야 한다.
3) CCTV 설치 사실의 표시: 공공장소 설치 CCTV는 반드시 해당지역 진입 전, 혹은 진입하면서 그 사실을 알 수 있도록 표시하여야 한다. 이러한 표시에는 설치 및 관리책임자, 설치 목적, 연락처가 기재되어 있어야 한다.

(2) 데이터보호법 제51조 제3항 제2호에 근거하여 정보감독관은 2000년 7월 CCTV 사용자들의 적절한 이행을 돕기 위하여 시행기준(Code of practice)을 발표하였다. 정보감독관은 이 시행기준에 근거하여 데이터관리자의 동법위반 여부를 판단하여 시정명령을 내릴 수 있으며, 시정이 있을 때까지 데이터사용자의 정보처리를 금지시킬 수 있다.

이 시행기준에서는 CCTV의 설치 및 사용 이전에 기기사용의 목적을 명확히 설정하고 이를 문서화하도록 하고 있는 한편, CCTV 설치위치, CCTV에 기록된 이미지의 질과 처리과정, 제3자에의 제공 및 데이터주체의 열람권 등에 대한 지침을 제공하고 있다. 그 구체적인 내용들을 간단히 살펴보면 다음과 같다.[37]

---

37) http://www.securitydirect.co.uk/en-gb/dept_101.html 참조.

1) 초기설치운영절차에 관한 기준: CCTV 설치시 목적을 분명히 하여 문서화하도록 하고, 최초의 설치목적을 벗어나 이용하는 것을 금지하고 있다. 그리고 CCTV 시행기준을 이행할 책임이 있는 사람이나 기관을 규정하고 문서화하도록 하고 있다(제7항).
2) 카메라의 위치에 관한 기준: CCTV 설치시 이에 대해 알리는 표지판을 달 것을 규정하고 있는데(제7항 이하), 주변 상황에 따라 그 크기가 어느 정도이어야 하는지에 대한 예까지 구체적으로 제시하고 있다. 예를 들어, 건물의 입구에 설치하는 경우에는 A4 정도의 크기로, 주차장 입구의 경우에는 운전자가 쉽게 알아 볼 수 있도록 A3 정도의 크기로 표지판을 설치해야 한다고 규정하고 있다. 표지판에는 CCTV의 목적, 관리 주체, 책임자(부서) 연락처 등을 명시하여 공지하도록 하고 있다. 또한 CCTV가 설치의 목적을 넘어 다른 곳을 비추는 것을 금지하고 있으며, CCTV의 조작자가 규정된 곳 이외의 곳을 보기 위해 임의로 조작하는 것도 금지하고 있다. 부득이하게 목적을 넘어선 부분까지도 촬영하게 될 때에는 최대한 프라이버시를 보호하도록 규정하고 있다. 그리고 일반인의 대화를 녹음하는 데 CCTV를 사용하는 것도 금지하고 있다(제12항).
3) 화질에 관한 기준: CCTV로 수집된 정보의 정확성을 보장하기 위하여, 설치시 CCTV의 정상 작동 여부를 반드시 점검하도록 하고 있으며, 이를 위해 화질에 관한 기준 관리일지를 기록해야 한다. 또한 테이프를 사용할 경우에는 좋은 품질의 녹화테이프만을 사용하도록 하고 있으며, 카메라의 위치, 날짜, 시간 정보 등을 정확하게 유지하도록 규정하고 있다.
4) 제3자의 이미지 접근 및 공개에 관한 기준: 법에 명시적으로 밝혀진 경우 이외에 목적을 넘어선 제3자 공유를 금지하고 있으며(제1항), 이미지를 녹화한 장비에 대한 접근은 모두 문서화하도록 하고 있다(제2항).
5) 영상처리에 관한 기준: 관리책임자 혹은 지정된 인원에 한해서만 모니터를 볼 수 있게 하고, 녹화기록에 대한 재생은 보다 엄격하게 규정하고 있다(제5항 이하). 특히 필요 이상으로 영상물을 보유하는 것을 금지하고 있는데, 예

를 들어 도심이나 공공도로의 영상은 31일 이상 보유하지 못하도록 하고 있으며, 보유기간이 지나 삭제하는 경우에도 그에 대한 자세한 기록을 남기도록 하고 있다(제8항).

6) 정보주체의 접근에 관한 기준: 정보주체의 자신의 정보의 접근에 관하여 상세한 규정을 두고 있다(제7항). 관리자 등은 촬영당한 사람이 신청할 경우 이에 대해 21일 이내에 서면으로 답변을 해야 한다.

7) CCTV 감독기준: 관리주체는 시행기준이 준수되고 있는지를 감독하기 위하여 문서화된 절차를 정기적으로 감독하고 정보주체에게 제공하여야 한다고 규정하고 있고, 시스템의 효율성에 대한 연간평가를 수행하여 공식적으로 공개할 것을 정하고 있다(제6항 이하).

(3) 2004년 2월 정보감독관은 데이터보호법의 적용대상이 되는 CCTV의 범위를 좀더 명확히 제시할 수 있도록 지침서를 추가로 발간하였다. 여기에서 규정하고 있는 내용을 간단히 살펴보면 다음과 같다.[38)]

우선 개인이 정보의 초점이 되고 해당 정보가 개인에 관한 특이사항을 담고 있는 경우 법적용의 대상이 됨을 밝히고 있다.

다음으로 적용범위와 관련하여 2~3대 정도의 카메라만 설치되거나 원격 이동이 불가능한 기본적인 CCTV 시스템의 운용은 원칙적으로 데이터보호법의 적용대상이 아니다. 하지만 특정인의 활동을 촬영하기 위해 원격으로 각도를 조절하거나 줌인·줌아웃을 하는 등 카메라를 작동하거나 혹은 녹화 이미지를 경찰과 같은 사법당국 이외의 자에게 제공한 적이 있는 등의 경우에는 동법이 적용될 수 있다.

그리고 도심 혹은 대형 매장 등에서 좀 더 복잡한 형태로 CCTV 시스템을 사용할 경우(카메라의 초점 이동, 특정인 찾기 혹은 범인이나 증인의 확인, 직원의 근무행위평가 등을 위해 녹화된 이미지를 조사하는 행위 등), 특정인의 활동을 주시하는데 사용될 수 있으므로 이들은 데이터보호법의 적용을 받게 된다.

만약 데이터보호법의 적용을 받는다고 판단되는 경우, 정보감독관에게 통지 및

38) http://www.informationcommissioner.gov.uk 참조.

서명 확인, 이미지 보관기간 결정, 정확한 장비작동의 상태를 확인하여야 한다.

(4) 한편, 카메라폰의 사용과 관련하여 2003년 5월 북잉글랜드의 Bolton 시의회는 허가증을 패용할 것을 조건으로 허용되는 불가피한 촬영의 경우를 제외하고는 레저센터의 탈의실, 화장실, 샤워룸에서 촬영하는 행위를 금지시키기로 결정한 바 있다.[39]

다. 독일의 경우

독일의 Hessen주에서는 1970년에 이미 데이터보호법률(Datenschutzgesetz)을 제정한 바 있었는데, 이는 개인정보보호에 관한 세계 최초의 입법으로 평가되고 있다. 연방의 차원에서는 1977년 1월 27일에 제정된 연방데이터보호법(Bundesdatenschutzgesetz; BDSG), 즉 「데이터처리에 있어서 개인에 관한 데이터의 남용방지에 관한 법률」이 제정되었다.

한편, 인터넷 등 새로운 정보통신수단의 급속한 확산으로 개인정보침해의 양상이 종래와는 사뭇 다른 형태로 전개되자 정보통신서비스를 효율적으로 규율하기 위한 특별법을 제정할 필요성이 대두되었다. 이에 「1997년 7월 22일 전자통신서비스에서의 데이터보호에 관한 법률」(Das Gesetz über den Datenshutz bei Telediensten vom 22. Juli 1997, BGBl I S. 1870)이 제정되었다. 약칭 '전자통신서비스데이터보호법'(Teledienstdatenschutzgesetz; TDDSG)으로 불리는 이 법률은 연방데이터보호법(BDSG)의 특별법으로서의 성격을 가진다.[40] 이 법의 규정은 서비스제공자가 개인데이터의 수집・유포・이용시에는 전자통신서비스법상의 통신서비스이용자의 개인데이터보호에 대하여 적용되며(제1조 제1항), 이 법에 규정되지 아니한 사항은 데이터가 파일로 처리되거나 이용되지 않는 경우에도 개인데이터보호에 관한 규정이 적용된다(제1조 제2항).

독일은 2003년 연방데이터보호법(Bundesdatenschutzgesetz; BDSG)에서 비디오감시

---

39) http://news.bbc.co.uk/1/hi/england/manchester/3043931.stm

40) S. Engel-Flechsig, "IuKDG vom Budestag verabschiedet. Änderungen des TDDG und des SiG," *DuD* 1997, S. 8 ff.

(제6b조)와 개인이동통신장비(제6c조)에 관한 규정을 신설함으로써 전자감시사회에서의 기본권침해에 적극적으로 대처하고 있다.

먼저, 제6b조에 의하면 비디오감시는 1) 공공기관의 임무수행의 경우, 2) 주거권의 실현을 위한 경우, 3) 구체적으로 확립된 목적을 위해 권리 있는 이익의 실현을 위하여 필요하고 관련 당사자의 보호받을 이익이 우월하지 않은 경우에 한하여 허용된다(동조 제1항). 수집된 데이터의 처리와 이용은 그 데이터가 달성하려는 목적을 위하여 필요하고 당사자의 보호법익이 우월하지 않을 때에만 인정되며(동조 제2항), 다른 목적을 위한 개인정보의 처리와 이용은 위험의 방지와 국가와 공익의 안전을 위하여 그리고 범죄행위의 추적을 위하여 필요한 경우에 한하여 허용된다(동조 제3항). 그리고 비디오감시를 통하여 수집된 데이터가 특정한 개인과 연결될 경우에는 그 처리와 이용에 관하여 이를 당사자에게 통지하여야 하고(동조 제4항), 그 데이터가 목적달성을 위해 더 이상 필요치 않을 경우 또는 지속적인 저장이 당사자의 보호법익에 상충될 때에는 지체없이 삭제되어야 한다(동조 제5항).

다음, 제6c조에 의하면 개인이동통신장비(즉, 이동성 있는 개인적 저장 및 처리장비)를 교부하거나 전부 또는 부분적으로 그러한 매체에서 진행되는 자동화된 개인데이터의 처리를 위한 절차를 그러한 매체에서 진행시키는 담당자는 당사자가 모르고 있을 경우 그 당사자에게 ① 신분과 주소, ② 처리될 수 있는 개인정보의 종류를 포함하여 그 매체의 작동에 대해 일반적으로 이해될 수 있는 형식, ③ 제19조, 제20조, 제34조와 제35조에 따라 행사할 수 있는 당사자의 권리, ④ 매체의 분실이나 멸실의 경우 마련되어야 하는 대책을 통보하여야 한다(제1항). 제1항에 따라 책임자는 질의응답을 위해 필요한 기계나 설비를 적정한 방법으로 무상으로 이용할 수 있도록 배려해야 하며(제2항), 그 매체로 처리할 수 있는 통신의 과정을 당사자에게 명백하게 알 수 있도록 해야 한다(제3항).

라. 기타 EU 회원국의 동향

일부 EU 회원국들은 헌법, 법률 또는 여러 국가 기관에서 발표한 명령(order) 및 판결(decision)을 바탕으로 비디오감시 관련 사례연구를 이미 진행하고 있다. 가령 포르투갈의 헌법재판소는 “일반 시민들을 대상으로 하는 사설 보안기관의 전자감

시장비의 사용 및 모니터링 작업은 헌법 제26조에 기술된 사생활보호의 권리를 침해한다"고 판시한 바 있다(255/2002). 그리고 벨기에의 경우 정보보호법을 준수하지 않은 이미지의 수집행위는 법원에서 증거거부의 사유가 될 수 있다.

일부 국가의 경우 개인정보처리 여부에 관계없이 CCTV의 설치 및 사용은 국가정보보호기구로부터 사전승인을 받도록 규정하고 있으며, 현재 비디오감시 관련법이 없는 나라의 경우도 정보보호기구가 주관하여 지침, 의견서 및 행동지침 등의 정보보호규정작업을 활발히 진행하고 있다.[41)]

마. 덴마크

2000년 2월 Consolidation Act(비디오감시금지법)에서 민간단체들의 공공장소(거리, 도로, 광장 혹은 이와 유사한 지역)에서의 비디오감시행위를 금지하였다.

2002년 6월에는 정보보호감독기구가 대형슈퍼마켓의 비디오감시 및 인터넷 publishing을 통한 전송과 관련하여 의견서를 발간하였고, 2003년 7월에는 "민간이 운영하는 대중교통수단에 설치된 비디오감시시스템은 균형성의 원칙과 덴마크 정보보호법에 포함된 규정을 준수할 것"이라는 내용의 의견서를 발간하였으며, 2003년 11월에는 공공기관의 비디오감시행위에 대한 특정 제한규정을 마련한 바 있다.

바. 스웨덴

비디오감시는 일반비디오감시관련법(1998:150)과 비밀감시(범죄조사)법을 통해 규제된다. 일반적인 비디오감시는 보통 국가행정위원회의 승인이 요구되며, 비밀스러운 비디오감시는 법원의 승인을 받아야 한다. 하지만 우체국, 은행 그리고 상점 등의 경우는 제외되며, 국가행정위원회의 결정에 대하여 법무부장관은 항소할 수 있다.

디지털기술을 통한 비디오녹화는 개인정보의 처리로 간주되어 일반비디오감시법에서 특별히 규정하지 않는 범위까지 정보조사위원회의 감시대상이 된다.

---

41) http://e-privacy.or.kr/mailing/Mailimg/newsletter/200401/B/pds/CCTV.pdf 참조.

사. 네덜란드

1997년에 발행된 정보보호감독기구보고서에는 공공장소에서의 개인 및 재산 보호를 위한 비디오감시지침이 포함되어 있으며, 2004년에 갱신된 보고서가 공개될 예정이다. 그리고 2004년 1월부터 형법전(Penal Code)에서 규정하는 범죄행위의 범위를 공공장소에서 통지 없이 이루어지는 사진촬영으로까지 확대하는 개정안이 최근 하원을 통과하였다.

정부는 최근 일정한 조건에서 공익을 목적으로 비디오감시시스템을 공공장소에서 사용할 수 있는 명확한 권한을 시장과 시의 위원회가 부여할 수 있도록 하는 지방법의 변경을 제안하였다.

아. EU의 경우

2002년 7월 12일 유럽의회 및 유럽연합 이사회는 전자통신부문에서의 개인정보보호와 관련하여 그 동안의 정보통신서비스 시장과 기술의 발전사항을 반영하기 위한 「전자통신부문에서의 개인정보처리와 프라이버시보호에 관한 지침」(프라이버시와 전자통신에 관한 지침; Directive 2002/58/EC)[42]을 새로이 제정하였다.

이 지침에 의하면, 공중통신망 또는 공개 전자통신서비스 사용자나 가입자에 관한 위치정보의 처리는 당해 정보를 반드시 익명으로 또는 사용자나 가입자의 동의를 받아서 부가서비스 제공에 필요한 한도와 기간 내에서 이루어져야 하고, 서비스제공자는 사용자나 가입자의 동의를 받기 이전에 처리할 전송정보 이외의 위치정보의 종류, 해당 처리의 목적과 기간, 그리고 부가서비스 제공을 목적으로 그 정보를 제3자에게 전송할 것인지의 여부를 사용자나 가입자에게 설명하여야 한다(제9조 제1항).

그리고 위치정보의 처리에 관한 사용자나 가입자의 동의를 이미 받은 경우라도 사용자나 가입자가 간단한 방법으로 비용을 들이지 않고 네트워크접속시마다 또는 통신전송시마다 해당 정보처리를 일시적으로 거절할 수 있는 가능성을 계속하여 부

42) Directive 2002/58/EC of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector(Directive on Privacy and Electronic Communications). *Official Journal* L 201, 31/07/2002 P. 0037－0047.

여하여야 한다(제9조 제2항).

이러한 위치정보의 처리는 공중통신망 제공자나 공개 전자통신서비스 제공자 혹은 부가서비스를 제공하는 제3자의 감독을 받는 자에 국한되어야 하며 또한 부가서비스 제공목적상 필요한 범위로 제한되어야 한다(제9조 제3항).

자. 한국의 경우

1980년대부터 우리나라에서는 행정전산망을 포함하여 국가기간전산망사업을 추진하였으나, 국가기관 내에서 개인정보의 전산화가 확대됨으로써 잘못된 정보의 입력, 전산정보의 유출 등으로 인한 개인의 사생활침해 가능성이 현저히 증대하였다. 이에 대하여 기존의 법률들로는 충분히 대처하기 곤란하였기 때문에 학계와 언론 등에서 개인정보보호에 관한 법률의 제정을 촉구하였고 이에 따라서 행정에 대한 신뢰성을 확보한다는 차원에서 1992년 4월 10일 입법예고, 1993년 말 국회를 통과하여 마침내 1994년 1월 7일 공공기관의개인정보보호에관한법률(법률 제4734호)이 공포되어 1995년 1월 8일부터 시행되었다. 개인정보보호법은 “공공기관의 컴퓨터에 의하여 처리되는 개인정보”를 그 보호의 대상으로 하고 있다(법 제1조). 여기서 개인정보는 “생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)”를 말한다(법 제2조 제2호). 따라서 이 법률은 공공부문에 한하여 적용되며, 컴퓨터에 의해 처리되지 않는 정보에 대해서는 적용되지 아니한다.

한편, 민간부문에서의 정보통신망이용 증대에 따른 개인정보의 보호와 관련하여서는 현재 정보통신망이용촉진및정보보호등에관한법률이 규율하고 있다. 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 하고 있다(제1조). 따라서 이 법률은 정보통신망의 이용촉진 및 개인정보의 보호, 그리고 정보통신망의 안전확보를 위한 입법이라 할 수 있다.

한편, 우리나라의 경우 전자감시장비의 설치 및 사용이 꾸준히 증가하고 있음에

도 불구하고 그 설치와 이용을 전체적으로 규율할 수 있는 법제도가 마련되고 있지 않다. 1994년의 공공기관의개인정보보호에관한법률이 있으나, 그 적용범위의 협소성으로 말미암아 전자감시에 대한 충분한 대응장치를 갖추고 있지 못하다.

4. 관련 사례의 고찰

가. CCTV 관련 사례

국내에서도 서울과 부산, 인천 등 6개 광역시 경찰청이 운영하는 1,178대, 서울의 종로, 관악, 강남구청이 운영하는 107대의 CCTV가 있다고 한다. 그리고 최근 강남구청은 구 전역에 방범 CCTV 300여대를 추가로 설치할 계획인 것으로 알려지고 있다. 게다가 기업빌딩과 학교, 지하철, 찜질방, 편의점, 술집, 주택 등에 설치되어 운용되고 있는 민간부문의 감시카메라까지 감안하면 전체적으로 수십만 대에 이를 것으로 추산된다.[43] 이처럼 CCTV의 설치 및 사용이 꾸준히 증가하고 있음에도 불구하고 그 설치와 이용을 전체적으로 규율할 수 있는 법제도가 마련되고 있지 않다.

그러나 현재 우리나라에서는 특히 초상권의 침해를 처벌하는 처벌의 규정은 따로 존재하지 않는다. 민사상으로는 CCTV와 관련하여 법적으로 다투어지고 있는 사례가 더러 있으나, 그 대부분은 손해배상청구와 관련된 사건들이다. 그러한 사건에 있어서 법원은 대체로 공익의 목적과 비례의 원칙 등을 충족할 경우 CCTV 등 촬영도구를 이용한 공공장소에서의 공적인 촬영행위는 적법한 것으로 보는 경향이 있다.[44]

나. 강남구 CCTV 사례

최근 2004년 4월 19일 국가인권위원회 제1소위원회는 “CCTV의 설치·운영이 지방자치단체나 경찰서장의 재량에 의해 이뤄지고 있고 장비의 성능이 점차 향상돼 운영방법 등에 따라 국민의 기본권을 침해할 요소가 크다”고 판단하면서, 국회의장과 행정자치부 장관에게 CCTV의 설치・운영에 관한 법적 기준을 마련할 것을 권고한 바 있다.

---

43) 동아일보 2004. 2. 19.

44) http://e-privacy.or.kr/mailing/Mailimg/newsletter/200401/B/pds/CCTV.pdf

여기서 국가인권위원회는 CCTV의 설치·운영은 촬영되는 사람들에 대하여 초상권과 개인정보자기결정권(헌법 제10조), 사생활과 가정, 주거의 자유 및 이를 법으로 보호받을 수 있는 권리(헌법 제17조, 시민적및정치적권리에관한국제규약 제17조)를 침해할 수 있다고 인정하였다. 그리고 현재 CCTV의 설치·운영에 관한 법적 근거가 없는 상태에서 지방자치단체나 경찰서장의 재량에 의하여 그것을 범죄 수사 등에 활용하는 것은 헌법이 규정한 기본권 제한원칙인 적법절차원리와 법률유보원칙에 위배되는 것이라고 판단하였다.[45]

이하에서 국가인권위원회의 결정문에 나타난 주요 내용은 다음과 같다. 즉, "범죄예방을 위하여 공공기관이 CCTV 등 무인단속장비를 공공장소에 설치·운영하는 것은 그 설치지역과 운영방법 등에 따라 개인의 초상 그 자체뿐만 아니라 특정시간에 어디서 어떤 모습으로 누구와 함께 있었는가에 관한 개인정보를 취득하는 것이며, 설치·작동 방법에 따라서는 개인의 사생활 영역내의 모습을 녹화·저장하는 것도 가능하다. 따라서, 범죄예방을 위한 CCTV 등 무인단속장비의 설치·운영은 CCTV 등 무인단속장비에 촬영되는 사람들의 초상권과 개인정보자기결정권 침해 문제를 야기할 수 있고, CCTV 등 무인단속장비의 설치 지역에 거주하는 주민의 사생활의 비밀과 자유를 침해할 수 있다. … 현재 범죄예방을 위한 CCTV 등 무인단속장비의 설치·운영 계획은 경찰 혹은 지방자치 단체 등에서 CCTV 등 무인단속장비의 필요성, 설치지역 및 운영방법, 절차 등을 임의로 판단하여 설치하고 있다. CCTV 등 무인단속장비가 행인의 초상과 행적에 관한 개인정보 및 그 설치·운영에 따라서는 사생활을 촬영·녹화할 수 있어서 국민의 기본권을 침해하고 있으며, 아무런 법적 규제 없이 확대 시행될 우려가 있다. 따라서, 범죄예방을 위한 CCTV 등 무인단속장비가 설치 목적에 맞게 제한적으로 사용되고, 개인의 초상권과 개인정보자기결정권 및 사생활의 비밀과 자유권을 침해하지 않도록 설치에 대한 법적 근거 마련 및 그 운영 절차와 방법, 요건 등을 법률로 정할 필요가 있다."[46]

---

45) 국가인권위원회 2004. 4. 19.자 결정, 공공기관의 CCTV 등 무인단속장비의 설치·운영 관련 정책 권고.

46) 국가인권위원회공보, 제2권 제3호, 381－384면.

이어서 국가위원회는 CCTV 등 무인단속장비의 설치・운영에 관한 법률의 제정에 있어서 반드시 포함되어야 할 사항들을 다음과 같이 제시하고 있다.

1. CCTV 등 무인단속장비 설치 목적을 법률에서 명확히 규정하고, 특별한 경우를 제외하고는 목적 외 용도로 사용할 수 없도록 할 것, 2. CCTV 등 무인단속장비 설치에 대한 사전, 사후 고지 의무 및 촬영대상자의 동의절차를 갖출 것, 3. CCTV 등 무인단속장비 관리에서 녹화・보존된 내용의 정확성을 확보할 것, 4. 촬영범위를 제한할 것, 5. 녹음기능을 사용할 수 없도록 할 것, 6. CCTV 등 무인단속장비로 촬영된 녹화기록물에 대한 제3자 제공에 대하여 엄격히 규제하고, 자료의 보유기간을 명시할 것, 7. 기술적 보안 조치는 물론, 운영 권한, 촬영된 자료에 대해서 접근할 수 있는 권한을 제한하는 등 인적 보안 조처를 할 것, 8. CCTV 등 무인단속장비 시스템의 기본적인 사항에 대해 모든 사람이 알 수 있도록 공지할 것, 9. CCTV 등 무인단속장비 운영에 대하여 정보주체의 관리 통제권을 보장할 것, 10. 설치, 관리, 유지와 관련하여 그 주체와 자격을 명확히 할 것.

다. 시흥시립도서관 CCTV 사례

시흥시립도서관은 개관 당시부터 심야의 무인경비시스템으로 CCTV를 설치, 운영하였으나, 열람실 내부에서 각종 도난사고가 발생하고 여자화장실내 불미스런 사건 및 화재 등이 발생함에 따라 2003. 2. 각 열람실 내부와 화장실 입구에 3대의 CCTV를 추가 설치하였다. 이에 대해 도서관 열람실 내부에까지 CCTV를 설치, 운영하는 것은 도서관 이용자들의 사생활의 비밀을 침해한다는 취지의 진정이 국가인권위원회에 제출되었다.

이에 대해 국가인권위원회 제1소위원회는 2004년 7월 14일자 결정에서 기본권의 침해는 인정되나 이미 문제점이 시정되어 별도의 구제조치가 불필요하다고 하면서 국가인권위원회법 제9조 제1항 제3호에 따라 기각결정을 내렸다.[47] 그 구체적인 언급내용을 살펴보면 다음과 같다.

---

47) 국가인권위원회 2004. 7. 14.자 03진인6416 결정, 공공기관의 CCTV 등 무인단속장비의 설치・운영 관련 정책 권고.

즉, “현재까지 공공시설내 CCTV 설치, 운영에 관한 법률적 근거가 마련되지 않은 가운데 공공도서관의 열람실 내부까지 CCTV를 설치하여 이용자들의 모습을 촬영하고, 이를 도난 사고 예방이나 범죄자 적발에 이용한 것은 적법절차의 원리(헌법 제12조)를 위반하여 시민의 초상권(헌법 제10조) 및 사생활의 비밀과 자유(헌법 제17조) 등 기본권을 침해하는 것이고, 특히 모니터 화면을 개방된 장소에 공개함으로써 촬영 대상자의 모습이 불특정 다수의 공중에게 무차별적으로 보이게끔 방치하고 있는 것은 더욱 심각한 문제로 판단되나, 이에 대해서는 이미 우리 위원회가 공공시설내 CCTV 설치, 운영에 관한 법률 제정을 국회의장과 행정자치부장관에게 권고한 바 있고(2004. 4. 17. 국가인권위원회 결정), 위원회 조사과정에서 피진정인은 진정인의 요구를 받아들여 열람실내 CCTV를 열람석이 아닌 출입구 방향으로 촬영방향을 조정하였고, 모니터 화면을 도서관 게시판 설치물로 막아 평소에는 아무도 이를 볼 수 없도록 조치하였으며, 관계기관인 문화관광부도 법률적 근거가 없는 상태에서 공공시설내 CCTV 설치・운영은 인권 침해 가능성이 높다는 점을 인정하고, 향후 법률 제・개정 전에 공공도서관내 CCTV를 부득이 설치할 경우에는 CCTV 설치 여부, 설치목적, 운영방법, 관리책임자 및 감독체계 등 기준과 절차를 마련하여 이용자들이 쉽게 볼 수 있는 형태로 공지하고, 일정 시기(15일) 경과 후 녹화된 정보가 자동 삭제되도록 하며, 보관된 정보의 유출 등 오남용 사례가 없도록 유의할 것 등을 공공도서관에 권고하였다. 따라서 이 부분에 대한 진정내용에 대해서는 별도의 구제조치가 필요하지 않은 경우로 판단된다.”[48)]

라. 평가

CCTV에 관한 국가인권위원회의 결정은 사법부의 재판이 아니지만, 인권보호를 목적으로 하는 국가기관의 유권해석이라는 점에서 큰 의미를 가진다고 할 수 있다. 특히 위의 2004년 4월 19일자 국가인권위원회 결정은 관련 법률의 정비방향을 아주 자세하게 제시하고 있을 뿐만 아니라, 문화관광부나 공공도서관협의회 등에 의해서 수용되고 있다.[49)] 따라서 이 결정은 CCTV의 설치와 운영에 관한 한 중요한 선례로

48) 국가인권위원회공보 제2권 제4호 657－658면.

서 그 법적 지위를 가질 수 있다고 본다.

마. 카메라폰 관련 사례

최근 카메라폰 등의 등장으로 말미암아 누구든 마음만 먹으면 아무 데서나 촬영・인화・인터넷 배포를 할 수 있게 되었고, PC 방, 개인집, 사무실의 PC를 켜기만 하면 인터넷과 접속하여 아무 때나 피사 인물에 대한 동의 없이 그의 비밀스런 부위나 인상이나 뱉은 말까지도 마구 유포시킬 수 있게 되었다. 이로써 몇 해 전부터 사회를 감시의 눈초리로 만들어 버린 몰래카메라가 개인의 수중에 들어간 상황이라 할 수 있다.

최근 부산에서 한 카메라폰 사용자가 지하철 내에서 짧은 치마를 입고 있던 여대생의 은밀한 부분을 촬영하다 이를 목격한 승객에게 붙잡혀 처벌받은 사례, 서울의 한 여자 회사원이 최근 전자우편 스팸메일을 정리하는 도중 '목욕탕 몰카'라는 제목으로 수신된 한 음란웹사이트 광고에서 옷을 벗고 있는 자신의 뒷모습이 짧은 동영상으로 배포되고 있는 것을 확인하여 신고한 사례, 부산의 한 여대생은 자신과 사귀던 남자 친구가 카메라폰으로 몰래 찍어둔 자신의 나체 사진을 학교와 친구들에게 무차별 유포하여 심각한 정신적 충격을 받은 사례 등이 있었다.

국내에서는 카메라폰의 사용을 직접 규제하는 특별한 법률이나 규정은 없다. 물론 비밀장치의 기록을 촬영하거나 억지로 촬영하거나 함부로 유통 또는 공개하는 행위는 현행법상으로도 처벌의 대상이 될 수 있다. 가령 비밀장치한 사람의 편지, 문서 또는 전자기록 등 특수매체기록을 카메라폰을 이용하여 촬영할 경우 형법 제140조 제3항이나 제316조 제2항에 따라 처벌 가능하고, 사람을 비방할 목적으로 정보통신망을 통하여 공연히 사실을 적시하여 타인의 명예를 훼손할 경우 정보통신망이용촉진및정보보호등에관한법률 제61조에 의하여 처벌할 수 있다. 또한 카메라 기타 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 타인의 신체를 그 의사에 반하여 촬영하는 것은 성폭력범죄의처벌및피해자보호등에관한법률 제14조의2에 의해, 그리고 자기 또는 다른 사람의 성적 욕망을

49) 2004년 7월 20일 국가인권위원회 보도자료 참조.

유발하거나 만족시킬 목적으로 전화·우편·컴퓨터 기타 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건을 상대방에게 도달하게 하는 것은 성폭력범죄의처벌및피해자보호등에관한법률 제14조에 따라 처벌의 대상이 된다. 한편 사람을 비방할 목적으로 정보통신망을 통하여 공연히 사실 또는 허위의 사실을 적시하여 타인의 명예를 훼손하는 것은 전기통신사업법 제53조의 불법통신금지규정에 의해 처벌하는 것도 가능하다. 하지만 그와 같은 규정들로는 공공장소에서의 카메라폰의 이용으로 발생하는 개인정보보호의 문제에 일반적으로 적용되기는 어렵다.

현재 삼성전자와 LG전자 등 일부 대기업에서는 자구책으로 연구소 등에 카메라폰 반입을 금지하거나 사용을 제한하는 조치를 취하고 있을 뿐이다. 그리고 정보통신부는 2003년 11월 휴대폰 제조업체와 시민단체 등과 협의하여 카메라폰의 촬영음 의무화를 추진하기로 한 바 있으며, 한국정보통신기술협회(TTA)가 2004년 5월에 확정한 카메라폰촬영음크기표준(TTAS.KO-06.0063)에서는 2004년 7월 1일 이후 신규 출고되는 모든 카메라폰 촬영시 반드시 60～68dBA의 촬영음을 내도록 규정하기에 이르렀다.[50] 그런데 이미 출시되고 있는 휴대폰을 보면 진동모드에서는 촬영음이 들리지 않아 은밀한 촬영이 여전히 가능한 형편이다.

바. 위치추적의 사례

오늘날 보편화되고 있는 위치기반서비스(Location Based Systems)는 가장 가까운 곳에 있는 식당, 약국, 주유소, 병원 등을 찾는 서비스나 사용자의 위치를 자동으로 응급치료기관에 전송하는 비상서비스, 사용자에게 위험, 교통정체, 나쁜 기상상황을 아려주는 경고서비스, 부모들은 자녀들의 위치를 확인할 수 있는 후견적 서비스 등 다양한 형태로 활용되고 있다.

그런데 이러한 위치확인정보는 주로 이동전화, 개인의 데이터단말기, 이동무선설비가 장착된 자동차 등을 사용하는 기술장치에 관련된 정보로서, 대부분의 경우에는 이 데이터들이 이런 유형의 장비를 소유하거나 적어도 사용하는 개인과 연결될

50) 디지털타임스 2004. 5. 28.

수 있다. 만일 이런 정보가 신뢰할 수 없는 것이라면 데이터의 민감도는 증가한다. 따라서 모든 상황에서 위치확인정보는 개인정보로 취급되어야 한다.[51] 심지어 그러한 정보가 대중에게 공개되어 개인적 데이터로서의 속성을 상실하는 경우에도 그와 같은 정보를 무단으로 활용하려는 자에 대해서는 개인정보로서 보호될 필요가 있다. 특히 위치기반서비스에 의한 상호접속과 서버에 저장된 위치확인정보의 오용은 심각한 개인정보의 침해를 야기할 수 있다.[52]

무선전화는 신호를 나르거나 수신하기 위하여 기지국(base station)에 그 위치를 교신해야만 한다. 따라서 무선전화를 사용하거나 신호를 수신하기 위하여 설정할 때마다 그 이용자의 위치를 매우 짧은 간격으로 효과적으로 확인시켜 준다. 무선전화 지역이 더 세밀해지면 질수록 사람의 위치는 더욱 정밀하게 확인될 수 있다.

이에 따른 개인의 사생활 침해를 막기 위해 미국은 2000년 8월에 제정된 무선통신과공중안전법(Wireless Communications and Public Safety Act)에서 유선, 무선, 광역 PCS 사업자들이 도청의 권한을 갖고 있는 법집행기관은 FCC에 대하여 이동전화의 송수신지국의 위치를 알려줄 것을 요청할 수 있다고 명시하고 있다.[53]

그리고 스위스 정부도 국가안보에 "필수적인" 무선전화를 누가 이용하고 있는지를 식별하기 위하여 이용될 수 있도록 해야 한다면서, 시민들이 "간편한" 무선전화를 취득할 때 등록하는 제도를 도입할 것을 제안한 바 있다.[54]

국내에서는 자신도 모르는 사이에 장기간에 걸쳐 위치 추적을 당해온 삼성SDI 노동자들이 삼성 쪽이 불법복제 휴대전화를 이용해 위치 추적을 지시했다고 주장하면

---

51) Hansjürgen Garstka, "Data Protection and Freedom of Information", 2002 개인정보보호 국제 컨퍼런스 발표문, 2002.11.28, 참조.

52) 다카토 나츠이, "상업적 목적 및 프라이버시 보호를 위한 위치기반서비스", 2002 개인정보보호 국제 컨퍼런스 발표문, 2002.11.28, 참조.

53) FCC, Third Report and Order in the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97－213, ¶¶ 12, 21, 22, Aug. 26, 1999 http://www.fcc.gov/Bureaus/Engineering_Technoloy/Orders/1999/fcc99230.wp.

54) Michael Froomkin, "The Death of Privacy", 52 Stanford Law Review, 1461, 2000, pp. 1479～1480.

서 서울중앙지검에 고소장을 제출한 사례가 있었다.[55] 그리고 최근 공무원노조파업에 대응하는 과정에서 정부가 휴대전화로 파업에 참가할 가능성이 있는 조합원들의 위치를 추적하는 사례가 발생하였다는 주장이 제기되어 논란이 되고 있다.[56]

한편, 정부의 독점적인 재산이었던 고품질의 위성사진은 이제 누구나 구입하여 이용할 수 있다. 오늘날 판매 중에 있는 최첨단의 사진은 길이가 2미터밖에 안 되는 목표물까지 구별해낼 수 있다. 그동안 미국정부는 유죄판결을 받고 집행유예, 보석중인 형사범을 감시하는데 위성추적을 이용해 왔다. 이들 범죄인은 GPS(global positioning satellites)로부터 좌표를 수신하여 그것을 감시센터와 교신하는 자그마한 추적장치를 지니고 다닌다. 영국에서는 과속을 방지하기 위한 GPS 시스템의 채택을 고려하고 있다. 자동차들은 GPS 모니터를 장착하게 되며, 그 모니터는 그 차량의 정확한 위치를 파악하고, 내장된 컴퓨터와 연결되어 전국의 도로정보망을 담게 되며, 적절한 속도제한을 식별하고, 그 차량이 특정한 속도를 초과할 경우 내장된 통제기에 연료공급의 중단을 지시한다. GPS 시스템은 수신자가 위성의 참조에 의하여 그 위치를 결정할 수 있도록 하지만, 누구에게나 수신자의 위치를 실제로 전송하지는 않는다.[57] 하지만 내장된 컴퓨터는 연료가 충분히 공급되는 한 그 자동차가 가는 어느 곳이든 영구히 기록할 수 있을 것이다. 지속적으로 그리고 실시간으로 모든 운송수단의 위치에 관한 정보를 취득할 수 있으며,[58] 운전자의 모든 여행기록이 낱낱이 저장될 수 있다.[59] 어떤 나라에서는 또한 자동차의 식별을 용이하게 하기 위하여 등록번호판에 코드를 붙일 방안까지 고려되고 있다.[60]

---

55) 한겨레신문 2004. 7. 14.

56) 연합뉴스 2004. 11. 15.

57) Michael Froomkin, *op. cit.*, pp.1496～1498 참조.

58) Margaret M. Russell, “Privacy and IVHS: A Diversity of Viewpoints,” 11 *Santa Clara Computer & High Tech. L. J.* 145, 163 (1995).

59) *Id.*, pp.164～165.

60) Andrew Sparrow, “Car Tagging May Help Cut Theft, Say Minister”, Daily Telegraph (London), Oct. 17, 1998, *available* in 1998 WL 3053349.

5. 법제정비의 방향

이상에서 전자감시에 의해 초래될 수 있는 기본권침해의 양상과 그에 대한 각국의 입법적 대응 및 관련 사례들을 살펴보았다.

전술한 바와 같이 과연 유비쿼터스 컴퓨팅의 환경은 인류에게 보다 더 편리하고, 보다 더 풍요롭고, 보다 더 행복한 세상을 가져다줄 것이라는 유토피아적 메시지를 던져주고 있다. 하지만 다른 한편으로는 어쩌면 그것이 비밀이 없는 세상, 서로가 서로를 감시하는 끔찍한 지옥의 상황을 초래하는 것이 아닐까 하는 심각한 우려를 자아내는 것도 사실이다. 하지만 다른 한편으로 그것이 우리에게 가져다준 생활상의 편익 또한 실로 막대하다는 점을 결코 부인할 수 없다. 가령 CCTV의 설치와 사용으로 인하여 범죄의 예방이나 증거의 확보가 훨씬 용이해지는 것이 사실이다. 그리고 위치추적시스템의 활용은 길찾기, 교통상황의 안내 등 이루 말할 수 없는 편리함을 제공하며, 때로는 유괴범의 추적에 상당한 공헌을 하기도 한다. 따라서 그 첨단기술의 혜택을 누리려는 사람들의 수요를 가벼이 여겨서는 안 될 것이다.

그렇다면 결국 전자감시사회에 있어서도 인권보호의 요청과 그 효율적 활용의 측면을 적절하게 조화시킬 수 있는 방안을 모색하는 것이 무엇보다도 중요하다고 하겠다. 그것은 개인정보보호의 요청을 충돌되는 공공의 이익 내지 통신의 자유나 업계의 영업상 자유 등과 같은 타인의 기본권과 조화시킬 수 있는 원칙들에 관한 논의로 수렴될 수 있을 것이다. 그 구체적인 내용은 기본권제한의 일반원칙과 개인정보보호에 관한 특수원칙 등에서 찾을 수 있다고 본다. 그리고 개별적인 문제로서 검토되고 있는 분야에 관한 특별법의 정비와 관련하여서는 해당 기술의 특수성과 그에 대한 수요 등을 충분히 고려하여 법적 규율의 형태나 정도가 결정되어야 할 것이다.

이하에서는 개별적인 문제에 대처하기 위한 법제의 정비방향에 대해 의견을 제시하는 것으로 이 글의 결론에 갈음하고자 한다.

먼저, 개인정보보호에 관한 법제를 통합기본법으로 정비할 경우 국제 가이드라인과 외국의 입법례를 참고하여 비디오감시에 관한 원칙을 정하는 규정을 두어야 할 것이다. 그와 별도로 CCTV를 설치할 수 있는 주체, 설치장소, 장비의 종류, 그 운영

방법과 절차, 본인에 의한 통제방법, 감독기관의 감독 등을 포괄적으로 규정하는 비디오감시 관련 특별법을 제정할 필요가 있다고 본다. 다만 전반적인 개인정보보호법제의 체계정비가 지체될 경우 공공기관의개인정보보호에관한법률의 개정을 통해서나마 CCTV의 공적 설치 및 운영에 관한 구체적인 요건, 절차, 감독기관, 개인의 권리 등에 관한 규정을 두는 것도 필요할 것이다.

다음으로, 카메라폰에 의한 개인정보침해의 피해현황을 정확하게 조사하고 신종기술의 개발에 따른 새로운 개인정보의 침해유형을 면밀히 분석하여 그에 대한 법적·제도적 장치를 마련하는 것이 시급하다고 하겠다. 그런데 여기서는 카메라폰 이용자와 촬영 상대방의 권리를 조화롭게 보장한다는 관점이 무엇보다도 강조될 필요가 있다. 카메라폰에서 특별히 문제가 되고 있는 것은 통화기능이 아니라 촬영기능에 있다. 만약 통화기능과 촬영기능을 분리하여 규제할 방법이 있다면, 통화기능까지 전면 차단하기보다는 촬영기능만 규제하는 방식을 고려함이 상당할 것이다. 이는 곧 기본권제한에 있어서 준수되어야 할 필요최소한의 원칙에 부응하는 길이 된다. 이러한 점에서 카메라폰의 전면적인 시판금지라든가 공공장소에의 반입을 금지하는 방식보다는 은밀한 촬영에 사전적으로 그리고 사후적으로 규제를 가하는 방안이 바람직할 것으로 본다. 구체적으로는 무단촬영에 대한 행위규제라는 법적 방안과 더불어 일정한 지역에서의 촬영기능을 중단하거나 촬영사실을 표시하도록 하는 기술적 방안도 고려될 수 있을 것이다.

마지막으로, 위치추적시스템에 의한 개인정보침해의 문제를 해결하기 위해서는 프라이버시보호를 위해 보다 나은 기술을 활용하거나 불필요한 프라이버시 정보수집기능을 삭제하도록 하는 방안과 국제 프라이버시보호기준을 토대로 보다 나은 지침을 정하거나 관련 당사자들이 공통된 프라이버시 관련 목표에 합의하도록 하는 자율규제의 방안도 고려될 수 있겠다. 하지만 무엇보다도 실효성이 있는 것은 역시 법적 방안이라 하지 않을 수 없을 것이다. 이 문제에 대처하기 위한 우리의 법제정비에 있어서도 대체로 다음과 같은 개인정보보호의 원칙이 반영되어야 할 것이다. 우선 위치확인정보의 수집과 이용은 원칙적으로 사전설명에 기초한 당사자의 동의를 얻도록 하고, 그 처리는 부가서비스 제공에 필요한 한도와 기간 내에서 그리고

익명화에 의해서 이루어지도록 하여야 할 것이다. 또한 위치기반서비스에 의한 불필요한 상호접속은 법으로 금지하거나 제한하고, 위치확인정보를 불필요하게 수집하는 것은 법적으로 제한하여야 한다. 그리고 위치기반시스템에 내재된 취약성은 수정되거나 제거될 수 있도록 조직적·절차적적 조치가 강구되어야 한다. 나아가 수집한 위치확인정보를 심각하게 남용할 경우 형사처벌을 할 수 있도록 하여야 할 것이다.

제 4 절 RFID 발전에 따른 정보 프라이버시 보호에 관한 법적 연구

1. 서 론

현대의 정보통신기술의 눈부신 발전은 마침내 차세대 기술의 발전방향을 '유비쿼터스'라는 개념에 그 초점을 맞추도록 요구하고 있다. 이러한 신정보사회를 선도할 핵심주자중의 하나인 RFID(Radio Frequency Identification)는 현재 학계 및 산업계의 커다란 주목을 받고 있다. RFID는 전자태그와 판독기를 통해 비접촉식으로 정보를 송수신하는 기술로서, 비접촉식이며 전자태그 내에 정보를 기록할 수 있다. 특히 현재 사용되고 있는 바코드를 대체하여 제품에 부착될 경우 재고관리, 유통관리, 이력관리 등에 획기적인 전기를 마련하게 되고 생산성을 높일 수 있다는 장점을 가지고 있다. 그러나 비접촉식이라는 특성, 유일한 제품코드, 그리고 이력에 대한 정보가 전자태그 내에 저장될 수 있다는 RFID의 특성은 판독기를 통해 읽어들인 정보를 개인정보와 연결하는 경우 개인의 프라이버시를 심각히 침해할 수 있게 된다는 문제점이 있다.[61]

---

61) 기술이 무책임하게 발전한다면 우리는 사회에서 그 발전에 따른 혜택을 누리는 것이 아니라 뜻하지 않게 소비자 감시의 도구가 남발하게 되는 '감시기반구조'(surveillance infrastructure)를 창조할 수도 있다. Beth Givens, "*Implementing RFID Responsibility: Calling for a Technology Assessment, Testimony submitted to the Federal Trade Commission*", RFID Workshop, Washington, D.C., Radio Frequency Identification: Applications and Implica-

이러한 문제점에 대한 대응방안의 제시를 위하여 이 논문은 RFID가 초래할 수 있는 개인정보 침해의 요소를 분석하고 그에 대한 대응방안을 헌법적인 시각에서 논의하고자 하는 목적에서 출발하고자 한다. 이 논문의 범위는 RFID와 관련된 법적 문제에 핵심에 있는 개인정보보호라는 법적 권리의 구체적 내용 및 RFID 관련 각국의 입법동향을 분석하고 향후 우리나라의 입법방안을 모색하는 것까지 이다.

이 논문의 제2장에서는 RFID의 특성이 개인정보에 어떠한 영향을 미치는 영향과 규제적 접근방식을 고찰하기로 한다. 제3장에서는 RFID가 초래할 수 있는 개인정보의 헌법적 침해와 관련하여 프라이버시와 개인정보의 관계 및 개인정보자기결정권을 검토하고자 한다. 또한 제4장과 제5장에서는 RFID 개인정보보호에 관한 각국의 입법적 대응방안을 분석한 후, 우리나라의 입법방안을 구체적으로 논의하기로 한다.

2. 유비쿼터스 사회에서의 RFID와 개인정보 침해의 위협

가. RFID의 정의

RFID의 정의에 대하여는 각 기관 및 연구단체마다 차이를 보인다.[62] 국외에서는 EPCglobal의 경우 RFID를 “무선 신호를 보내는 태그와 그 신호를 받는 판독기를 포함한 기술”로 정의하고 있다.[63] RFID는 사람, 자동차, 화물, 가축 등에 개체를 식별

---

tions for Consumers (2004. 6. 21.).

62) 우리나라 정보통신부는 u-센서 네트워크 서비스로서 RFID를 정의하고 있는데, 이는 “사물에 전자태그를 부착하고 각 사물의 정보를 수집/가공함으로써 개체 간 정보교환, 측위, 원격처리, 관리 등의 서비스를 제공하는 것”으로 정의하고 있으며, 산업자원부는 RFID에 대해 “제품에 부착된 칩의 정보를 주파수를 이용해 읽고 쓸 수 있는 무선 주파수 인식으로 사람, 상품, 차량 등을 비 접촉으로 인식하는 기술”로 정의하고 있다. 국내 연구기관의 정의로는 IITA의 경우 “Micro-chip을 내장한 Tag, Label, Card 등에 저장된 Data를 무선 주파수를 이용하여 Reader기에서 자동 인식하는 기술”로 정의하고 있으며, ETRI는 “무선 주파수를 사용하는 소형 IC칩을 사용하여 비 접촉으로 사물을 인식하는 기술로서, 사물의 위치파악 및 경로추적을 통해 기업에게 실시간으로 제품의 상황에 관한 정보를 전달할 수 있는 기술”로 설명하고 있다. 이은곤, “RFID 확산 추진현황 및 전망”, 정보통신정책 제16권 제6호, 2면 참조.

하는 정보를 부가하는 시스템으로 그 부가정보를 무선통신 매체를 이용하여 비접촉식으로 해독함으로써 종래 사람의 손에 의지하고 있던 각종 애플리케이션을 자동화할 수 있다. RFID 시스템은 전자태그와 판독기, 미들웨어, 데이터베이스 등의 하드웨어 시스템과, 전자제품코드(Electronic Product Code) 등의 규칙으로 이루어져 있으며, RFID 태그 내의 정보를 비접촉식으로 판독기가 읽어 그 정보를 미들웨어가 필터링을 하여 원격지에 있는 데이터베이스에 저장하는 시스템이다. 판독기가 보내는 전파를 이용해 RFID 태그가 활성화되기 때문에 태그가 별도의 전원을 갖지 않는 것이 일반적이나, RFID 태그 내에 전원이 있는 경우도 있다.[64] 판독기가 보내는 주파수, 전자태그의 저장용량, 전자태그 내의 전원 유무에 따라 전자태그와의 교신 거리, 적용분야, 사용기간 등이 달라진다.

RFID 기술은 사용이 간편하고 여러 개의 RFID 태그를 동시에 인식할 수 있으며 고속인식이 가능하여 시간을 절약할 수 있다. 또한 감지거리가 길기 때문에 시스템 특성이나 환경여건에 따라 적용이 손쉬우며 비교적 응용영역이 넓다는 장점으로 그 활용범위와 시장규모가 확대되고 있다.

나. RFID 기술과 개인정보 침해의 위협

RFID는 물품의 재고관리, 유통과정 추적, 보안, 전자지불 등의 분야에서 획기적인 효율성 향상을 가져오는 것을 가능하게 하여 최근 세계 각국에서는 이 기술을 산업계에 적용하여 기존의 바코드 시스템을 대체하려는 움직임을 보이고 있다.[65]

그러나 RFID는 그 특성상 반도체 칩에 기록된 정보를 제3자가 손쉽고 은밀하게 판독할 수 있고, 장기적으로 태그 정보와 연동된 데이터베이스를 축적·이용할 수 있다는 점에서 개인정보의 침해 가능성이 제기되고 있다. 특히 RFID 태그를 탑재

---

63) 〈http://www.epcglobalinc.org/about/faqs.html#6〉 (2004. 7. 10.).

64) RFID 태그내에 별도의 전원을 가지고 능동적인 통신이 가능한 것을 능동형(active)이라고 하고, 별도의 전원이 있으면서도 수동적으로 통신을 하는 것을 반수동형(semi passive), 별도의 전원이 없고 수동적으로 통신을 하는 것을 수동형(passive)이라고 한다. 〈http://www.ftc.gov/bcp/workshops/rfid/engels.pdf〉 (2004. 7. 1.).

65) "아듀! 바코드, 웰컴! EPC (3) 불붙은 표준과 시장경쟁", 전자신문(2004. 9. 10.) 참조.

또는 부착하여 언제 어디서나 RFID 태그에서 전송되는 정보를 이용할 수 있고, 실시간으로 물건, 사람 혹은 동물의 움직임을 파악하여 상황정보를 분석할 수 있다는 점에서 그 침해 가능성은 가히 놀랄만한 것이라 할 것이다. 또한 RFID의 무절제한 사용으로 고객정보가 무작위로 유출된다면 이 역시 개인정보 보호에 대한 큰 위협이 될 것이다. RFID의 발전에 따른 개인정보의 침해요소들은 다음과 같다.[66]

첫째, 숨겨진 태그의 장소는 개인정보의 중대한 침해요소 중의 하나이다. 이는 RFID 태그는 소유주인 개인들이 알지 못한 상황에서 사물들과 문서에 내장되어질 수 있기 때문이다. 무선전파는 섬유, 플라스틱, 다른 물질들을 쉽게 조용하게 통과할 수 있기 때문에 지갑, 쇼핑 백, 옷가방 등에 들어있는 사물 또는 옷에 부착된 RFID 태그들을 읽을 수 있으며 이는 개인정보 침해의 중요요소가 된다.[67]

둘째, RFID 태그는 전세계 모든 사물들을 위한 유일한 식별자가 될 수 있다. 전자제품코드(EPC)는 지구상에 있는 모든 사물에 자신의 유일한 신분증(ID)을 가지게 할 수 있다. 유일한 식별(ID) 번호의 사용으로 개별의 물리적인 사물이 판매 또는 이전 시점에서 신원이 확인되고, 구매자 또는 소유자와 연결될 수 있는 전세계적인 사물 등록 시스템의 창조가 가능하게 될 수 있다.[68]

셋째, RFID가 야기 할 수 있는 또 하나의 정보 프라이버시 침해요소는 대규모 데이터 통합이다. RFID 배치는 유일한 태그 데이터를 포함하고 있는 대량 데이터베이스의 개발을 요구한다. 따라서 이러한 기록들은 특히 컴퓨터 메모리와 프로세스 능력이 확장되면서, 개인 신원확인 데이터와 연결될 수 있다.[69]

넷째, 숨겨진 판독기(reader) 역시 정보 프라이버시의 위협요소이다. 인간 또는 사물이 모여져 있는 어떤 환경에서도 보이지 않게 섞여질 수 있는 판독기들에 의해 태그들은 시야의 제한 없이 멀리서 읽혀질 수 있다. RFID 판독기들은 이미 실제로

---

66) 이용필, “소비자제품에 RFID 태그 부착에 따른 미국 개인정보 보호단체들의 대응 사례 및 성명서 검토”, 한국정보보호진흥원 TM, 2004. 2.; 〈http://www.rfidprivacy.org/papers/givens_paper.htm〉 (2003. 12. 20.).

67) Beth Givens, 전게주 1) 참조.

68) 전게주.

69) 전게주.

바닥 타일들에 내재되어 소비자들이 언제 '스캔'되고 있는지 없는지에 대한 인식을 불가능하게 하고 있다.[70]

마지막으로 RFID는 개인정보의 프로파일로 그 개인을 추적하여 개인정보를 침해한다. 개인적인 신원이 유일한 RFID 태그 번호와 연결되어 있다면 개인들은 인식되지 못하고 프로파일(profile)되고 추적 당할 수 있기 때문에 개인정보보호에 대한 중대한 위협이 된다.[71]

다. RFID 개인정보 침해와 규제적 접근방식

개인정보 침해에 대한 규제적 접근방식은 법으로 정한 집행기관에 의해 수행하는 규제와 산업계에 의한 자율규제로 양분할 수 있다. 자율규제는 소비자 선호에 따라 업체 행동이 결정되는 시장접근법과는 차이가 있다. 순수한 시장접근법에서는 소비자들이 강력한 프라이버시 보호를 실현하고 있는 회사와 사업을 하기를 선호할 것이라 가정한다. 반대로 자율규제는 정부의 전통적인 세 가지 요소인 입법, 집행, 평가에 기반을 두고 있고, 이들 기능들은 정부에 의하기보다는 민간 분야에 의해 수행된다.[72]

입법은 적정한 규칙, 규칙위반시 집행행위의 시작에 의한 강제, 그리고 회사가 프라이버시 규칙을 위반하였는지에 관한 평가와 관련한다. 산업체의 자기규제적 노력에도 불구하고 프라이버시 옹호자들의 주장에 따르면 많은 데이터베이스 소유자들은 공정정보수행(fair information practices)의 원칙을 따르지 않고 있다고 한다. 데이터베이스 소유자들에 의한 공정정보수행의 결여와 함께 다른 프라이버시 이슈들이 존재한다. 특히 인터넷은 기관 또는 단체들이 소비자의 즉각적인 인식 없이 정보를 공개할 수 있게 하였다. 주된 문제는 RFID 의 도움으로 수집된 데이터가 차후 접근당할 수 있고 의도하지 않았던 형태로 사용될 수 있다는 것이다.

RFID와 관련된 전자제품코드 체계(EPC)를 만들고 있는 EPCglobal에서는 가이드

---

70) 전게주.

71) 전게주.

72) 이용필, 전게주 6) 참조; Rakesh Kumar, "*Interaction of RFID Technology And Public Policy*", RFID Privacy Workshop @MIT, (2003. 11. 15.) 발표자료 참조.

라인을 제시하였다.[73] 이 가이드라인에는 소비자 공지, 소비자 선택, 소비자 교육과 수집된 정보에 대한 정책을 웹 사이트나 별도로 발표하도록 하고 있으며, 2005년 1월 1일부터 적용할 것을 명시하고 있다.

MIT Auto-Id의 자기규율적 프레임워크를 따르면서 Simson Garfinkel은 RFID의 상업적인 배포를 위한 자발적인 5가지 권리[74]를 담고 있는 일련의 원칙인 'RFID 권리장전'을 제안하였다. 이 장전의 정신은 미국 소비자보호단체인 CASPIAN에 의한 '2003년 RFID 알권리법안'에도 유사하게 담겨졌다. 제안에는 제품이 RFID 태그를 포함할 때 소비자들에게 알릴 수 있는 강제적 표식(mandatory labeling)을 요구한다. 여기에는 회사들이 칩을 개인식별정보로 연결하는 것을 또한 금지한다.

향후 제조업자, 공급업자, 또는 소매업자들은 완전한 프라이버시 문제를 보장하는 정책과 절차와 같은 모든 측면을 포괄하고, 이러한 정책들이 소비자 사이에 더욱 폭넓게 가용하도록 하는 종합적 프레임워크를 생산할 필요가 있으며, 현재 발표된 가이드라인들은 RFID의 발전에 따라 수정 보완될 것으로 보인다.

3. RFID 개인정보보호에 관한 헌법적 고찰

가. 헌법상 개인정보보호와 프라이버시

처음 미국에서 프라이버시권이 등장했을 때, 이는 혼자 있을 권리라는 소극적 권리로서 불법행위 법리로 해석하였다. 그러나 정보기술의 발달로 종래의 소극적 프

---

73) EPCglobal 에서는 Public Policy Steering Committee를 구성하여 RFID의 진화에 따른 프라이버시 침해 가능성에 대응하도록 하고 있다.
〈http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html〉.

74) 'RFID 권리장전'의 구체적인 내용은 다음과 같다.
1) RFID 태그를 붙인 제품에 대해 소비자의 알 권리
2) 구매시 태그 기능을 제거 또는 정지시킬 권리
3) 소비자가 RFID 태그와 관련된 데이터에 접근할 수 있는 권리
4) RFID 태그의 강제적 사용없이 서비스를 접근할 권리
5) RFID 태그에 있는 데이터에 언제, 어디서, 왜 접근하는지 알 권리
〈www.simson.net/clips/2002.TR.10.RFID_Bill_Of_Rights.pdf〉.

라이버시권 개념에 대한 재검토가 논의되게 되었고, 적극적 의미로서 프라이버시권 개념이 등장하였다.[75] 이는 개인이 사회에서 살아가기 위해서는 사회에 의한 간섭을 받지 않는 비밀의 영역이 불가결한 것이고 그러한 의미에서 개인에게는 자기에 관한 개인정보를 자기가 통제할 수 있는 권리가 인정되어야 한다는 것이다. 따라서 프라이버시권에는 남에게 알리고 싶지 않은 일정한 사적인 개인정보에 대하여 개인정보의 수집, 개인정보의 이용·제공, 개인정보의 유지·관리의 각각의 수준에서 정보주체에 의한 통제의 권리가 보장되어야 함과 동시에, 그 권리들의 실효성을 확보하기 위해 개인정보의 열람청구권, 정정청구권 등을 인정하여야 함을 의미한다.[76]

이러한 프라이버시 개념의 정의에 대해서는 다양한 입장들이 존재한다. 미국의 프라이버시는 복합적인 개념으로서 한마디로 정의하기가 어렵다.[77] 그러나 미국에서 프라이버시 일반적으로 다음의 네 가지 논의로 정리할 수 있다. 첫째, 개인의 데이터를 통제하고 취급하는데 관련한 정보 프라이버시(information privacy), 둘째, 침해행위에 대한 개인신체의 존엄성과 관련한 신체적 프라이버시(bodily privacy), 셋째, 다양한 통신형태로 의사소통하는 개인의 이해관계와 관련한 통신 프라이버시(privacy of communications), 넷째, 특정공간이나 영역으로의 침입을 제한하거나 경계설정과 관련한 영역적 프라이버시(territorial privacy)이다.[78]

프라이버시 옹호자들은 프라이버시를 하나의 재산으로 정의한다.[79] UCLA 법대

---

75) 졸고, "미국에서의 인터넷 프라이버시 보호와 프라이버시 에스크로 시스템에 관한 연구", 헌법학연구 제8집 제4호, 2002, 361－368면 참조.

76) 황인호, "개인정보보호제도에서의 규제에 관한 연구", 공법학회 제30권 제4호, 229－233면 참조.

77) 프라이버시의 이슈에 관하여는 수많은 관점이 있다. Edward Bloustein은 프라이버시를 "신성한 인격, 인간의 자주성, 존엄, 그리고 고결성을 보호하는 인간개성의 한 이해관계"로 묘사한다. Edward J. Bloustein, "*Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*", 39 N.Y.U. L. Rev. 962, 971 (1964).

78) David Banistar & Simon Davis, Privacy and Human Rights: An International Survey of Privacy Laws and Practice 〈http://www.gilc.org/privacy/survey/intro.html〉.

79) Paul Rose, "*A Market Response to the European Union Directive on Privacy*", 4 UCLA

Jerry Kang 교수는 “프라이버시 옹호자들은 개인이 개인정보를 명백히 소유한다고 주장한다. 따라서 정보수집가들은 허가없이 그 재산을 사용해서는 안될 것이다. 정보수집가들은 개인과 정보수집가의 동등한 참가자로 상호작용하면서 정보가 전송된다고 반박한다”[80]는 점에 주목한다.

개인정보에 대한 재산권을 주장하는 사람들은 정보에 특별한 가치를 부여한다. 융자를 얻거나 신용거래의 지원, 전화서비스 신청과 같은 전형적인 거래들은 개인들이 전송된 개인정보의 가치에 대하여 거래당사자와 분쟁을 만들면서 비능률적이고 복잡해질 것이다.[81] 이러한 재산권 접근방식은 비실제적으로 보일 수 있기 때문에, 익명기술은 평범한 사람들에게 사용가능한 프로파일의 거부를 위한 유일한 기술이 될 수도 있을 것이다.[82]

프라이버시의 범위 내에서는 여러 가지 사실들이 발생하게 되며 그러한 사실들은 여러 가지 기록을 남기게 되는 바 그 사실들의 기록은 서로 종합되고 저장되어지게 된다. 예를 들어, 범죄경력기록, 질병기록, 매매기록, 신용카드사용기록, 휴대전화사용기록 등의 사실들이 발생하고 이러한 사실들이 기록이라는 형태로 남겨지고 이러한 기록이 포착되어 종합되고 집적되고 관리되어 가치를 갖게되고, 가치를 가짐으로서 유출의 대상, 매매의 대상이 되는 것이다. 이것이 바로 프라이버시가 개인정보로 바뀌어 정형화되어 가는 모습이다. 프라이버시는 본래는 포착될 수 없는 사적 영역의 사건이었지만, 그것이 기록 가능한 정보의 형태를 취하게 됨으로써 개인정보로 바뀌는 것이다. 따라서 개인정보는 프라이버시의 발현형태라고 할 수 있으며 프라이버시가 정보라는 형태를 취해 외형적으로 나타남으로써 취급 및 관리가 가능한 것이 되는 것이다.[83]

J. Int'l L. & For. Aff. 445, 451 (1999).

80) Jerry Kang, “*Information Privacy in Cyberspace Transactions*”, 50 Stan. L. Rev. 1193, 1246 (1998).

81) A. Michael Froomkin, “*Regulation of Computing and Information Technology: Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*”, 15 J. L. & Com. 395, 492 (1996).

82) 전게논문.

프라이버시권의 헌법상 근거에 대해서는 현행 헌법이 제17조(사생활의 비밀과 자유)를 두어 프라이버시와 관련된 규정을 두고 있다. 그 밖에도 현행 헌법 제10조(인간의 존엄성 존중 조항) 및 헌법의 제12조의 신체의 자유, 제16조의 주거의 자유, 제18조의 통신의 자유, 제21조제4항의 타인의 명예나 권리침해방지, 제36조제1항의 혼인과 가족생활에 있어서의 개인의 존엄과 평등 등이 프라이버시권의 근거 규정과 관련이 있고, 뿐만 아니라 제37조 제1항(헌법에 열거되지 아니한 자유와 권리의 존중 조항)도 프라이버시권의 헌법상 근거가 될 수 있다고 한다.[84)]

나. 인격권, 사생활의 비밀과 자유와 프라이버시권과의 관계

먼저 인격권은 헌법 제10조(인간의 존엄성 존중), 제17조(사생활의 비밀과 자유), 제37조제1항(헌법에 열거되지 아니한 자유와 권리의 존중) 등을 근거로 보장된다고 한다. 사생활의 비밀과 자유에 관한 권리에는 ① 사생활 비밀의 불가침, ② 사생활 자유의 불가침, ③ 자기정보의 관리통제와 같은 권리 등을 그 내용으로 하는 복합적 권리라고 하고 있다. 프라이버시권을 제2설로 해석할 경우 사생활의 자유와 비밀에 관한 권리와 같다고 볼 수 있다. 따라서 인격권, 프라이버시권, 사생활의 자유와 비밀에 관한 권리와의 관계에 다음과 같이 표현할 수 있다.[85)]

이렇게 할 경우 프라이버시권의 내용은 적어도 사생활의 비밀과 자유에 관한 권리와 같은 권리이거나, 더 폭넓은 개념이라고 정의할 경우 그 내용에는 사생활 비밀의 불가침, 사생활 자유의 불가침, 자기정보의 관리통제와 같은 권리가 포함되어 있다고 할 수 있다.

첫째, 사생활 비밀의 불가침은 자신에 관한 비밀을 공개당하지 않을 권리로 사적 사항, 명예나 신용 등을 훼손 내지 공표 당하지 않을 권리 등과 본인을 나타내는 징표가 도용되지 않을 권리 등을 말한다. 둘째, 사생활 자유의 불가침은 사생활의 자유로운 형성과 전개를 방해받지 않을 권리로서 자신이 원하는 바에 따라 사생활을

---

83) 황인호, 전게주 16), 232면 참조.

84) 전게논문.

85) 정연수, "「개인정보보호법」인가, 아니면 「프라이버시보호법」인가", 프라이버시 보호법제의 규율대상과 범위 워크샵 자료(2003) 1－2면 참조.

자유로이 형성하고 전재할 수 있도록 법적 안전성과 행동의 자유를 보장하는 것이다. 예를 들면 취미생활이나 주거의 형태를 강제하거나 타인의 전화 등을 도청하는 행위 등이 사생활의 자유를 침해하는 행위이다. 셋째, 한편 자기정보의 통제관리라 함은 자신에 관한 정보를 보호하기 위하여 자신에 관한 정보를 자율적으로 결정하고 관리할 수 있는 권리를 말한다.

다. RFID와 개인정보자기결정권

개인정보자기결정권이란 자신에 관한 정보가 언제 어떻게 그리고 어느 범위까지 타인에게 전달되고 이용될 수 있는지를 그 정보주체가 스스로 결정할 수 있는 권리를 의미한다.[86] 헌법상의 인권으로서의 자기결정권은 자신의 책임에 속하는 문제를 스스로 결정하는 권리를 말하며 그밖에 '독특한 생활방식' 또는 '위험의 각오'라는 특징을 갖는다. 자기결정권과 그 밖의 권리간에 명확한 경계를 설정하기는 어렵지만, 자기결정권이 자유나 행복추구권과 같은 것은 아니다.

자유나 행복추구권 중에는 자기결정권 이외에 인격가치에 속하는 권리, 예컨대 명예권 등도 포함된다. 이러한 자기결정권은 헌법 제10조 이외의 조문(단독으로 또는 제10조와 결합하여)에 근거로 둔 것으로 보기도 하지만[87] 헌법 제10조 행복추구

---

86) 독일 연방헌법재판소는 1983년의 인구조사판결에서 '정보적 자기결정권'이라고 명명하였다. 우리의 경우 용어가 통일되어 있지 않은데, '자기정보관리통제권' 또는 '개인정보자기결정권'(권영성, 헌법학원론, 법문사, 2001, 427면), '자기정보에 대한 통제권'(성낙인, 헌법학, 법문사, 2001, 439면), '자기정보통제권'(차맹진, "프라이버시와 자기정보통제권", 인하대 박사논문, 1991), '정보자기결정권'(김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 공법연구 제29집 제3호, 한국공법학회, 2001) 등으로 다양하게 용어를 쓰고 있다. 미국은 정보 프라이버시(information privacy)라고 부르기도 한다. Jerry Kang, 조규범 역, 사이버스페이스 프라이버시, Jinhan M&B, 27면. 이인호, "전자정부에서 정보프라이버시의 실현과제", 국가인권위원회 토론회 자료집 (2003. 8. 19.) 12면; 이인호, "개인정보자기결정권의 한계와 제한에 관한 연구", 한국정보보호진흥원, 2001, 23면 참조.

87) 허영 교수는 행복추구권은 다른 기본권에 대한 보충적 기본권으로 될 뿐 행복추구권의 독자적인 기본권성은 인정될 수 없다고 한다. 한국헌법학신론, 박영사, 2001, 320－321면 참조.

권에서 근거를 두고 있는 것으로 보아야 하며,[88] 자유권적 성질과 청구권적 성질을 갖는다.

판례의 경우 헌법 제17조에 보장된 '사생활자유'의 적극적 해석 및 개인정보자기결정권의 도출에 긍정적이다.[89] 그러나 헌법재판소의 경우에는 약간 다른데, 헌법상 보장된 '사생활자유'에 관하여 나름대로 언급하고는 있으나, 아직까지는 개인정보자기결정권의 헌법상 근거나 그 내용 등에 관하여 구체적으로 설명하고 있지는 않다.[90]

RFID를 관리하고 정보를 취급하는 주체에게 개인정보자기결정권을 행사하기 위해서는 이 권리가 미치는 효력범위, 즉 정보주체가 타인의 어떠한 개인정보처리에 대한 통제권을 행사할 수 있는가가 문제된다. 개인정보자기결정권은 개인인격의 구성요소들이 전자적 형태로 기록화됨으로써 정보주체의 총체적인 인격상이 타인의 수중에 들어가는 위험성을 사전에 차단하기 위해 요구되는 기본권이므로 이같은 위험성이 없는 개인정보의 수집·처리에 대해서는 개인정보자기결정권의 효력이 미치지 않는다고 보아야 한다.

보호객체가 되는 개인정보는 '신원을 확인할 수 있는 자연인에 관한 일체의 정보'를 말한다. 따라서 신원을 확인할 수 없는 형태로 수집·처리되는 어떤 자연인에 관한 정보는 개인정보에 해당하지 않는다. 그러나 이같은 비신원확인정보라도 그 속에 개인의 인격적 특성이 담겨 있게 되고, 다른 개인정보들과 결합하여 쉽게 신원확인이 가능한 비신원확인정보도 개인정보자기결정권의 보호대상이 된다고 할 것이다. 또한 1차 수집된 자료들을 분석하여 얻은 개인에 관한 2차 정보도 당연히 개인정보자기결정권의 효력이 미치는 개인정보에 해당된다.

한편, 개인정보자기결정권의 보호대상이 되는 "개인정보"는 공개적으로 이루어지

---

88) 학설상으로는 정보의 자기결정권을 헌법 제21조의 표현의 자유에서 찾는 입장도 있다. 박종보, "정보공개제도와 알권리", 공법연구 제28집 제1호, 7－8면; 권영성, 헌법학원론, 법문사, 2000, 429면.

89) 대판 1998. 7. 24. 96다42789 및 서울고법 1995. 8. 24. 94구39262 참조.

90) 헌재 1999. 9. 10. 89헌마82, 헌재는 '행복추구권'으로부터 '성적 자기결정권'을 도출하고 있다. 김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 한국공법학회 제94회 학술발표회 자료, 2001, 100면 참조.

는 개인의 행동에 관한 정보도 지속적이고 체계적으로 수집·처리되고 다른 개인정보들과 결합되는 경우 개인의 전체적인 인격성이 쉽게 드러날 수 있기 때문에 헌법 제17조의 "사생활비밀의 불가침"조항 및 제18조의 "통신비밀의 불가침"조항에서 보호하는 개인의 "비밀"보다 넓은 개념이다.

정보주체의 개인정보자기결정권이 자의적으로 침해되지 않기 위해서는 정보주체에게 통상 익명권, 정보처리금지청구권, 열람 및 갱신청구권, 정보분리청구권이 보장되어야 한다. 이러한 권리의 행사는 네트워크이용관계에 있어 경제적으로나 지적인 면에서 약자인 정보주체에 대해 충분한 설명 내지 위험에 대한 설득을 전제하여야 하며(소위 Informed Consent), 이를 전제하지 아니한 정보제공 동의나 이용관계의 설정은 정보주체의 정보자기결정권에 대한 침해로 새겨야 할 것이다.

첫째, 익명권은 정보주체가 국가 등의 제3자와 교섭 또는 거래를 할 때 불필요하게 자신의 신원을 밝히지 않을 권리를 말한다. 특히 신용카드를 이용해 RFID가 부착된 제품을 구매하는 경우 신용카드에 의해 자신의 신원 노출되면서, RFID와 개인의 신원이 연결된다는 점에서 익명성은 중요한 문제가 될 수 있다.

둘째, 정보처리금지청구권은 기본적인 정보처리원칙이 충족되지 않는 경우에 개인정보의 수집, 이용, 제공 등의 정보처리를 금지하도록 요구할 수 있는 권리이다. 이러한 정보처리금지청구권의 인정여부를 판단하기 위한 기준으로서 정보처리에 관한 3가지 원칙을 들 수 있다. '수집제한의 원칙',[91] '목적구속의 원칙',[92] '시스템공개의 원칙'[93]이 요구된다.

---

91) 수집단계에서부터 개인정보자기결정권의 보장이 이루어져야 하는데 "(ⅰ) 정당한 수집목적, (ⅱ) 필요한 범위 내에, (ⅲ) 공정하고 합리적인 방식으로, (ⅳ) 정보주체의 분명한 인식 및 동의 하에 수집되어야 한다"는 원칙이다.

92) 목적구속의 원칙이란 "개인정보를 수집하는 목적은 (ⅰ) 수집 당시에 명확히 특정되어 있어야 하고(목적의 특정성), (ⅱ) 그 후의 이용은 이 특정된 수집목적과 일치되어야 한다(목적일치성)"는 원칙이다. 이 원칙에서의 이용은 제3자 제공은 포함되지 않고, 수집기관 내부의 자체 이용만을 의미한다. 제3자 제공의 경우에는 수집제한의 원칙과 목적구속의 원칙이 별도로 적용된다고 할 것이다.

93) 시스템 공개의 원칙이란 "개인정보처리시스템의 설치 여부, 설치목적, 정보처리방식,

셋째, 정보열람권과 정보갱신청구권이 인정되어야 한다. 이것은 타인에 의해 처리되고 있는 개인정보의 내용에 대해 정보주체가 이를 열람하여, 그 정확성과 최신성 및 완전성을 유지하도록 요구할 수 있는 권리이다.

넷째, 정보분리청구권이 보장되어야 한다. 특정 목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 통합되지 않고 분리된 상태로 유지될 것을 요구하는 권리이다.

RFID 시스템에 대해서도 이러한 익명권, 정보처리금지청구권(수집제한의 원칙, 목적구속의 원칙, 시스템공개의 원칙), 정보열람권과 정보갱신청구권, 정보분리청구권은 동일하게 적용될 것이다.

라. RFID와 개인정보자기결정권의 한계

프라이버시권을 보호하기 위한 한 방안으로서 개인정보자기결정권을 보장하는 것으로 개인정보 보호가 만족할 만큼 보장되는지는 의문이다. 전형적인 국가 활동에 있어서 감시감독은 주요한 수단이 되며, 이러한 시스템이 유지되기 위해서 핵심적인 요소는 정보로, 행정국가의 관리 능력은 사회 전반에 대한 광범위한 지식정보의 관리에 달려 있다.[94] 당근과 채찍정책처럼, 자발적으로 원형감옥(panoptic gaze) 하에 남아있는 이들에게는 인센티브(소득, 복지혜택 등)가 주어지는 반면, 이러한

처리정보의 항목, 시스템운영책임자, 처리시스템에 의한 자동결정이 이루어지는지 여부 등이 일반에게 투명하게 공개되어야 한다"는 원칙이다. 이 시스템 공개의 원칙은 정보주체의 열람청구권과 갱신청구권 행사의 전제가 된다.

94) 근대시민국가에서는 그 성립의 목적이 된 독립성을 가진 개인들에 대한 정보를 필요로 하였다. 상비군의 구성원이 될 개인들의 신상을 파악하기 위하여, 국가재정의 근간이 될 조세의 징수원을 확보하기 위하여, 관료에 의한 합리적인 국가경영을 위한 기초정보를 확보하기 위하여, 개인의 요구사항과 그 정치과정에서의 실현을 위하여 개인들의 정보를 수집・처리・유지하여야 했다. 결국 자유롭고 독립된 개인의 지위를 확보하기 위한 근대시민국가의 성립은 역설적으로 개인의 정보에 대한 국가의 통제력을 강화하는 방향으로 진행되었다. 또한 복지국가 하에서는 개인의 후견자로서 국가의 위상을 보편화시켰으며 후견활동의 효율을 위해 국가는 개인의 생활을 총체적으로 감시하는 체제의 성격을 가지고 있다. 김종철, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론", 인터넷법률 제4호, 2001, 23－44면.

범위에서 벗어나는 이들에게는 제재가 가해진다. 공공・민간 부분의 거대조직에서는 예방이 사후 처벌보다 보다 효과적이고 사회적으로 덜 파괴적이라는 점에서 자본주의하의 기업이 투자에 대한 미래수익에 관심을 두듯이 감시적(panoptic)국가도 미래지향적이고 정보의 예측력에 주의를 기울인다.[95]

기존의 개인정보통제권에 대한 논의는 본질적으로 사생활보호에 바탕을 둔 프라이버시권의 우산하에 논의됨으로써, 정보사회의 진전에 따라 개인정보보호로 그 외연이 확대되어 왔음에도 불구하고 그 정당성을 개인의 인격성의 보호나 자율성의 보호라는 사생활영역의 보장에 한정시킴으로써 일상화된 정보관리에 대한 적극적 통제나 정치 및 경제권력에 대한 견제권으로서의 정치적, 헌법적 의미를 담보하기에는 미흡하다는 지적이 있다.[96]

즉, 소극적 프라이버시권뿐만 아니라 자기정보통제권이라는 적극적 프라이버시권에서도 개인의 정치적 의사형성과 사회적 자율성의 전제로서 기본적으로 사적 성격의 개인정보를 보호하여야 한다는 발상에 근거하고 있으므로 그 기본전제가 사생활보호에 천착하고 있는 점에서는 소극적 프라이버시와 동일하다는 한계를 지니고 있다고 한다.

이에 반해 새로운 개인정보통제권은 자신의 정보가 어떻게 수집, 처리, 관리, 이용되는지에 대한 감독권을 의미한다. 사생활보호의 차원에서의 개인정보란 절대적 보호되는 것이 아니며 그 경계도 자연적으로 정해지는 것이 아니라 정치과정을 통해 재조정되는 유동적인 것이다. 공동체의 운영과 직접적으로 관련이 없는 정보는

---

95) Reg Whitaker, The end of privacy－How Total Surveillance Is Becoming A Reality, New York, 1999.

96) 일부에서 적극적 개인정보통제권의 헌법적 의의를 인간의 존엄성 확보외에도 자유민주적 기본질서의 유지에서 찾으려는 시도가 없었던 것은 아니다. 예를 들어, 성낙인 등, “개인정보보호를 위한 정책방안 연구”, 정보통신부, 1999, 25－26면 참조; 그러나 이 경우에도 Big Brother로서의 국가의 역량강화가 자유민주적 기본질서의 기본적 전제조건으로서의 국민의 개인적 사회적 자율성의 확보를 위한 것으로 인식하였다. 이 인식은 궁극적으로 인간의 존엄성 보장논리와 다르지 아니하여 단순한 개인의 자율성 ‘보호’를 넘어 권력행사에 대한 적극적 ‘통제권’으로서의 새로운 개인정보통제권의 의미를 인식하는데 한계를 보인다. 김종철, 전게논문, 28면 참조.

개인의 인격성의 보호라는 전통적 프라이버시의 보호 차원에서 계속 프라이버시권의 보호를 받을 수 있지만 공동체의 운영상 필요에 의해 일정한 개인정보의 수집은 적법한 절차적, 실체적 권리를 인정하는 것이 필요하다. 그리고 이 권리는 단순히 사생활 보호의 측면에서가 아니라 정보활용권을 가지는 정치적, 사회적 권력체에 대한 민주적 통제와 감시권으로서 새로이 인식할 필요가 있는 것이다.[97]

4. RFID 관련 각국의 입법동향

가. 미국

1) 미국 소비자단체 CASPIAN의 RFID알권리법안

미국의 시민단체중 하나인 '수퍼마켓의 프라이버시 침해에 대한 소비자 단체'(CASPIAN)[98]은 2003년 6월 11일 '2003년RFID알권리법안'[99]을 제안하였고, 동년 8월에는 캘리포니아주 의원 등에 RFID의 프라이버시 침해 위협 가능성 및 이슈에 대한 설명회를 개최하였다.[100]

이 법안의 제1장은 법안의 이름을 규정하고 있으며, 제2장에서 제5장까지는 음식, 약품, 화장품, 알콜, 담배의 경우 무선인식태그(RFID tag)를 장착한 제품에는 이를

---

97) 따라서 개인정보통제권을 개인정보의 사용과 공개에 관한 권한 권리로 파악하는 기존의 입장에서 공개에 관한 권리는 사생활보호권으로 계속 유지시키고 사용에 관한 통제권만을 개인정보통제권으로 파악하는 셈이다.

98) CASPIAN은 미국 수퍼마켓 소비자 인권침해 단체인 Consumer Against Supermarket Invasion And Numbering의 약자로 1999년 이래로 수퍼마켓 등의 소비자 감시에 대항하는 순수 민간의 소비자 그룹이며, 미국 50개 주의 구성원들과 세계 20여 개 나라에서 참여하고 있다. CASPIAN은 소비자제품에 RFID을 도입하고 있는 경우 의무적으로 이를 알리도록 하는 "2003년 RFID 알권리법"이라는 법안을 마련하여 입법을 요구하고 있다. 이 법안은 원격 감시장치가 내장된 제품을 의식하지 못하면서 구매하는 소비자들을 보호하려고 한다. 자세한 내용에 관하여는 〈http://news.com.com/2100-1029_3-5065388.html?tag=st_rn〉 참조.

99) 2003년 알권리법안(RFID Right to Know Act of 2003)이 포함하는 세부적인 조항에 대하여는 〈http://www.nocards.org/rfid/rfidbill.shtml〉 참조.

100) 〈http://news.com.com/2100-1029_3-5065388.html?tag=st_rn〉 참조.

고지하는 라벨을 표기해야 함을 규정하고 있다. 또한 제6장은 소비자의 프라이버시를 보호하기 위한 조항들과 소비자와 사업자 교육에 대한 내용을 포함한다. 법안은 RFID 태그가 부착되어 있는 제품의 경우 이를 소비자가 알 수 있도록 공지하는 내용 이외에도 제6장에서는 소비자의 프라이버시를 보호하기 위한 조항들과 소비자와 사업자 교육에 대한 내용을 구체적으로 포함하고 있다.

2) 미국 소비자보호단체들의 RFID 성명서

상술한 미국 '수퍼마켓의 프라이버시 침해에 대한 소비자 단체'(CASPIAN)의 법안 제시와 더불어 최근 미국에서는 소비자단체들을 중심으로 RFID의 기술 특성상 프라이버시 침해 위험이 높은 현실과 이에 대한 보호방안이 불투명한 상태에서 RFID의 전면적인 도입에 대한 반대운동을 전개하고 있다. 이의 일환으로 2003년 11월 14일, 미국의 개인정보보호 단체들은 공동으로 소비자 제품에 RFID를 사용하는 것에 대한 성명서[101]를 발표하였다. 이번 성명서는 앞서 살펴본 '슈퍼마켓의 프라이버시 침해에 대한 소비자 단체'(CASPIAN), 전자프라이버시정보센터(Electronic Privacy Information Center; EPIC) 등 8개 단체가 공동으로 발간하였고, 세계 19개 단체가 후원을 했으며, 미국 및 세계 개인정보보호 관련 대표자 46명 등이 서명을 했다.[102]

발표된 성명서는 성명서 본문과 2개의 부록으로 구성되어 있다. 성명서 본문에서는 RFID에 대한 간단한 소개와 RFID의 어떤 특성이 프라이버시와 자유에 대한 위협을 주는지를 설명하고, 이러한 RFID를 사용하는데 있어서의 권리와 책임의 기반 구조를 제안하고 있다. 이어서 첫 번째 부록에서는 RFID의 한계점 등으로 인해 RFID의 프라이버시 침해위협은 크지 않다는 주장에 대해 그 반론을 제기하고 있고,

---

101) Position Statement on the Use of RFID on Consumer Products(2003. 11. 20.), 이 성명서에 참여한 단체는 후게주 참조.

102) 성명서 발표에 참여한 단체들은 '수퍼마켓의 프라이버시 침해에 대한 소비자 단체'(CASPIAN), '프라이버시 권리 정보센터'(Privacy Rights Clearinghouse), '전자 프라이버시 정보 센터'(Electronic Privacy Information Center; EPIC), '정크버스터즈'(Junkbusters), '미국자유인권연합'(American Civil Liberties Union; ACLU), '메이다 온라인'(Meyda Online), '전자선도재단'(Electronic Frontier Foundation; EFF), '프라이버시 액티비즘'(Privacy Activism) 등이 있다.

두 번째 부록에서는 현재까지 산업계에서 제안한 프라이버시 보안 솔루션들에 대해 비판하고 있다.

성명서에는 RFID의 속성 중에서도 프라이버시와 시민자유에 대한 위협이 되는 부분을 식별하고 있다. 이러한 위협은 1) 숨겨진 태그 장소,[103] 2) 전세계 모든 사물들을 위한 유일한 식별자,[104] 3) 대규모 데이터 통합,[105] 4) 숨어있는 판독기,[106] 5) 개인추적과 식별(profiling)[107]이다.

이 성명서는 결론부분에서 지금까지는 RFID의 효과성과 적용범위의 다양성이 부각되면서 기존 대형 유통업체 중심의 시험적인 적용에서 향후 정부를 중심으로 적극적인 시범사업 추진이 계획되어있거나 착수되고 있음을 지적하고, 권한이 있으면

---

103) 무선인식태그(RFID tag)들은 소유주인 개인들이 알지 못하는 상황에서 사물들과 문서에 내장될 수 있다. 라디오 파장(radio waves)은 섬유, 플라스틱 등을 인식할 수 없는 형태로 통과할 수 있기 때문에 지갑, 쇼핑가방, 옷가방 등에 들어있는 사물 또는 옷에 부착된 무선인식태그(RFID tag)들을 읽을 수 있다. CASPIAN etc., Position Statement on the Use of RFID on Consumer Products 참조 〈http://www.privacyrights.org/ar/RFIDposition.htm〉 (2004. 5. 31. 검색).

104) RFID에 사용되는 전자코드는 지구상에 있는 모든 사물에 자신의 유일한 ID를 가지게 할 수 있다. 유일한 ID 번호의 사용으로 개별의 물리적인 사물이 판매 또는 이전되는 시점에서 신원이 확인되고, 구매자 또는 소유자와 연결될 수 있는 전세계적인 사물등록시스템의 창조가 가능하게 되었다. 전게주 참조.

105) RFID의 배치는 유일한 태그 데이터를 포함하고 있는 대량 데이터베이스의 개발을 요구한다. 이들 기록들은 특히 컴퓨터 메모리와 프로세스 능력이 확장되면서 개인의 신원확인 데이터와 연결될 수 있다. 전게주 참조.

106) 인간 또는 사물들은 판독기에 의하여 시야의 제한 없이 멀리서도 읽혀질 수 있다. RFID 판독기들은 이미 실제로 바닥 타일들에 내재되어 있고, 카펫이나 마루매트에 넣어져 있으며, 문가에 숨겨져 있는 등 소비자들이 언제 '스캔' 당하고 있는지에 대한 인식을 불가능하게 만들고 있다. 전게주 참조.

107) 개인적인 신원이 유일한 무선인식태그(RFID)의 번호와 연결되어 있으면 개인들은 인식하지 못한 상태에서 식별(profile)되고 추적 당할 수 있다. 예를 들어 신발 속에 내재되어 있는 태그는 신발을 신고 있는 사람을 위한 사실적인 인식자로 기능한다. 사물수준의 정보가 일반적인 수준으로 있다 하더라도, 사람들이 입고 있거나 지니고 있는 사물에 대한 식별은 개인들을 정치적인 모임과 같은 특별한 사건과 연결시킬 수 있다. 전게주 참조.

그에 대한 책임도 증가하도록 해야 한다고 주장한다. RFID의 시장활성화를 도모하는 것과 더불어 그 부작용에 대한 고려도 병행하여야 한다. 이를 위해 기술적 특성이 어떠하며, 프라이버시 침해 위협이 어떠한 것인지를 예의주시하고, 자율적 규제나 시장에의 규제 못지 않게 법적, 제도적 장치 등의 정책적 접근과 기술적 접근 등을 더불어 같이 생각해야 하며, 세계 각국이 이를 해결하기 위해 같이 힘써야 할 시점임을 강조한다. 그런 의미에서 이 성명서는 RFID에 대한 사회적 고민의 산출물의 의미로 해석되어질 수 있을 것이다.

3) 캘리포니아 RFID법안

미국 소비자보호단체들의 성명발표와 더불어 캘리포니아주 상원의원 데브라 보웬(Debra Bowen)은 2004년 2월 20일 RFID 상용화와 관련한 소비자 사생활보호 등을 주장한 법안 SB 1834를 제안[108]하였다. 이후 법안은 4월 1일, 6월14일 두차례 수정되어 주상원에 계류중이다.[109] 이 법안은 2개조로 구성되어 있는데, 첫 번째 조항으로 수정된 안은 개인을 식별하기 위한 정보를 수집하고 이용하기 위해 전자태그와 판독기를 사용하기 위해서는 일정한 조건을 준수하도록 하고 있다. 그 조건으로는 법에서 인정한 수준에서만 개인식별정보를 수집할 수 있고(제22650조a항), 개인식별정보는 전자태그가 부착되어 있는 제품을 소비자가 구매하는 경우 거래성사와 관련된 수준의 정보만 제공할 수 있으며(동조b항), 거래 행위 성사 이전 또는 이후에 개인식별정보를 수집해서는 안된다고 규정하고 있다(동조c항). 또한, 수집되는 정보는 실제 구매나 대여를 하기위해 제품을 제시하는 사람과 제품에 대한 것이어야 한다(동조d항). 두 번째 조항은 일반 상점을 대상으로 하는 것 이외에 도서관을 적용대상에 규정하고 있다. 이는 도서관에서는 직접 제품을 판매하는 것이 아니라 책 등을 관리하고, 대출하는 과정이 일반적인 프로세스이므로 RFID를 사용할 경우

108) California Senate Bill, No. 1834로 제안되었으며, 캘리포니아사업및직업규약(Business and Professions Code)의 제8부(Division 8)에 추가하는 형식을 따르고 있다.

109) 최초의 법안은 RFID 전자태그가 소비자 제품에 장착되어 있는 경우에 적용되며, 정보수집과 제3자에게 정보공유를 할 경우 정보주체로부터 서면동의를 받아야 한다고 되어 있다. 또한, RFID 시스템 태그는 소비자가 그 상점을 이탈하기 이전에 분리 또는 파기하도록 되어 있었다.

많은 도움을 받을 수 있는 부분으로 여겨지고 있다.

4) 유타주 RFID알권리법안

미국 캘리포니아 상원의원 보웬(Bowen)이 RFID프라이버시법안을 의원 입법안으로 제안(Senate Bill 1834, 2004. 2. 20.)[110]한 이후, 유타주에서도 하원의원 호이그(Hogue)의 제안 하에 'RFID알권리법안'이 하원의회를 통과하였다.[111] 유타주의 'RFID알권리법안'의 구조를 살펴보면 RFID과 관련된 조항을 규정하기 위해 '유타주소비자판매행위법'(Utha Consumer Sales Practices Act)을 개정하고 있음을 알 수 있다.[112]

유타주 'RFID알권리법안'에서의 프라이버시에 관한 규정을 살펴보면 다음과 같다. 즉, 1) 제품 판매전인 판매점 안에서도 소비자 프라이버시를 보호하기 위해 사업자에게 제품에 부착되어 있거나 패키지에 부착된 RFID 태그가 리더기에 정보를 제공할 수 있음을 소비자에게 사전에 고지하고, 2) 고지하는 방법으로 전시 제품 주위와 판매대에 로고로서 하거나, 눈에 잘 띄는 다른 방법으로 하도록 하고 있으며, 3) 소비자가 원하지 않는 한 제품 판매 완성 시점 이전에 RFID 태그의 기능을 정지시킬 것을 요구하고 있다.

표에서 살펴본 바와 같이 유타주에서는 RFID 태그로부터 개인식별정보의 수집 자체에 관해서는 별다른 규정을 하고 있지 않다. 유타주에서는 RFID 관련 내용을 고지하고, 태그 기능을 정지시킬지 여부에 대해 소비자에게 선택권을 주도록 하고 있고, 판매완료시점 이전에 태그의 기능을 정지시킬 수 있도록 함으로써 판매완료시점에 개인식별정보와 제품과의 연계를 끊도록 하고 있는 특징을 보이고 있다.

유타주의 RFID 알권리법안은 미국 캘리포니아주에 이어 두 번째 입법으로써 RFID 관련 입법안이 다른 주로 확산될 가능성을 보여주고 있다. 캘리포니아주 입법안과 차이가 나는 것은 판매완료 시점 이전에 무선인식태그(RFID tag)의 기능을 정

---

110) 졸고, "캘리포니아주 RFID 관련 프라이버시 법안－SB 1834", 한국정보보호진흥원 전자거래보호 이슈리포트, 제1권 제4호(2004) 참조.

111) 유타주 하원의원 입법안(House Bill) 251(2004. 2. 23.).

112) 이 법안의 제1조는 항목을 정의하고 있고, 제2조는 공급자에 의한 기만 행위들에 대한 구체적인 예들을 열거한다. 그리고 제3조는 시행일을 규정하고 있다.

지시키도록 하고 있으며, 기능 정지에 대해 소비자 선택권을 명시적으로 규정하고 있는 점이다. 국내에서도 RFID 관련 입법을 준비하면서 규제를 어느 수준으로 어느 시점까지 해야 하는지, 소비자 선택권을 어디까지 보장해야 하는지에 대한 다양한 검토사항이 이루어져야 할 것이다.

5) EPCglobal의 공공정책가이드라인

EPCglobal 에서는 공공정책조정위원회(Public Policy Steering Committee)를 구성하여 RFID의 진화에 따른 프라이버시 침해 가능성에 대응하도록 하고 있다. EPCglobal의 공공정책가이드라인은 소비자 고지(Consumer Notice), 소비자 선택(Consumer Choice), 소비자 교육(Consumer Education), 수집된 정보에 대한 정책을 웹 사이트나 별도로 발표(Record Use, Retention and Security)하는 등 4가지 원칙을 제시하고 있다.[113] 이러한 공공정책가이드라인은 2005년 1월부터 적용할 예정이며, EPCglobal 회원사의 테스트 단계에서 적용중이다.[114]

나. 일본

1) 일본 경제산업성의 가이드라인 초안

일본은 유비쿼터스 환경에 대해 1980년대부터 사카무라겐 교수를 중심으로 적용방법에 대해 연구해 왔으며, EPCglobal과 별도로 독자적인 상품코드체계를 개발하여 추진하고 있고, 이를 시범사업에 연계하여 산업계에 적용하기 위해 노력하고 있다. 이러한 노력과 더불어 2003년부터 개인정보보호차원에서 RFID의 문제에 대해서도 준비해 온 것으로 보인다. 일본은 「개인정보보호에관한법률」(2003. 5. 23. 제정, 이하 "개인정보보호법"이라 함)을 제정한 후 RFID를 통한 정보에 개인정보보호법에서의 개인정보에 포함되지 않는 부분이 있다하더라도 개인프라이버시에 침해위협이 될 수 있다고 인식하고, RFID 프라이버시 보호 가이드라인을 준비하였다.

일본은 경제산업성이 주도하여 「상품 유통관리의 향상에 관한 연구회」(경제 산업성 주최, 국토 교통성, 농림 수산성, 후생 노동성이 참가)를 만들어, 2003년 12월 22

113) 〈http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html〉.

114) 〈http://www.ftc.gov/bcp/workshops/rfid/board.pdf〉.

일에 “RFID 기술에 관한 프라이버시 보호 가이드라인(안)”을 정리하였고, 2004년 1월 21일에 이를 발표하였다. 가이드라인의 주요내용을 보면 다음과 같다.[115)]

가이드라인의 대상사업자는 소비자에게 물품이 교부된 후에도 해당 물품에 전자태그를 장착해 두는 경우 해당 전자태그 및 해당 전자태그가 장착된 물품을 취급하는 사업자이다(제2조). 일단 소비자가 물품을 구매한 후에도 전자태그가 장착되어 있는 경우를 규제대상으로 삼고 있고, 소비자가 물품을 구매하기 전인 매장 안에서는 이 가이드라인이 적용되지 않음을 알 수 있다.

사업자가 소비자에게 상품을 인도한 후에도 전자태그를 장착해 두는 경우에는, 전자태그가 장착되어 있는 사실, 기억되고 있는 정보의 내용 등을 소비자에게 설명 혹은 게시하거나, 또는 상품・포장 상에 표시 할 필요가 있다(제3조).

소비자가 전자태그가 장착된 제품을 구매한 후 전자태그의 기능을 활성화시킬지 여부에 대한 선택권을 소비자에게 부여하고 있고, 전자태그의 판독을 막을 수 있는 구체적인 방안을 예시하고 있다(제4조). 예시에서 소개한 예로는 패러데이 캐이지 방식과 같이 알루미늄 막으로 판독기와 전자태그와의 통신을 차단하는 방안, Kill 태그 방식과 같이 태그를 비활서화 시키거나 태그내의 정보 전체 또는 소비자가 선택하는 일부의 정보를 소거하는 방식, 태그자체를 떼어내는 방식 등을 들고 있다.

상품 구매 후에도 전자태그를 판독 못하도록 할 경우에 발생하는 문제점이 있을 수 있다. 이에 대해 사업자는 상품 판매 후 전자태그 판독을 하지 못하도록 했을 경우 사회적 이익이나 소비자 이익이 손상되는 경우가 있을 수 있다는 정보를 소비자에게 제공할 노력이 있다(제5조).

개인정보보호법과 관련해서 전자태그 그 자체로는 개인 식별 정보가 될 수 없지만 개인정보 데이타베이스와 전자태그의 정보를 연계하여 개인을 식별할 수 있는 경우에는 개인 정보 보호법의 적용(제6조)을 받게 되며, 소비자에 대한 전자태그의 이용목적, 성질, 그 이점 및 불리점 등에 대해 정보를 제공 할 것을 규정하고 있다(제7조). 소비자와의 관계에서 사업자들이 추가적인 고려를 하도록 규정하여 사업

115) 〈http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp92_en.pdf〉.

자 자율규제 등에 대한 근거를 마련하고 있고(제8조), 사회정세의 변화, 기술 진보 등에 따라 가이드라인의 수정(제9조)에 대한 조항을 규정하고 있다.

2) 경제산업성과 총무성의 전자태그(IC태그)에 관한 프라이버시 보호 가이드라인

한편, 총무성에서도 2004년 2월 23일 'RFID 개인정보보호 가이드라인'의 제정 필요성과 기본내용을 발표한바 있다. 이에 총무성과 경제산업성이 협력하여 2004년 6월 8일 '전자태그(IC태그)에 관한 프라이버시 보호 가이드라인'을 발표하였다.[116] 경제산업성이 제안한 초안과 중복되는 점 이외에 새로 추가된 내용은 다음과 같다.

먼저, 개인정보를 전자태그에 기록하여 취급하는 사업자는 이용목적을 본인에게 통지하거나 공표해야 하며, 목적 외 사용의 경우에는 본인의 동의를 얻도록 해야 한다(제7조). 이는 경제산업성 초안에 개인정보 취급에 대한 사전동의 조항이 없던 부분을 보완하도록 한 조항이다. 하지만, 개인정보를 취급하는 경우 사전 통지나 공표하도록 하고, 목적 외 사용에 대해서만 사전동의를 받도록 노력할 필요성이 있다고 규정하고 있는 것으로 보아 강제성이 강한 조항은 아니다.

초안에 빠졌던 정보수정과 관련한 조항도 추가하였는데, 사업자가 전자태그 내의 정보의 정확성을 유지하기 위한 노력 필요성을 규정하고 있다(제8조).

그 외 개인정보보호법과 같이 정보의 적정한 관리 및 불평의 적절하고 신속한 처리를 위해 책임을 지는 정보 관리 책임자를 설치하고 연락처를 공표하도록 하고 있다(제9조).

한편, 초안에 있던 사업자의 행동(제8조)과 가이드라인의 수정 예정조항(제9조)은 가이드라인 조항에서 가이드라인의 "1.전자태그에 관한 소비자의 프라이버시 보호의 필요성"의 후반부에 추가되었다.

일본의 경우 특이한 점은 경제산업성과 총무성이 발표한 가이드라인을 ISO표준

116) 경제산업성과 총무성 사이에 정보기술(IT) 분야에서의 제휴를 강화하기 위해, 복수의 시책분야(전자태그, 정보가전, 정보보안 등)에 대해, 양성이 협력관계를 구축하는 것을 검토하고 있으며, 이번 가이드라인은 그 협력의 첫 번째 성과물이라고 볼 수 있다고 한다. 이는 우리나라에도 매우 큰 시사점을 주고 있는데, 유비쿼터스 환경에서 행정자치부, 산자부, 과학기술부, 정보통신부 간의 업무협조체계가 강화되어야 할 것이다.

으로 제정할 움직임을 보이고 있다는 점이다. 이는 자국내의 표준에 그치지 않고, 이를 국제적 표준으로 이끌어, RFID를 산업계에 적용시킴에 따라 프라이버시 관련 규제가 영향을 미칠 것을 예견하고, 이를 표준화하여 주도권을 계속 행사하려는 움직임으로 보인다.

다. 유럽

EU에서는 개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의 지침 제29조 데이터보호 실무작업반(Article 29 Data Protection Working Party)[117]에서 기술적 이슈중 하나로 RFID를 다루고 있고, 2004년 결과물을 목표로 진행중이다.[118]

EU 각 나라별로는 프라이버시와 관련된 시민단체들이 활동하고 있고, RFID 입법안을 만들 것을 요구하고 있다. 아직까지는 미국의 CASPIAN의 입법례나 미국, 일본의 입법례에 대해 주의를 기울이고 있는 상황이다.

영국에서는 국가소비자위원회(National Consumer Council)[119]가 2003년 초부터 소비자 관련 이슈로 인식하고, 2004년 2월 이해관계자 대표회의(summit)를 마련하였다.[120] 회의결과를 발전시켜 5월 4일에는 “전자칩에서의 요청?”(calling in the chips?)이라는 RFID 관련 보고서를 작성하였다.[121] 이 자료에는 회의에서 나온 6개의 권고사항(recommendation)과 RFID 기술 소개, RFID 기술의 소비자 사용사례, RFID 기술 발전과 소비자에 미치는 영향, 소비자에 대한 잠재적 위협, RFID 기술의 편리성이 소비자 위험을 능가하는지, 향후 논점 사항 등을 담고 있다. 권고사항에서는 토론

---

117) 실무작업반은 개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의 지침(Directive 95/46/EC)의 제29조에 의하여 설립되었다.

118) “Work Programme 2004 Article Working Party,” 〈http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp92_en.pdf〉.

119) 정부로부터 지원을 받지만 독립적인 소비자보호기관 〈http://www.ncc.org.uk〉.

120) 이 자리에서는 얼마나 넓게 기술이 사용될는지, 어떻게 사용될지, 소비자에 대한 잠재적인 이익과 위험이 어느 정도인지에 대해 고려하였다. 이를 위한 준비자료로서 “소매상에서의 RFID 기술”에 대한 브리핑 자료를 만들었다. 〈http://www.ncc.org.uk/pubs/rfid.pdf〉.

121) 〈http://www.ncc.org.uk/pubs/pdf/calling_in_chips.pdf〉 참조.

내용에 대해 국가소비자위원회가 일정한 입장을 표명하는 식으로 표현되어 있다. 법제도적인 측면에서는 현재의 규제가 RFID의 응용에 소비자 보호에 적용될 수 있는지에 대한 검토를 요구하고, 다른 규제의 원칙을 가진 다른 나라에서의 사용에 대해 조사를 강력하게 요구하였다. 또한 국제적인 공조의 필요성을 제기하면서, 데이터보호 실무작업반에서 유럽지역에 적용될 가이드라인을 제시할 것과 OECD가 국제적인 수준에서의 해결방안을 내는 것의 중요함을 지적하고 있다.

자율규제에 대해서는 그동안의 자율규제가 문제점이 있음을 지적하면서 자율규제로는 한계가 있으므로, 프라이버시 보호 차원의 법적인 규제가 필요함을 제기하였다. 이와 별개로 시민단체에서도 RFID의 입법과 관련해 두 가지 관점을 제시하고 있다.[122)]

5. 우리나라의 RFID 관련 개인정보보호 법제 정비 방안

가. 기존 입법으로의 규율 가능성

RFID 관련 개인정보보호 입법을 고려할 때 무엇보다도 먼저 현재의 개인정보보호법률 등에서 규정하는 내용이 어느 정도까지 RFID와 관련된 개인정보보호를 할 수 있는지 어느 부분은 감당하지 못하는지를 구분하여야 할 것이다.

공공부문에 있어서는 개인정보 보호에 관한 일반법으로 '공공기관의개인정보보호

122) 첫째는 미국과 같은 신규입법을 하는 방안과, 둘째는 컴퓨터 관련 기존 법들에 의해 수용될 수 없는가 하는 점이다. 두 번째 관점에서 소비자 수준 RFID 태그들과 관련한 RFID 프라이버시 이슈 해결책 중의 가능한 한 방법은 RFID 태그 칩을 컴퓨터로 보는 것이다. 그 경우 영국 컴퓨터 부정사용 법 제1장의 "무권한 접속(unauthorised access)"과 영국 데이터 보호법(UK Data Protection Act)이 이 시스템에 적용될 수 있다. 데이터보호법 하의 개인 데이터(personal data)는 다른 컴퓨터 기록 또는 데이터베이스 시스템에서 참조하는데 사용될 수 있는 단순 일련 번호를 포함한다.
특히 소비자 동의를 포함하고 있는 데이터 보호 원칙이 적용될 필요성이 있다. 슈퍼마켓 등에서 다른 소매상의 RFID 컴퓨터 칩 또는 RFID 컴퓨터(제품 패키지의 부분으로서 소비자에게 팔리거나 제품에 포함된)를 판독하는데 법적용이 된다면 흥미있을 것이라고 언급하고 있다. 〈http://www.spy.org.uk/cgi-bin/rfid.pl〉.

에관한법률’이 있고, 민간부문에 있어서는 ‘정보통신망이용촉진및정보보호등에관한법률’(이하 정보통신망법)이 일반법으로 역할을 하고 있다. 그러나, 최근 개인정보보호에 대한 관심이 높아지면서 현행 입법의 미비점을 보완하려는 측면으로 입법이 보완되거나,[123] 개정을 진행 중에 있다. 특히, 정보통신망법이 정보통신망 이용촉진이라는 사업자측면과 개인정보라는 소비자측면의 서로 상충되는 이익을 한 법에 담고 있는 모순을 제거하고, 개인정보보호의 범위를 확충하는 측면으로 개인정보보호에 관한 부분을 따로 떼어내어 ‘민간부문의개인정보보호에관한법률(안)’(이하 개인정보보호법(안)이라 한다.)이 마련되어 입법예고 되어 있다.[124]

정보통신망법에서 ‘보호되는 개인정보’의 범위는 ‘정보통신서비스제공자’가 수집, 처리, 이용 및 제공하는 ‘개인정보’에 해당하는 경우를 말한다. 먼저 ‘개인정보’부터 살펴보면, 정보통신망법 제2조제1항제6호에서는 ‘개인정보’를 생존하는 개인에 관한 정보로서 당해 개인을 알아볼 수 있는 정보로서, 직접 관련이 없다하더라도 다른 정보와 용이하게 결합하여 알아볼 수 있는 경우에도 포함한다고 말하고 있다.[125]

---

123) ‘신용정보의이용및보호에관한법률’(이하 신용정보법)이 2004년 1월 개정되었는데, 신용정보 수집·조사업무의 효율성을 높이기 위하여 신용정보업자 또는 신용정보집중기관이 공공기관에 대하여 신용정보의 열람 또는 제공을 요청한 경우 공공기관이 이에 응하도록 하고, 신용정보의 오용·남용을 막고 정보보호를 강화하기 위하여 신용정보주체에게 신용정보업자 등으로부터 신용정보의 제공사실을 통보받을 수 있는 권리를 부여하는 등 현행제도의 운영상 나타난 일부 미비점을 개선·보완하여 개인정보보호를 강화하는 내용으로 개정되었다.

124) 2004. 5. 19. 입법예고.

125) 정보통신망법 제2조제1항제6호에는 “개인정보”를 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.”고 규정하고 있다. 한편, ‘민간부문의개인정보보호에관한법률(안)’ 제2조제1호에는 개인정보를 “생존하는 개인에 관한 정보로서 당해 개인을 알아볼 수 있는 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 말한다)를 말한다.”고 규정하여 개인을 알아볼 수 있는 정보에 대한 범위를 예시된 내용으로 축소 해석할 우려를 막았다.

따라서 이러한 개인을 식별할 수 있는 정보에 해당하는 내용을 RFID가 수집하고 있는 경우에는 당연히 정보통신망법의 개인정보에 해당한다. 그리고, 당해 RFID로부터 수집된 정보 또는, RFID에 포함되어 있는 정보(제품코드 등)가 직접 개인을 식별할 수 있는 정보가 될 수 없다하더라도 그 RFID의 정보와 신용카드번호, 주민등록번호 등이 서로 연결할 수 있는 형태로 저장되어 관리되는 경우 그 RFID로부터 얻은 정보 또는 RFID에 포함된 정보는 정보통신망법의 개인정보라고 할 수 있다.

다음으로 정보통신망법에서 규정하는 수범대상자는 '정보통신서비스제공자'이다. 전기통신사업법제2조제1항제3호에 의하면 '정보통신서비스제공자'라 함은 전기통신사업법 제2조제1항제1호의 규정에 의한 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. '전기통신역무'라 함은 이중 "영리를 목적으로 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자"는 PC통신, 인터넷 등을 이용하여 정보 및 서비스에 관한 정보를 제공하는 자를 의미한다.[126] 그러므로 RFID 칩을 판독기가 읽어 이를 저장하는 시스템을 사용한다 하더라도 전기통신역무를 이용해 정보 및 서비스를 제공하지 않는 자는 정보통신망법 상의 정보통신서비스제공자가 해당되지 않는다. 따라서 현행의 정보통신망법은 RFID를 이용한 개인정보를 수집하는 자가 '전기통신서비스제공자'에 해당하지 않는 경우 적용되지 않는다.

나. 개인정보보호법(안)에 따른 규율 가능성

개인정보를 취급하는 많은 분야가 있는데, '전기통신서비스제공자'에 해당하지 않는다는 이유로 이 법의 적용을 받지 않는 사업자가 많다는 문제점으로 인해 개인정보보호법(안)에서는 '개인정보취급사업자'를 새로 규정하였다. 법안 제2조제4호에서 '개인정보취급사업자'를 "영리를 목적으로 정보주체의 개인정보를 수집하여 이를 처

126) 구체적으로는 인터넷 등의 정보통신망을 이용하여 방송프로그램 등의 디지털 정보를 제공하는 웹캐스팅(web casting), 신상품이나 이벤트(event)의 안내, 구직·구인 알선, 경품제공 등의 정보 및 서비스를 제공하기 위하여 회원모집 등의 방법으로 개인정보를 수집·이용하는 법인 및 개인 등이 이에 해당한다. 정보통신부, "개인정보보호지침 해설", 2002, 28면.

리・이용하는 자”로 규정하여 오프라인으로 개인정보를 취급하는 자와 함께 CCTV, RFID 등 새롭게 등장하는 정보기기를 통해 수집・처리되는 개인정보까지 확대함으로써 개인정보보호의 사각지대를 획기적으로 방지하고자 하였다.[127]

따라서 법안과 같이 수범대상자가 확대되면 RFID에 의해 수집되는 정보가 개인정보에 해당할 경우에는 개정될 개인정보보호법(안)의 규율을 받게 된다. 대략적인 내용으로는 아래와 같다. 개인정보취급사업자는 개인정보의 수집을 할 경우에 동의를 받아야 하고, 수집 시 고지의무가 있으며, 개인정보 수집의 제한(동법안 제10조 내지 제13조)을 받게 된다.

개인정보의 처리, 이용 및 제공 등에서도 개인정보관리책임자를 지정해야 하는 등(제14조 내지 제19조)의 조치를 취해야 하며, 정보주체는 동의철회, 열람・내역 및 정정 요구 등을 할 수 있다(제20조 내지 제23조). 이러한 각각의 조항들은 RFID에서도 대부분 적용이 가능하다. 또한 개인정보 정보주체의 동의철회, 열람 및 정정 요구권, 법정대리인의 권리, 손해배상 같은 권리에 관한 조항도 RFID의 사용과 관련해 적용이 가능하다.

다. 별도의 RFID 관련 규율의 필요성

먼저 개인정보보호법(안) 이외의 별도의 RFID 관련 규율이 필요한지 여부이다. RFID와 관련된 개인정보에 대해서는 개인정보보호법(안)의 적용을 받지만 RFID의 부착여부에 대한 소비자 선택권 및 선택방법, RFID의 고지방법, 소비자 교육 등의 세부적인 내용에 대해서는 별도로 이를 규정할 필요가 있게 된다. 특히, 개인정보를 포함하지 않고 다만 제품코드나 제품 이력 등을 담고 있는 RFID 칩일 경우에는 개인정보보호법으로는 규율되지 않는 부분이 존재하게 되므로 별도의 개별적인 법률 등을 통해 규율해야 한다. 즉, 제품에 이들 칩을 달고 다닐 경우 발생할 이후의 침해 위협에 대응하기 위해서라도 이를 사전에 고지하고, 부착여부 및 기능 활성화

127) 동법안 제2조제5호에서는 “처리”를 “정보통신망 또는 컴퓨터, CCTV 등 정보기기를 활용하여 개인정보를 입력・저장・편집・검색・삭제・출력 및 기타 이와 유사한 행위를 하는 것”이라고 규정하고 있다.

여부에 대한 선택권의 부여, 이를 부착하도록 유도하는 방향으로의 마케팅 금지, RFID 부착에 따른 소비자 이익 외에 소비자 프라이버시 침해 가능성에 대한 교육 등의 내용을 규정할 필요가 있다.

라. RFID 관련 규율의 형태

RFID 기술처럼 이제 개발이 진행되고 도입되기 시작한 기술과 서비스에 관한 법 모델을 모색함에 있어서는 일단은 지침(guidline)이나 권고(recommendation) 등을 통한 일종의 연성법적 접근(soft law approach)을 시도해 볼 필요가 있다고 주장하기도 한다.[128] 우리의 법체계에서는 이러한 내용은 가이드라인 또는 고시의 형태로 규정될 수 있다. 가이드라인의 경우 법적인 효력을 부여하지 않음으로써 자율규제의 형태를 취하게 된다.

자율규제는 민간이 자율적으로 시행지침을 마련하고 이를 준수하게 하는 것으로, 필요에 따라 부분적 입법을 통하여 개인정보를 보호하고 있으며 통제하기 위하여 별도의 정부기관을 운영하지 않고 부분적 법률을 기초로 업계 스스로 지침을 마련하여 준수하도록 하는 규제방식을 말한다. 개인정보 보호와 관련해서는 민간 사업자들이 기본법을 토대로 업계의 현실적인 수행가능성에 맞게 세부지침을 마련하여 자율적으로 적용하고 준수해 나가는 제도를 말한다. 자율규제중심의 국가는 미국, 캐나다, 일본 등이 속한다.[129] 그러나 사적부문에 대하여도 자율규제의 한계성 및 유럽연합(EU) 1995년 개인정보보호지침 제25조(제3국으로 개인정보의 이전의 원칙) 등의 영향으로 정부규제방식을 채택하는 것이 세계적인 경향이라고 할 수 있다.

정부규제는 정부의 적극적인 주도로 이루어지는 것으로, 개인정보보호에 관한 법률 등을 마련하고 개인정보의 취급과 유통을 통제하고 감시하면서 이를 위반한 당사자에게는 강력한 집행수단을 통해 처벌을 내리는 규제방식이다. 이러한 정부규제중심의 국가에는 영국, 프랑스, 독일, 스웨덴 등 주로 유럽국가들이 포함되어 있다.

---

128) 홍준형, "유비쿼터스 환경에서의 개인정보 보호－법정책적 고찰", 한국공법학회 제117회 국제학술발표회 자료집(2004.6.), 60면.

129) 황인호, 전게주 16), 242면 참조.

EU의 각 나라는 RFID가 한 국가내의 규율로 해결될 수 있는 것이 아니라는 점을 인식하고, EU 차원에서 해당 국가들에게 공통적인 가이드라인을 제시하기를 요구하고 있다.[130] EU의 1995년의 개인정보보호지침의 경우를 미루어 볼 때, 정부규제의 형태를 취할 가능성이 높아 보인다. 또한 자율규제를 선호하는 미국의 경우에도 주 차원이긴 하지만 구체적인 정부규제 입법형태로 움직이고 있음을 알 수 있다. 다만, 일본의 경우에서는 정부 주도로 만들어진 가이드라인 형태를 제시하고 있는데, 개인정보에 해당하는 경우에는 개인정보보호법을 적용하고, 그 외의 경우에는 사업자는 가이드라인을 따르도록 권고하고 있다.

마. RFID 개인정보보호 규정의 기본내용

개인정보보호에 관한 기본원칙으로 국제적으로 일반적으로 인정되고 있는 것들을 프라이버시 보호 관련 규정에 적용할 수 있을 것이다. 개인정보 보호에 관한 OECD 8원칙,[131] EU의 개인정보보호 지침, 미국의 세이프 하버 원칙과 UN의 '컴퓨터화된 개인정보 파일의 규율에 관한 가이드라인' 등이 그러한 기준이 될 수 있을 것이다. 개인정보보호와 관련된 법에서 다루는 것과 중복되지 않는 범위에서 제3장 제3절에서 언급한 개인정보자기결정권의 구체적인 권리들인 익명권, 정보처리금지청구권, 정보열람권과 정보갱신청구권, 정보분리청구권 등이 적용될 수 있는 부분을 반영해야 할 것이다.

6. 결 론

우리나라에서도 RFID가 소비자들의 프라이버시 및 개인정보보호에 어떠한 영향을 미치는지에 대한 사전적 분석과 이에 대한 법제도 및 기술적 대응방안 마련이

130) 〈http://www.ncc.org.uk/pubs/pdf/calling_in_chips.pdf〉 참조.

131) 8원칙으로는 ① 수집제한의 원칙(Collection Limitation Principle), ② 정확성원칙(Data Quality Principle), ③ 목적의 명확화/특정 원칙(Purpose Specification Principle), ④ 이용제한의 원칙(Use Limitation Principle), ⑤ 안전조치의 원칙(Security Safeguards Principle), ⑥ 공개의 원칙(Openness Principle), ⑦ 개인 참여의 원칙(Individual Participation Principle), ⑧ 책임의 원칙(Accountability Principle)이 있다.

시급한 실정이라 할 것이다.

유비쿼터스를 지향하는 신정보사회에서 개인정보통제권은 자신의 정보가 어떻게 수집, 처리, 관리, 이용되는지에 대한 감독권을 의미한다. 사생활보호의 차원에서의 개인정보란 절대적 보호되는 것이 아니며, 그 경계도 자연적으로 정해지는 것이 아니라 정치과정을 통해 재조정되는 유동적인 것이다. 공동체의 운영과 직접적으로 관련이 없는 정보는 개인의 인격성의 보호라는 전통적 프라이버시의 보호 차원에서 계속 프라이버시권의 보호를 받을 수 있지만, 공동체의 운영상 필요에 의해 일정한 개인정보의 수집은 적법한 절차적, 실체적 권리를 인정하는 것이 필요하다. 그리고 이 권리는 단순히 사생활 보호의 측면에서가 아니라 정보활용권을 가지는 정치적, 사회적 권력체에 대한 민주적 통제와 감시권으로서 새로이 인식할 필요가 있는 것이다.

우리는 이제 기술의 급격한 발전에 대한 미봉책으로써의 개인정보보호 논의는 이제 접어야할 시점이다. 기술에 따른 혜택과 부가가치가 이미 자리잡은 상태에서 개인정보보호에 대한 논의를 하기에는 너무 늦은 논의가 될 수 있기 때문이다. 기술의 발전을 예측하고, 방향성을 제시하여 때로는 기술의 발전방향을 선도할 수 있는 법제 및 정책제시가 필요하다 할 것이다. RFID가 제품과 연결되어 유비쿼터스 사회를 선도하여 엄청난 경제적 이익을 초래할 수 있다고 하더라도, RFID 정보의 오남용 문제와 더불어 개인정보의 유출 및 사업자들의 고객정보 불법거래 및 남용의 문제는 바로 현재의 시점에서 논의되지 않으면 그 의미를 더 이상 찾을 수 없을 것이다.

우리나라의 경우 개인정보보호에 관하여는 민간부문과 공공부문, 혹은 그 모두를 포괄하는 기본법 제정 등 다각적인 측면에서 법제화 논의가 진행되고 있으나, 이러한 법안에서는 RFID와 관련한 개인정보의 수집, 처리, 이용 및 제공, 정보주체의 권리 등에만 적용할 수 있으며, RFID 부착여부에 대한 소비자 선택권, 선택방법, RFID의 고지방법, 소비자 교육 등 세부적 내용에 대해서는 별도로 이를 규정할 개별적인 법률이 필요하다고 판단된다. 즉, 제품에 이들 칩을 달고 다닐 경우 발생할 수 있는 개인정보의 침해위협에 대응하기 위하여 이를 사전 고지하고, 부착여부 및 기능 활성화 여부에 대한 선택권의 부여, 이를 부착하도록 유도하는 방향으로의 마케

팅 금지, 그리고 RFID 부착에 따른 소비자 이익 외에 소비자 프라이버시 침해 가능성에 대한 교육 등에 대한 규정을 담을 수 있는 개별법의 제정에 대한 논의가 구체화되어야 할 것이다.

제 4 장 민간 부문에서의 유비쿼터스 제도화 구현 및 역기능 대비

제 1 절 U-commerce 확산 및 안정성에 관한 IT 법률의 정비방안

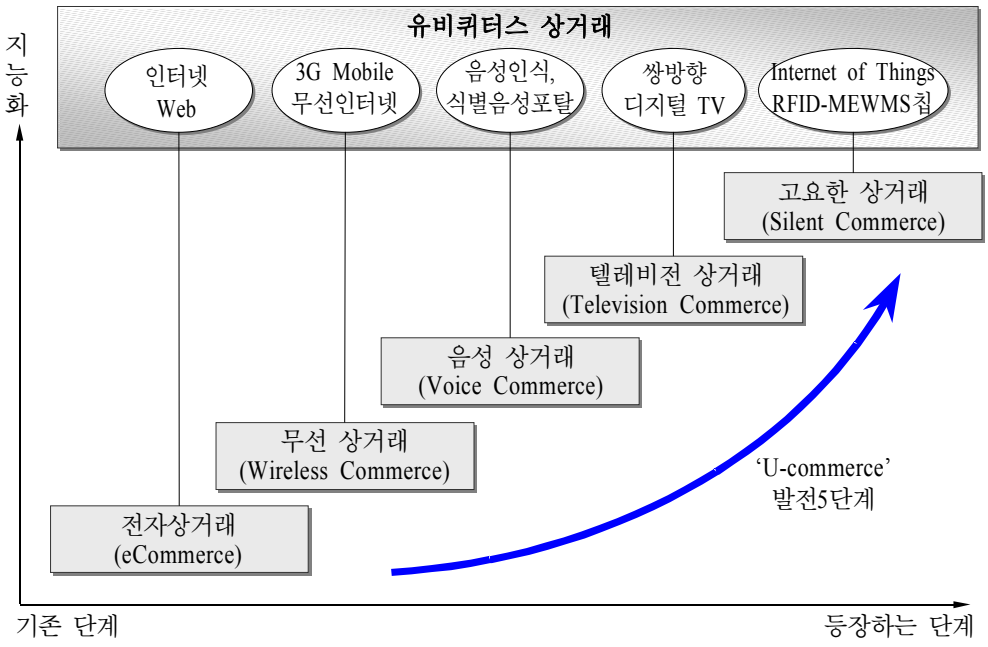
유비쿼터스 컴퓨팅과 네트워크를 기반으로 등장할 수 있는 비즈니스 사업은 인터넷을 이용한 e-commerce를 발전시킨 U-commerce이다. U-commerce는 유비쿼터스 컴퓨팅과 네트워크를 기반으로 하여 일상생활 속에서 고객의 소비활동을 촉진시키고, 고객이 구매하려는 상품이나 기업의 생산, 마케팅, 물류 판매나 고객관리 등의 비즈니스 프로세스를 도와준다. 즉, 모든 상품과 소비자, 기업이 항상 연결되어 있으며(always connected), 또한 항상 연결되어 있다는 것을 인식하고 있으며(always aware), 모든 상품이나 프로세스가 지능화 되어(always smart), 생산성과 소비를 촉진시키는 방향(always active)으로 가는 것이다.

현재 인터넷을 통한 e-commerce, 즉 전자상거래가 활성화 되면서 산업 전반적으로 투명한 거래가 활성화 되어 경영의 스피드가 향상되고 기업구조가 개선되었으며, 정보화의 대상이 기업 내부뿐만 아니라 기업외부에까지 확산되었다. 즉, 전자상거래는 인터넷 기반의 정보화를 통해 새로운 기업 경쟁력을 확보하고 원가를 절감하며, 경제 활성화를 촉진시키는 원동력이었던 것이다. 세계적인 시장조사기관은 ovum에서도 B2B 전자상거래의 시장규모는 향후 몇 년 동안 급속하게 증가할 것이라고 예측하고 있다. 또한 디지털 위성방송이 시작되면서 텔레비전을 보면서 상품을 주문하는 T-commerce에 대한 관심 역시 증대하고 있다. 2001년 T-commerce의 세계시장 수익은 7억달러 정도였지만 이후에는 급격한 성장을 보여 2007년에는 250억 달러에 달할 것으로 예측하고 있다.[132] 무엇보다 한국에서는 휴대폰을 이용한 모바

132) T-Commerce (2nd edition): Analysis and Forecasts for Global Transactional TV

일 결제 서비스도 증가하고 있는데 이동성과 접근성에 기반하여 U-commerce 환경의 필수적인 모바일 결제가 조기에 실현될 수 있을 것이라고 예상된다.

〔그림 4－1〕 U-commerce의 발전단계



무엇보다 유비쿼터스 환경에서 경제활동을 하는 각 주체(사업자, 중개자, 소비자)가 현실공간과 똑같이 안심하고 거래를 할 수 있는 법적 환경을 정비할 필요가 있다. 우선 유비쿼터스 환경에서의 거래와 같은 경제 활동을 안심하고 수행하는데 있어서 기본이 되는 민사법령이 필요하며, 그런 다음에 사업자가 갖는 불안에 대응하여 지적재산보호 법령을, 소비자의 불안에 대응하여 소비자의 신뢰를 확보할 수 있는 법령을 각각 정비할 필요가 있다. 마지막으로 유비쿼터스 환경에서의 활동을 안전하게 수행 할 수 있는 보안의 확보도 필요 불가결하다. 여기서는 유비쿼터스 환경에서의 상거래(U-commerce)를 위해 크게 민사법령이 정비와 지적보호재산권에 대한 정비로 나누어 설명하고자 한다.

제2절 지적재산보호에 관한 법령정비

유비쿼터스 환경이 발전하기 위해서는 양질의 정보재(콘텐츠 등)가 충분히 공급되고 이용되어야 하며, 지적재산보호 제도는 이를 위한 유효한 제도로 인식되고 있다. 그러나 현재의 지적재산제도는 현실공간을 전제로 하여 구축되어 왔으므로 유비쿼터스 환경의 극적인 변화에 충분히 대응할 수 없으며 유효한 기능을 수행하지 못하는 경우가 있다.

따라서 여기에서는 ① 유비쿼터스 환경에서 어떻게 하면 적절히 지적재산의 보호를 도모할 수 있는지 또는 ② 지적재산권 등에 유래하는 독점적인 권리남용에 의한 폐해를 어떻게 배제하여 유비쿼터스 환경의 혁신을 가져올 수 있는가 하는 논점을 제기한다.

이러한 논점에는 ① 유비쿼터스 환경에서는 거래에 참여하는 당사자를 식별하기 위한 특유의 표식(도메인네임과 메타태그 등)이 이용되고 있으나, 이것이 현실공간에서의 상표와 오인되는 경우가 발생하고 있으며, 이러한 문제에 어떻게 대처하여야 하는지에 대한 「유비쿼터스 환경에서의 거래 질서의 유지」와 관련한 논점이 있다. ② 유비쿼터스 환경에서 콘텐츠 등이 거래되는 과정에서 이전과 비교하여 가치가 증가한 지적재산(데이터베이스, 비즈니스 모델 또는 방법과 관련한 특허 등)에 대해서 어떻게 보호하고 콘텐츠 등의 개발 유인을 공급자에게 적절히 부여할지에 대한 「콘텐츠 등의 개발 유인 부여」라는 논점이 있다. ③ 현행의 지적재산권 법제에서 규정되어 있지 않은 인터넷상의 무체물의 유통과 대량으로 용이하게 이뤄지는 복제행위에 의한 새로운 이익침해행위에 대해서 어떻게 대응[133]하고 유비쿼터스 환경에서의 콘텐츠를 적정하게 이용할 지에 대한 「콘텐츠의 적정한 이용」이라는 논점이 있다.

---

133) 인터넷상의 저작물의 유통에 대응하기 위해, WIPO(World Intellectual Property Organization: 세계지적소유권기관) 저작권조약이 성립되어, 인터넷상의 송신 및 송신을 가능하게 하는 행위를 저작권 침해로 규정하고 있다.

1. 유비쿼터스 환경에서의 거래질서의 유지

유비쿼터스 환경에서는 거래에 참가하는 당사자를 식별하기 위한 특유의 표식(도메인 네임이나 메타태그 등)이 이용되고 있으나, 타인의 상표가 당해 식별표식으로 사용되어 유비쿼터스 환경 상에서 당해 식별표식과 상표를 오인하는 일이 발생하고 있다. 또한 상표 등이 웹사이트 상에서 유비쿼터스 환경을 통하여 국경을 초월해 전 세계에서 볼 수 있기 때문에 해외의 상표에 관한 권리관계로 분쟁이 발생하기 쉽다.

이와 같이 유비쿼터스 환경의 등장에 의하여 현실공간에서 안정된 거래질서 유지에 도움이 되어 온 표식에 관한 보호제도가 커다란 영향을 받고 있다. 따라서 여기에서는 유비쿼터스 환경과 현실공간이라는 양자의 거래질서를 어떻게 보호해 갈지에 대해서 아래의 세 가지 논점에 대해서 논하기로 한다.

가. 도메인네임

도메인네임은 이른바 인터넷상의 「주소」를 말한다. 현실공간의 「주소」는 자기 스스로 결정할 수 없으나 도메인네임은 선착순으로 스스로 선호하는 것을 선택할 수 있다. 이 결과 타인의 상표 등과 동일하거나 유사한 도메인네임을 취득・사용하는 것이 가능하며, 이러한 도메인네임을 고액으로 전매하려 하거나 성인 사이트를 운영하는 등 상표권자과의 사이에서 분쟁이 일어나는 사례가 발생하고 있다.[134)]

이러한 문제를 해결하기 위해서 작년 말 민간 측에 의한 통일분쟁처리절차가 개시됨과 동시에[135)] 미국은 작년에 법령을 정비하였다.[136)] 따라서 일본에서도 법령 정

---

134) ① 미국의 캘리포니아주에 거주하고 있는 Y는 약 100달러로 등록한 「worldwrestlingfederation.com」의 도메인네임을 세계레슬링연맹에 1,000달러에 살 것을 제안하였다. 그런데 본 건에 대해서 ICANN의 분쟁처리제도(WIPO중재센터)는 세계레슬링연맹으로 당해 도메인네임의 이전을 명령하였다.
② ICANN의 분쟁처리제도에 제기된 분쟁은 현재 1,000건을 넘고 있다.
③ 일본기업관련 분쟁도 많으며 예를 들면 「toshiba.net」, 「niftyserve.net」 등이 있다.

135) ICANN은 WIPO의 권고(인터넷 도메인네임 프로세스에 관한 WIPO보고서, 1999년)에 기초하여 통일분쟁처리제도의 운용을 작년 12월부터 개시하였다.

비(타인의 상표 등과 동일하거나 유사한 도메인네임의 부정한 목적의 취득・사용에 대한 규정)가 필요하다.

나. 상표가 인터넷상의 식별표식으로 모용되는 사례에 대한 대응

상기와 같은 도메인네임과 유사한 문제가 인터넷상의 식별표식과 관련해서도 발생하고 있다. 즉 유비쿼터스 환경에서의 검색용 키워드인 인터넷상의 식별표식(예를 들어 메타택,[137] 배너광고의 키워드[138] 등)에 대해서 타인의 상표와 동일하거나 유사한 것을 설정함으로써, 상표권자와의 사이에서 분쟁이 일어나는 사례가 점차 증가하고 있다.[139] 따라서 분쟁의 실태 등을 조사연구한 후에 인터넷상의 식별표식에

---

136) 미국에서는 "반사이버스쿼팅소비자보호법(1999년)"을 제정, 그 중에서 타인의 상표 등에 저촉하는 도메인네임의 불법등록 및 불법사용에 대해서 당해 상표보유자에게 도메인네임의 취소・이전을 요구하는 권리 및 도메인네임 등록자에 대한 금지・손해배상청구권을 부여할 것이 규정되어 있다. 또한 WIPO에서는 주지하는 바와 같이 상표보호규칙(1999년)의 권고가 결의되어 주지하는 상표와 유사한 도메인네임의 불법등록 및 불법사용에 대해서 도메인네임의 취소・이전을 요구하는 권리를 부여할 것이 규정되어 있다[사이버스쿼팅(cybersquatting): squatting이란 불법점거라는 뜻으로 사이버스쿼팅이란 어떤 사람이 도메인네임으로 타인의 상표 등을 등록하고 선착순이라는 등록관행을 이용하여 그 상표의 본래 소유자가 그 상표를 도메인네임으로 사용하는 것을 막고 또한 그 도메인 네임을 본래의 소유자에 팔아 이익을 획득하려 하는 것을 말한다].

137) 홈페이지는 HTML(Hypertext Markup Language)이라는 언어로 기술되나, 메타태그는 그 문서에 기입된 태그이며, 보통 눈에는 보이지 않는다. 메타태그로 지정된 키워드는 탐색엔진의 정보수집 대상이 된다. 예를 들면 탐색엔진에 「전자거래진흥원」이라는 키워드를 입력하면, 「전자거래진흥원」이라는 키워드가 메타태그로 지정된 홈페이지 검색결과를 나타난다.

138) 배너광고는 홈페이지상의 가로로 긴 광고를 말하며, 예를 들면 검색엔진에 키워드로 「컴퓨터」라고 입력하면, 검색결과 페이지에 나타나는 배너광고에서, 컴퓨터 메이커의 배너광고가 나타나도록 하여, 이와 같이 검색엔진과 배너광고를 연동시킴으로써 효율적인 광고가 가능해 진다. 이러한 검색엔지용 키워드와 배너광고의 세트가 검색엔진 제공자에 의해 판매되고 있다.

139) ① 검색엔진 제공자 Y가, 「Playboy」, 「Playmate」를 포함한 관련 키워드와 배너광고를 한쌍으로 하여, 성인용 오락서비스를 제공하는 자에게 판매한 바, 원고 X로부터 상표권 침해 및 딜루션을 이유로 한 소송이 제기되었다.[Playboy Enterprises Inc.

대해서 표식을 어떻게 보호할 지에 대한 검토가 필요하다.[140]

다. 인터넷상에서 표식을 사용한 경우 타국 상표권자의 침해로 인한 소송 대응

상표권자가 자신의 상표를 자신의 웹사이트에서 사용하면 당해 웹사이트는 전세계에서 열람 가능하다. 한편 상표권은 각국별로 권리가 부여되기때문에(상표의 속지주의), 동일상표에 대해서 타국에 다른 상표권자가 존재하고 이러한 타국의 상표권자의 상표권 침해로 인한 문제가 발생할 가능성이 있어 자신의 상표를 자신의 웹사이트에서 안심하고 사용할 수 없다. 이러한 문제를 해결하기 위해서는 WIPO의 국제규칙 정비에 적극적으로 참여할 필요가 있다.[141]

2. 콘텐츠 등 개발 유인의 부여

IT의 발달에 의해 방대하게 축적되어 있는 데이터에서 필요한 데이터를 용이하게 검색할 수 있게 되어 현재는 보호되지 않고 있는 창작성이 없는 데이터베이스의 재산적 가치가 증가하고 있다. 또한 IT의 발달 및 전자상거래의 발전은 비즈니스 방법(method) 관련 특허에 있어서 이전과 비교하여 지적재산의 가치가 증가하게 되었다. 이와 같이 이전과 비교하여 가치가 증가한 지적재산을 어떻게 보호할 지를 검토할 필요가 있다. 구체적인 검토는 다음과 같다.

---

v. Netscape Communications Corp., 1999 WL428233 (C.D.Cal. 1999)]

② 1981년의 「Playmate of the Year」인 피고 Y가, 자기가 개설한 웹사이트에 메타태그로서 「Playboy」, 「Playmate」를 사용하고 있었던 바, 원고 X에게서 상표권 침해를 이유로 한 소송이 제기되었다.[Playboy Enterprises Inc. v. Terri Welles, 7F. Supp. 2d. 1098 (S.D. Cal. 1998)]

③ 최근에는 메타태그와 키워드에 라이벌 회사의 상표를 이용하여 자기 회사의 홈페이지나 배너광고로 유도하는 등의 사건이 문제가 되고 있다.

140) WIPO에서는 「인터넷상의 표장 사용과 관계된 공업소유권의 보호규칙안」에서 기술발전에 의해 가능해진 새로운 표장의 사용 태양에 대하여 공업소유권의 보호를 검토하고 있다.

141) WIPO에서는, 「인터넷상의 표장 사용과 관계된 공업소유권의 보호규칙안」에서, 인터넷상에서의 각국 상표의 공존 조건을 검토하고 있다.

가. 데이터베이스의 법적 보호

창작성이 없는 데이터베이스에는 지적재산권이 설정되어 있지 않으며, 또한 지적재산의 제3자에 대한 사용을 제한하는 법률도 없다. IT의 발달은 방대하게 축적되어 있는 데이터에서 필요한 데이터를 용이하게 검색할 수 있게 하여 창작성의 유무와 관계없이 데이터베이스에 재산적 가치가 발생할 수 있다. 또한 IT의 발달에 의해 누구라도 간단하게 대량의 정보를 매우 간단하게 복제・가공할 수 있기 때문에 데이터베이스는 복제물의 대량 유포의 위험에 노출되어 있다. 따라서 창작성이 없는 데이터베이스에 대하여 이러한 데이터베이스의 침해실태에 관한 조사연구를 필요호 하며, 국제적인 동향에도 주의를 기울여 무단 추출・재이용을 규제할지에 대한 세밀한 검토의 필요가 있다.

나. 비즈니스 방법 관련 특허

비즈니스 방법(method) 관련 특허는 전자상거래 관련・금융관련・소프트웨어 관련 발명에 관한 특허로서 성립되는 경우가 많으며 그 출원이 최근 급증하고 있다. 비즈니스 방법 관련 특허에 대해서는 ① 너무 광범위하게 특허가 이루어져 비즈니스의 전개에 지장을 초래한다. 즉 선행자인 미국이 이를 선점하기 위한 것이라면 이에 대한 대책이 필요하며, ② 무엇이 특허되었는지를 알 수 없기 때문에 무엇이든 우선 출원되지 않을 수 없다 라는 지적이 있다.

①의 광범위한 특허문제에 대해서는 현재 일본과 미국에서 크게 차이가 없다는 견해가 제시되고 있다. 또한 장래 비즈니스 방법 관련 분야에서는 비즈니스 방법 그 자체는 예전부터 실시되고 있었음에도 불구하고 충분히 문서화되어 있지 않은 까닭에 선행 문헌의 축적이 부족하므로 선행 문헌인 데이터베이스의 정비에 대해 국제적인 협조를 함으로써 적절한 권리부여를 위해 노력할 필요가 있으며, 그 결과를 세심히 살피는 검토가 필요하다.[142] ②의 문제에 대해서는 비즈니스 방법 관련 분

142) 미국・유럽・일본 3극 특허청 전문가회의(2000년 6월)에서, ①「비즈니스방법 관련 발명에 관한 비교연구」에 대한 검토 결과에서, ㈀ 컴퓨터에 의해 실시되고 있는 비즈니스방법이 특허되기 위해서는 기술적 측면이 필요하며, ㈁ 이미 알고 있는 업무

야의 심사기준을 조속히 명확히 할 필요가 있다.

3. 콘텐츠 등의 적정한 이용

인터넷상에서는 대량으로 복제되어 배포가 가능한 특질을 가진 무체물인 고품질의 콘텐츠가 유통되고 있으나, 현행의 지적재산권 관련 법령은 이러한 유통형태를 상정하고 있지 않다. 이 때문에 컴퓨터프로그램의 네트워크상의 송신행위로 인해 컴퓨터 프로그램과 관련된 특허가 가지는 이익이 침해되는 사례, 사적복제의 권리제한 규정이 유비쿼터스 환경에서 저작권자의 이익을 침해하는 온상이 되고 있는 사례 등, 현재의 지적재산권 관련 법령이 상정하고 있지 않은 이익 침해행위가 나타나고 있어 이러한 새로운 이익침해 행위에 대해서 어떻게 대응해야 할지를 검토할 필요가 있다. 구체적으로는 이하와 같은 논점을 들 수가 있다.

가. 컴퓨터 프로그램과 관련된 네트워크상의 송신행위로 인해 이익이 침해된 사례

특허권이 부여된 컴퓨터 프로그램은 하드웨어에 내장한 형태(예를 들면 가전제품)이나 플로피디스크, Cd-ROM 등의 기억장치에 고정된 형태로 거래되는 경우에는 특허권자의 허락이 필요하다. 그러나 IT의 발달로 인해 컴퓨터 프로그램이 기억장치에 고정되지 않은 제품으로 네트워크 상의 송신행위에 의해 거래되는 사례가 늘어나고 있으나 네트워크를 매개로 한 거래에 대해서 특허법상의 취급이 명확하지 않기 때문에 원활한 유통을 저해하고 있다.

따라서 기억장치에 고정되어 있는지의 여부와 관계없이 컴퓨터 프로그램 그 자체가 법적으로 보호되도록 조속히 조치할 필요가 있다.[143)]

프로세스를 잘 알려진 방법으로 자동화한 것만으로는 특허가 되지 않음을 확인하여 미국과 일본의 심사결과는 총체적으로 일치한다 이해와 ② 비즈니스 방법 관련 분야의 선행문헌 자료를 정비할 필요성 및 관련된 선행기술의 가장 적절한 정보원을 특정하고, 이러한 정보원에 엑세스할 수 있도록 하기 위한 이용자측의 협력 가능성을 찾아야 한다는 점을 인식하고 「공동 서치프로젝트」를 가동하기로 합의함.

143) 미국특허청에서는 「프로그램 신호」와 같은 형태로 프로그램을 보호하고 있다. 유럽특허청에서는 유럽특허조약 52조 제2항(c)에서 컴퓨터 프로그램 그 자체는 보호되지

나. 사적복제 권리제한규정이 유비쿼터스 환경에서 저작권자 이익침해의 온상이 되고 있는 사례

저작물의 사적복제에는 복제 및 유통비용이 들며 복제할 때마다 품질이 떨어지고 또한 복제에 대한 현실적 과세 수단도 결여되어 현재 저작권은 원칙적으로 통용이 제한되고 있다(사적 복제에 관한 권리 제한). 그러나 유비쿼터스 환경에서는 복제가 저렴하고 대량으로 품질이 떨어지지 않는 제품의 송신이 가능하기 때문에 사적복제에 관한 제한규정을 마련하여 온 전제가 무의미하다. 또한 최근에는 네트워크상에서 복제물의 교환을 지원하는 다양한 법령이 출현한 결과 사적복제와 관련한 권리제한규정을 근거로 저작권자의 이익을 크게 침해할 수 있는 사례가 나타나고 있다.[144)]

한편 디지털 콘텐츠에 대해서는 (사적 복제라도) 복제횟수에 따른 저작권료에 해당하는 과세를 가능하게 하는 기술이 등장하고 있다.[145)] 이러한 디지털화・네트워크화의 발전에 따른 환경변화를 바탕으로 IT시대에 적합한 저작권 보호와 그 예외(사적 복제) 간의 균형을 어떻게 파악하여야 할지의 관점에서 사적 복제와 관련한 법령에 대해서 기술동향과 분쟁실태를 충분히 조사연구한 후에 검토를 할 필요가 있다.[146)]

않는다고 규정하고 있음에도 불구하고, 1998년 IBM심결(T1173/97, T0935/97)에서 「프로그램 product」와 같은 형태의 프로그램을 허용하는 심결이 내려졌다. 그 심결 결과 현재 유럽특허조약 52조 제2항(c)의 전단 제외규정에서 컴퓨터 프로그램을 삭제할 것이 검토되고 있다. 단 미국 유럽 모두 네트워크 상에서의 컴퓨터 프로그램의 송신행위가 특허권 침해에 해당되는지에 대한 사법판단은 아직 이루어져 있지 않다.

144) 인터넷을 이용하여 이용자간에 자신의 컴퓨터 하드디스크에 보존하고 있는 음악파일 콘텐츠(mp3파일)를 용이하게 교환할 수 있는 서비스인 「Napster」가 등장하고, 나아가 영화에 대한 「Scour」, 디지털 콘텐츠 형태라면 음악뿐만 아니라 영상 등 무엇이든 교환할 수 있는 「Gnutella」 등 냅스터와 유사한 후속 서비스도 나와 있어 저작권자의 이익을 크게 위협하는 것이 문제되고 있다. 2001년 현재 미국에서는 냅스터사와 스카우어사에 대한 저작권 침해소송이 제기되어 현재 대법원에 계류중에 있다.

145) 현재 디지털 복제에 대해 저작권료를 징수하는 제도로서는 하드웨어(복제기재) 및 장치(MD 등)에 착안하여 이들 가격의 일정한 비율(이른바 더빙 보상금)을 징수하는 제도가 있다(사적 녹음・녹화 보상금제도). 나아가 최근에는 디지털 콘텐츠의 인터넷을 매개로 하여 이뤄지는 복제에 대해서도 사용한 시간이나 복제 횟수에 따라 대가를 징수할 수 있는 기술이 실용화되고 있다.

제3절 RFID의 고도활용을 위한 제도적 기반

1. 개 관

유비쿼터스 정보기술이 급속도로 보급되면서 우리의 생활을 바꿔놓고 있다. 그 대표적인 사례가 언제 어디서나 네트워크를 통해 컴퓨터 시스템과 연결될 수 있게 하는 장치의 하나인 RFID(radio frequency identification)이다. RFID는 전파식별, 전자태그, 전자칩이라고도 하는데, 초소형 마이크로 칩과 안테나로 구성되어 있다. 이것은 이동용 단말기(mobile device)와는 달리 가격이 저렴하고 사용방법도 간편할 뿐만 아니라 그 용도가 무궁무진하여 유비쿼터스 컴퓨팅의 핵심소재로 이용되고 있다. RFID를 이용하여 유비쿼터스 컴퓨팅 환경을 구현하였을 때 우리는 공간과 거리의 제약이 없고, 통신용량의 제약도 없으며, 네트워크, 단말기, 서비스, 콘텐츠의 제한이 없는 환경 속에서 살게 될 것이다.

이와 같이 RFID가 자유롭게 사용되기 위해서 이용자의 수용태도라든지, 기술적 문제점 등 해결해야 할 과제가 많다. 단시일 내에 RFID를 보급할 수 있으려면 이용자들이 RFID를 인지하고 수용하는 태도가 긍정적이어야 한다. 무엇보다도 RFID를 이용하는 것이 두렵고 위험한 것이 아니라 편리하고 안전하고 유익하다는 확신이 있어야 한다.

예컨대 다음과 같은 응용분야에서 기대 이상의 성과를 거두었다고 할 때 RFID를 도입하는 기업들이 크게 증가할 것이다. 즉, 가전기기, 항공수하물 태그, 휴대전화, RFID를 부착한 청과물의 추적가능(traceability) 시스템은 RFID를 적용하고 그 효과

---

146) 미국에서 본 문제는 “fair use(미국저작권법 107조”)의 해석이 문제가 되어 냅스터의 문제에서도 fair use의 범위가 논란이 되고 있다. 일본에서는 냅스터의 문제에 대해서 다운로드한 이용자는 사적 복제의 권리제한 규정에서, 업로드한 이용자는 송신가능권 침해에서, 중개소프트웨어나 서비스를 제공하는 자는 민법의 불법행위 일반원칙에서 각각 문제가 된다고 볼 수 있다. 이와 같은 기술혁신의 속도에 대응하기 위해서는 개별 권리제한 규정의 수정뿐만 아니라 “fair use”라는 일반 조항의 도입도 더불어 검토할 필요가 있다는 의견도 있다.

를 테스트할 수 있는 무대가 되고 있다. 현재 우리나라에서 분야별로 추진되고 있는 RFID 시범사업의 내용은 〈표 4－1〉과 같다.

〈표 3－1〉 한국전산원의 RFID 시범사업 개요

기관	사업명	사업자	사업내용	기대효과
조달청	물품관리 시스템	LG CNS 컨소시엄	물품등록・보관・취득・이동의 실시간 관리	생산성 제고, 국가자산 관리, 시장수요 창출
한국공항공사	RFID기반 항공수하물 추적통제시스템	아시아나DT 컨소시엄	항공수하물 추적 통제, 분식방지, 도착정보 표시, 고객확인 등	정확한 수하물처리 통한 비용절감, 보안검색 강화 및 실시간 승객정보 확인
국립수의과학검역원	RFID이용 수입쇠고기 추적 서비스	한화S&C 컨소시엄	수입 쇠고기의 이력관리, 입・출고 및 원산지 관리, 판매정보 조회	유해 수입 쇠고기 추적 및 잔량 파악 통한 회수처리 속도 개선
국방부	RFID기술 적용 국방 탄약관리 시스템	LG 히타치 컨소시엄	탄약취득・보관・사용・처분 현황 실시간 파악	탄약적재관리 자동화에 따른 공간효율성 증대, 재물조사비용절감
산업자원부	RFID를 활용한 수출입국가물류 인프라지원	ECO 컨소시엄	EPC네트워크 플랫홈, 수출입무역망 연계기반 자동차부품 수출물류 파악	수출입물류 활용도 제고, 추적고도화, 대외신뢰도 향상

주: 한국전산원은 이 밖에도 원아안전관리, 중국발 일본행 물품의 이용경로 파악, 환자・의료인・의료장비 위치추적관리 시스템에 관하여 실증실험을 실시하고 있다.

자료: 이희욱, “세계는 지금 RFID행 Gold Rush”, Economy21, No.227, 한겨레이엔씨, 2003.12.7.

2. RFID 활용범위의 확장

RFID를 도입하는 조직, 기업이 많아질수록 그 활용범위가 확대될 것이다. 본래 RFID는 유비쿼터스 센서 네트워크(USN)에 많이 적용되고 있으므로 단일 조직에서 이용되기보다는 복수의 조직・업종이 서로 제휴를 맺고 RFID 및 여기서 취득한 정보를 고도로 활용할 수 있어야 한다. RFID 활용범위의 확대는 플랫폼의 개방화와 관련이 있는데 다음과 같은 3단계로 범위가 넓어지고 있다.

① 단일(single) 플랫폼: 하나의 이용자(조직)가 단일 플랫폼을 사용하는 경우

예컨대 자동차회사에서 공장 내의 공정관리, 부품관리, 작업지시의 목적으로 플랫폼을 구축하는 경우 네트워크의 활용범위는 크게 문제되지 않는다.

② 공통(multi) 플랫폼: 복수의 이용자(기업)가 단일 플랫폼을 사용하는 경우

예컨대 자동차부품을 생산하는 협력업체, 자동차공장, 물류회사 등 자동차산업에 속하는 복수의 기업이 RFID를 활용하여 공급체계를 통합 관리할 목적으로 플랫폼을 공유하는 경우이다. 업종이 유사하거나 관련이 있는 복수 기업간에 플랫폼을 공유하게 되므로 네트워크의 활용범위가 확대된다. 또 플랫폼의 공유를 통하여 각각의 기업이 RFID로부터 취득한 정보를 공유함으로써 업무효율을 제고할 수 있다.

③ 제휴(federated) 플랫폼: 복수의 이용자(기업, 조직)가 각자 보유하는 플랫폼을 상호 제휴하여 플랫폼을 공동 활용하는 경우

예컨대 자동차회사, 주유소, 보험회사 등 전혀 다른 영역에 속하는 복수의 기업 또는 조직이 각자 보유하는 RFID 플랫폼을 제휴함으로써 새로운 서비스를 제공하는 경우이다. 자동차회사는 생산관리를 위하여 RFID를 자동차에 부착하는데 주유소에서는 자동차의 RFID에 수록되어 있는 정보를 참조하여 고객에 적합한 서비스를 제공할 수 있다. 그리고 보험회사는 고객의 RFID에 들어 있는 본인의 정보, 운전상황을 참조하여 보험료를 조정할 수 있을 것이다. 이와 같이 RFID가 제휴 단계에 이르면 기업들은 RFID 플랫폼을 제휴하기 위하여 네트워크 활용범위를 크게 확대한다. 다른 기업·조직과의 융합을 통하여 새로운 서비스를 창출할 수 있다.

위에서 살펴본 바와 같이 RFID를 고도로 활용하는 경우 경제적으로 부가가치가 높은 서비스를 제공할 수 있다. RFID에 수록된 정보는 다음 세 가지로 나누어 볼 수 있다.

① 물적 정보: RFID가 부착되어 있는 물건의 제품정보, 생산국 등의 속성정보, 물건의 스테이터스(생산, 배송 등) 정보가 이에 해당한다.

② 이력정보: RFID가 부착되어 있는 물건이 어떠한 경로를 거쳐 왔는지, 스테이터스가 어떻게 변하였는지 알려주는 정보이다. 예컨대 쇠고기 포장에 부착된 RFID는 생산지 목장에서 도축장, 정육점에 이르기까지의 경로를 알려주므로 식품의 안전성을 보장할 수 있다.

③ 실시간으로 변하는 정보: RFID에서 취득하는 정보에 추가하여 센서로부터 취득하는 실시간(real time) 정보를 취합 활용하는 경우이다. 예컨대 병원에서 환자에게 제공하는 식사를 관리할 때 RFID에 생체 센서를 통해 파악한 환자의 컨디션을 고려할 수 있도록 한다면 환자에게 적합한 메뉴를 제공할 수 있게 된다.

3. RFID 고도활용의 전제

RFID가 사회 여러 분야에 사용되기 위해서 극복해야 할 첫 번째 과제는 기술적 문제점을 극복하는 것이다. RFID 관련기술은 계속 발전하고 있기 때문에 현재 기술적인 문제가 있다 하더라도 조만간 해결될 수 있을 것임에 틀림없다. RFID를 둘러싸고 종종 문제가 제기되는 것은 RFID의 성능 및 내구성, 기존 시스템과의 연결 작동 여부, 여러 기업간에 RFID를 제휴하였을 때의 시스템 오류에 관한 것들이다.

RFID에는 리더와 안테나가 필수 부품이므로 리더・안테나의 기술적 측면도 함께 고려하고, 시스템 네트워크의 기술적 과제도 해결하여야 할 것이다. 이를 위해서는 제도 측면에서 관습, 조직, 업무・거래 절차(business process)를 새롭게 설계하고 고려해야 할 체크 리스트를 만들어 점검할 필요가 있다.

둘째로, RFID는 기술적 표준화가 시급히 요청된다. 이는 RFID의 경우 ID코드의 관리와 할당이 효율적으로 이루어져야 그 이용이나 제휴를 통한 네트워크의 확대가 가능하기 때문이다. 그리고 RFID와 관련하여 제휴를 맺은 조직・기업은 RFID에 부여하는 ID코드를 서로 인식하고 정보를 공유할 수 있어야 한다. 표준화는 다른 RFID 특히 외국 제품과의 호환성 및 재활용성을 제고할 것이다. 일반적으로 국가가 체계적으로 관리하고 있지만, RFID에 사용되는 무선주파수 대역에 관하여도 통일된 관리기준이 마련되어야 한다.

그리고 RFID・리더의 표준화, 통신・데이터 프로토콜의 표준화, 업계이용의 표준화 등 표준화도 시급하다고 생각된다. 오퍼레이션의 변경, 에러 발생시의 대처, 이용자 교육, RFID가 여러 곳으로 옮겨졌을 때 그 전후에 관련된 오퍼레이션의 연결 문제도 기술적인 대처가 필요하다. 또한 RFID와 관련된 사업모델에 있어서는 복수

기업간의 연결작동 모델, 코스트 증가분을 흡수할 수 있는 사업모델이 요구되며, 개인정보의 침해를 방지하기 위한 RFID 프라이버시 보호 가이드라인도 요청되고 있다. 왜냐하면 RFID에는 개인정보가 축적될 수 있는데 다른 목적이나 별개의 장소에서 이용될 수 있기 때문이다.

셋째로, 여러 기업이 RFID 플랫폼에 제휴하는 경우의 보안 문제도 중요하다. 접근을 통제하기 위하여 본인식별장치가 갖춰져야 하며 정보 유출을 방지할 수 있어야 한다. 즉, 복수 기업간의 제휴와 그에 따른 거버넌스(자율규제방식), 코스트 분담, 보안 및 접근통제, 운용(operation)의 공통화, 데이터 형식의 공통화가 필요한 과제이다.

넷째로, RFID를 도입하기 전에 그에 따른 투자 대 효과(비용－편익) 분석도 있어야 할 것이다. RFID 도입에 있어서 단계별로 문제가 된 기술적인 과제는 별표와 같다. RFID가 기대한 효과를 발휘하려면 제조단계에서 최종 운용단계에 이르기까지 세심하에 신경을 써서 해결해야 할 과제가 이것 뿐만은 아닐 것이다.

이렇게 RFID가 활성화되기 위해서는 이용자들의 수용태도나 기술적 한계 극복, 기술적 표준화 등 해결해야 할 과제가 많다. 이러한 문제점들을 잘 해결한다면, 향후 비즈니스 부분에서 RFID가 적극적으로 활용될 수 있는 분야가 다양하다.

다섯째, 최근 RFID와 관련된 비즈니스 모델(BM)에도 관심을 기울여야 할 것이다. RFID와 관련된 비즈니스 모델을 놓고 특허 또는 기술특허를 출원하는 경향은 일본이 미국이나 유럽에 비하여 월등히 많다. 일본의 경우 내용상으로는 물류 분야보다도 판매유통 분야에 출원건수가 많다. 비접촉 IC카드 관련 특허에 의한 결제, ETC 관련 도로교통분야에도 BM특허가 많이 나와 있다.

향후 과제로서 컨버전스 모델이 증가하고 있기 때문에 복수 플랫폼을 제휴할 수 있게 하는 비즈니스 모델이 각광을 받고 있다. 이에 따라 여러 관련기업들이 RFID를 둘러싸고 서로 제휴할 수 있는 상황이 활발히 전개될 것으로 전망된다.

미국에서는 한정된 영역에서 복잡한 정보를 취급하는 응용분야에서 특허출원 건수가 증가하고 있다. 또한 추적 가능한(traceable) 영역과 고객의 구매이력을 활용한 비즈니스 모델에의 특허출원이 많고, 이력정보 활용분야에서도 출원건수가 증가하고 있다. 일본에 비하여 특정 기업에 의한 과점도가 낮고 분산되어 있는 것이 특징

이다. 유럽의 경우 출원건수 자체는 많지 않지만 일본과 마찬가지로 물류 분야보다도 판매유통 분야에서 특허출원이 많은 경향을 보인다.

〈표 4－2〉 RFID 적용단계별 기술적 과제

적용 단계		기술적 과제
↑ RFID 개체의 기능・성능	제조단계	물리적 강도
		생산 코스트, 호환성 확보
		소형화(신뢰성 유지/향상 포함)
	장착단계	제품수명에 대응한 내구성 및 성능 보장
		금속 등 다양한 제품에의 대응
		태그의 고부가가치화(센서의 추가)
	통신단계	주파수별 특성의 공유
		통신시간, 통신속도 등의 처리능력
		태그와 리더 사이의 통신거리
실제 활용 ↓	운용단계	프라이버시 보호, 정보보안
		상호운용(로칼형과 오픈형)
		어플리케이션 별로 다른 판독방법

본 연구에서는 RFID가 활용분야 중에서 아직 본격적으로 활용되고 있지는 않으나 발전 가능성이 큰 금융기관의 담보관리에 RFID를 활용하는 방안을 살펴보고자 한다. 종래 기계・기구, 재고자산 등 기업동산은 그 가액에도 불구하고 담보제공하는 방법이 제한되어 있어 금융기관으로부터 자금을 차입할 때 제대로 이용되지 못하였다. 이하에서는 금융기관의 RFID 이용 사례를 알아보고 해결해야 할 과제와 활용방안, 법제화 방안 등에 대하여 검토해보기로 한다.

4. 금융기관의 RFID 활용 제고방안

가. 현행 기업동산담보의 문제점

기업의 재고관리와 마찬가지로 지폐, 유가증권에도 RFID를 부착하여 지급결제, 어음교환에 이용할 수 있으며, 관련법제가 정비되면 담보관리에도 활용할 수 있을

것이다. 현재 금융기관은 기계・기구 등의 동산이나 재고자산을 담보로 이용할 수 있는 방법이 제한되어 있다. 무엇보다도 담보관리가 어렵고 특히 고가의 기계는 리스 물건과 혼동되기 쉬우며, 제3자에 의하여 선의취득될 가능성도 많다. 만일 공장에 설치되어 있는 기계・기구, 창고 안의 재고자산에 RFID 태그를 부착하고 물건의 제조연월일, 메이커 등의 속성, 소유자・담보권자 현황 등의 정보를 입력해 놓는다면 담보관리가 수월해지고 리스물건과 혼동되거나 불법 반출되는 것을 방지할 수 있을 것이다. 즉, 담보관리인이 정기 또는 수시로 현장을 방문하여 리더기를 휴대하고 담보물 설치장소를 순회하면 담보물건의 스테이터스를 자동으로 확인할 수 있게 된다.

현재 기업이 보유하는 동산(기계・기구, 재고품, 재고자산 등)은 아직까지 마땅한 공시방법이 없어 양도담보를 설정하거나 아니면 공장저당법에 의한 목록추가 방식으로 일괄하여 담보를 제공하고 있다. 대부분의 중소기업은 고가의 동산을 보유하고 있음에도 담보제공이 곤란하여 금융기관의 대출을 받을 수 없는 실정이다.[147] 즉, 기업동산의 공시방법으로는 양도담보가 고작이며 새로운 공시방법을 채택하려면 법제도의 개선이 필요하다.

현재 기업동산에 채용할 수 있는 공시방법의 요건은 신뢰성이 있고 일반이 간편하게 수용할 수 있어야하며, 현행 등기・등록제도에 큰 무리 없이 편입시킬 수 있고 도입에 큰 비용을 요하지 않아야 한다. 이러한 견지에서 기업동산의 공시방법을 갖추는 데는 소형이고 저렴하며 위・변조가 어려운 RFID가 최적이라고 할 수 있다.

---

154) 현행 민법상 물건변동에는 거래의 안전을 위하여 외부에서 인식할 수 있는 공시방법을 아래와 같이 요구하고 있다.
－부동산 및 특수동산(자동차, 중기, 선박): 등기, 등록
－동산: 점유(따라서 질권을 설정하려면 목적물을 인도해야 함)
－양도담보는 '신탁적 소유권이전'이라는 판례상의 공시방법을 취하고 있음
또한 기업동산은 기업이 계속 점유하고 사용해야 하므로 일반적인 공시방법을 취할 수 없고 금융기기관 앞 담보제공이 곤란하다. 기업동산에 대하여도 담보권의 존재를 대외적으로 표시할 수 있는 방법만 있다면 금융기관 앞 담보를 제공하고 대출을 받을 수 있을 것이다.

RFID는 기업의 담보관리 및 모니터링에 필요한 데이터의 읽고쓰기가 가능하며, RFID 자체의 위·변조, 복제, RFID 부착물의 불법반출을 막을 수 있다. 하지만 금속에도 부착 가능한 RFID는 아직 고가이지만 기술진보가 빨라 조만간 가격이 인하될 것으로 예상된다. 또한 RFID 플랫폼을 인터넷망에 연결하면 법원의 현행 등기 시스템에 적용하는 데 큰 문제가 없을 것이다.

나. RFID를 활용한 담보관리

실제 RFID를 활용한 기업동산 담보관리 사례를 가상해 보면 다음과 같다. 기업의 담보제공용 기계·기구, 재고자산에 RFID를 부착하여 RFID에 당해 담보물에 관한 정보를 입력하고 담보권을 설정, 관리한다. 여기서 RFID에 입력해야 하는 담보물에 관한 정보에는 기계·기구의 주요 부품, 원재료, 재고자산 등 목적물의 성격, 제조연월일, 메이커의 표시, 소유자의 주소, 성명·상호 기타 변동사항, 채권자/담보권자의 주소, 성명·상호, 기타 권리관계(질권, 양도담보, 리스 등) 등이다. 물론 여러 담보물(금속, 플라스틱류, 목재·종이류, 의류 등)에 부착가능한 RFID 소재를 개발하고, 앞서 언급한 것처럼 위·변조, 해킹, 복제방지 기술의 개발 및 대량·동시 판독상의 인식률 제고, 오류방지 기술을 개선하여 신뢰성을 확보하는 것이 시급하다. 또한 현행 등기·등록제도에 적용하기 위한 프로토콜을 개발하여 현행 제도와 호환이 되도록 하고, 플랫폼의 범용성 제고를 위해 플랫폼을 표준화할 필요가 있다.

이렇게 기업의 담보물에 RFID가 설치되면, 채권은행의 직원 또는 대리인이 RFID 리더를 휴대하고 여러 거래처의 공장을 순회하는 것만으로 담보관리가 가능해질 수 있다. 일단 담보물에 대해 RFID가 설치되면 인터넷을 통하여 관할 등기소에 접속, 목적물이 일치하는지 조회해보고 필요한 사항의 입력 또는 변경을 할 수 있으며, 당해 담보물에 대한 권리관계를 공시, 열람도 할 수 있다. 또한 담보권 실행을 위해 권리관계를 확인하는 등 RFID에 의한 담보권 설정 및 관리, 실행이 훨씬 용이해질 것이다.

다. 담보관리의 구체적인 방안

RFID를 이용한 기업의 담보관리는 〈표 4－3〉에서 보듯이 사업추진의 효과를 보

아가며 단계적으로 실시하는 것이 바람직하다. 이를 위해서는 우선 시범사업을 통하여 기술적 타당성을 검증해야 하는데 특히 RFID 기술 및 데이터의 표준화, 위·변조, 오류의 방지, 비즈니스 모델의 구축 등에 많은 노력을 기울여야 할 것이다. 이와 동시에 금융기관들로 하여금 채권담보의 법적 효력에 확신을 갖게 하는 관련법의 제·개정 등 법제면의 준비작업이 필수적이다. 그리하여 RFID를 활용한 담보관리가 성공적으로 이루어질 수 있다고 확신이 설 때에는 각종 대행 서비스, 중고기계 거래소의 설치, 수출 알선 등 관련사업의 인프라를 정비하고 경협사업 등 다른 분야에까지 RFID를 활용하는 방안에 대해서도 검토가 있어야 할 것이다.

〈표 4－3〉 RFID를 이용한 담보관리제도의 추진일정(예시)

단계별	추진 과제	관련기관
1. 타당성 검토	○ 기술적 타당성 검토 －RFID, Reader의 설계 및 적용 －데이터베이스 구축, 인터넷 연결 －법인등기부 등재 가능성 －비즈니스 모델 수립	－법학연구소 －한국RFID/USN 협회 －법원행정처(등기소)
2. 시범사업	○ 시범사업 실시 －중소규모 공장에의 적용 －일반 기업에의 적용	－중소기업중앙회 －중소기업진흥공단
3. 협력체제 구축	○ 관련기관과의 협력체제 구축 －금융기관의 대출가능성 검토 －중고기계 거래소의 설치	－전국은행연합회 －신보, 기술신보 －중소기업진흥공단
4. 입법추진	○ 법제화 추진 －관련부처(법무부, 재경부, 법제처) 협의 －국회 상임위 전문위원	－법무부 －재정경제부 －법제처
5. 확 장	○ 적용범위의 확장 －신기술 법제의 해외수출 －개성공단 등 북한지역에의 적용	－산업자원부(특허청) －통일부

담보관리용 RFID의 표준화는 담보관리 수요에 부응한 데이터의 표준화, 호환성

을 제고하기 위한 것이다. RFID 및 리더의 규격(spec), 프로토콜 부분과 해킹 등 정보보안(security) 시스템, 소유자・채권자 등의 개인정보보호(privacy) 정책 부분에서 표준화가 이루어져야만 기술의 효율성, 안정성이 확보될 것이다. 이를 위해서는 국가적 차원에서 ID코드・주파수대역의 관리 및 할당을 하는 것이 바람직하다.[148)]

이와 같이 RFID를 활용한 기업동산 담보관리의 비즈니스 모델(BM)을 구축하기 위해서는 궁극적으로 법원 등기소에서 관리하여야 하므로 이를 공익사업으로 수행하여야 함을 관련법률에 명시하는 것도 좋을 것이다. 그러나 RFID 담보관리에 의한 새로운 사업모델을 고안하여 이를 사업화하는 경우에는 비즈니스 모델에 특허를 인정하여도 무방할 것으로 생각된다. 예를 들면, 채권은행을 위한 전자방식의 담보관리 대행 서비스와 같은 것은 비스니스 특허를 통해 새로운 사업영역으로 인정할 수 있다. 또한 RFID 담보관리 기술 및 하드웨어/소프트웨어의 해외수출에 대비하여 주요국에는 RFID 비즈니스 모델 특허를 출원함으로써 국가적 경쟁력을 높일 수 있을 것이다.

라. 기업동산담보에 관한 법제도 정비

1) 기업동산담보에 관한 국내외 입법례

금융기관의 담보관리에 RFID를 활용한다는 것은 기계・기구 등 동산에 비점유형 담보권(non-possessory security interest)을 설정한다는 것이므로 현재 기업동산을 담보로 활용하는 국내외 입법례를 살펴볼 필요가 있다.

우리나라에서는 자동차, 건설기계, 항공기, 선박 등을 등기・등록함으로써 저당권을 설정하고 담보제공자가 계속 사용・수익할 수 있게 하는 특수담보제도를 운용하고 있다. 또 공장저당법에 의하면 공장의 기계・기구 기타 공용물에 대하여 토지・건물의 저당권의 효력이 미치는 공장저당제도를 시행하고 있다. 또한 광업재단저당법에서는 광업권자의 소유에 속하는 토지, 공작물, 기계・기구, 차량, 선박 등으로 광업재단을 구성하고 그 위에 저당권을 설정할 수 있게 하고 있다.

---

148) 현재 산자부 기술표준원에서는 2008년까지 50여종의 RFID 관련 국가표준(KS)을 제정・보급할 예정이다.

동산담보에 관한 선진규범인 美國 통일상법전(Uniform Commercial Code: UCC) 제9편의 담보부거래(Article 9. Secured Transactions)[149] 규정을 살펴보면, 동산 담보권은 동산 및 부동산의 정착물에 대하여 계약으로 담보권(security interest)을 설정하는 거래에 적용되고 있으며, 유체물(tangibles)은 물품(goods)과 설비(equipment)로 구분되고 물품은 다시 소비자용품, 재고품, 농산물 등으로 나뉜다. 이렇게 UCC에 의한 담보권은 담보권자가 담보제공자와 담보계약(security agreement)을 체결하고 담보물에 대한 점유(possession)와 지배(control)를 확립하여야 성립된다. 담보권이 대항요건(perfection)을 갖추려면 금융명세서(financing statement)를 등록하거나 특정 물품·증서의 점유 또는 지배, 자동적 완성(automatic perfection)[150] 중에서 택일할 수 있도록 하고 있다.

한편 UCC는 채무자가 목적물을 특정하지 않고 범위만 정하여 담보로 제공할 수 있게 하고 있다. 미국에서 인정되는 부동담보(floating charge)[151]는 채무자가 담보계약 체결 당시에 소유하는 동산뿐만 아니라 장래 취득할 재산(after-acquired property)에 대해서도 담보권을 설정할 수 있으며, 현재의 채권은 물론 장래의 대출(future advances)도 담보할 수 있다. 채무자는 통상의 영업과정(in the ordinary course of business) 담보물을 자유롭게 사용·처분할 수 있으나 그 밖의 경우에는 담보권자의 동의를 얻어야 한다.[152] 미국 동산담보법에 의하면 담보권자는 채무불이행시 담보권자는 계약 또는 UCC에 규정된 경매, 임의매각, 추심, 점유취득 등의 구제방법을 행사

149) UCC는 1990년대 들어 거래환경의 급속한 변화에 따라 대폭적인 개정이 불가피하였다. 그 결과 1962년에 제정되어 1970년대에 부분 개정을 거친 동산담보법은 1998년 대대적으로 개정되어 2001년 7월 1일자로 발효되었다. 그 내용을 보면 제1장 총칙, 제2장 담보계약의 효력과 담보권의 성립, 담보계약당사자의 권리, 제3장 담보권의 완성(대항요건) 및 우선순위, 제4장 제3자의 권리, 제5장 담보권의 등록, 제6장 채무불이행, 제7장 경과규정으로 구성되어 있다.

150) 소비자물품의 경우 매도인이 매수금담보권(purchase money security interest: PMSI)을 취득하는 경우에 한한다.

151) UCC §9－204.

152) 미국의 부동담보제도에 관하여는 박훤일, “미국의 부동담보제도 －우리나라의 담보법제에 대한 시사점”, 「비교사법」 제10권 4호, 2003. 12, 177～192면 참조.

할 수 있다.

독일의 경우에는 동산을 대상으로 하는 담보제도로서 일반적으로 양도담보, 채권양도, 소유권유보 등을 이용할 수 있다. 집합동산(Warenlager)에 대하여는 장소를 지정하거나 특정 표시를 하는 담보계약을 함으로써 목적물을 특정지어 담보로 제공하는 동산담보제도가 시행되고 있다. 또한 동산에 대하여 특정의 원칙, 일물일권주의(一物一權主義)의 범위 내에서 담보로 활용된다.

일본은 1958년 기업담보법을 제정하여 재단저당의 문제점을 해소하고, 주식회사의 사채 또는 특정 채권의 담보 목적으로 증감 변동하는 기업재산 전부를 담보로 제공할 수 있게 하고 있다. 이는 영국의 부동담보(floating charge)와 유사한 제도로서 저당권 등에 대하여 우선권이 없는 약한 담보권으로서 등기를 하여야 효력이 있다. 다만, 대상이 되는 기업이 주식회사로 제한되고, 피담보채권도 사채(社債) 등에 한정될 뿐만 아니라 담보제공자가 기계・기구 등을 제3자에게 양도하여도 담보권자가 추급할 수 없는 문제 등으로 활용도가 낮다는 문제점을 안고 있다. 그밖에 많은 기업들이 이용하고 있는 동산담보는 점유개정에 의한 양도담보와 소재지가 특정되어 있는 집합물양도담보 등인 바, 제3자의 선의취득 시 담보권을 주장할 수 없고, 담보대상 물건이 제한되는 등 적극적으로 활용되지 못하는 실정이다. 따라서 일부 고가의 동산설비에 대하여는 자산유동화 방식으로 자금조달방안 모색 중이다.

그밖에 사회주의에서 시장경제체제로 전환한 체제전환국(transition economies)의 담보제도를 살펴보면, 토지・기계 등 생산수단의 사유화를 금지한 구체제의 영향으로 동산, 채권등의 담보활용이 불가피한 실정이다. 따라서 EBRD의 모범담보법(Model Law on Secured Transactions)에서도 목적물에 제한을 두지 않고 등록을 전제로 한 등록담보권(registered charge)을 광범위하게 인정하고 있으며, 중국, 베트남 등은 자국에 실정에 맞게 동산을 담보로 제공할 수 있도록 법제화하고 있다.[153]

2) 기업동산담보관리에 따른 법제 정비

RFID를 활용하여 기업 담보관리를 위해 법제도를 정비함에 있어서는 우선 시범

153) 체제전환국의 담보제도 정비상황에 관하여는 박훤일, 「남북경협의 확대에 대비한 북한담보제도의 정비방안」, 집문당, 2004 참조.

사업을 통해 금융기관들이 새로운 동산담보에 대한 담보가치, 담보관리방법, 담보권 취득 및 실행절차에 만족하고 기꺼이 대출을 해줄 수 있어야 한다. 이에 관한 컨센서스가 이루어지면 새로운 비점유형 동산담보권(charge)을 인정하고, 현행 비송사건절차법을 개정하는 등 실체법(實體法)과 절차법(節次法)에 대한 양면적 접근을 요한다.

우선 비송사건절차법(非訟事件節次法)을 개정하기 위해서는 기업동산의 담보권 공시는 채무자기준으로 하는 인적 편성주의를 원칙으로 한다. 따라서 법인(회사)인 채권자가 전자방식으로 담보권을 취득하는 것을 인정하고, 제4장 상업등기, 제3절 등기절차, 제5관 합명회사의 등기에 소유자의 상호・명칭 및 본점・주된 사무소의 소재지, 담보권자의 상호・명칭 및 본점・주된 사무소의 소재지, 담보권 설정의 원인 및 그 일자, 채권의 총액, 기타 담보권과 관련된 사항, 등기번호, 등기연월일 등을 등기할 수 있도록 한다. 그리고 이를 다른 회사에도 준용하되, 필요한 경우 개인채권자에게도 상업등기부 신설할 수 있도록 한다.

이와 더불어 「기업동산 담보에 관한 특례법(가칭)」을 도입하여 기업이 담보로 제공할 수 있는 동산의 범위를 설정하고, RFID 등 전자적 장치를 이용한 공시방법을 법제도적으로 인정해 주는 제도장치가 필요하다. 또한 RFID를 통해 기업동산에 대한 담보권을 설정하고, 담보권 설정자 및 담보권자의 권리와 의무를 규정한다. 또한 RFID가 부착된 담보물건에 대해서는 리더기와 인터넷을 통해 법원의 법인등기부 시스템에 접속하여 담보권의 존재와 담보물건의 일치 여부를 확인하고, 담보권의 취득・실행・소멸을 가능하도록 한다.

나아가 이 법안에 현행 「자산유동화에 관한 법률」에서 유동화대상 자산인 매출채권 등을 금융감독위원회에 등록하는 것이나, 현재 입법 추진 중인 「전자금융거래법(안)」에서 외상매출채권 등의 전자채권을 금융결제원에 전자등록하는 것까지 포괄한다면 사실상 기업의 모든 재산을 담보로 제공할 수 있게 된다. 다시 말해서 일물일권주의를 유지하면서 기업의 담보제공능력을 획기적으로 개선할 수 있게 되는 것이다.

〈표 4－4〉 현행 공장저당제도와 새로운 기업동산담보제도의 비교

	현행 공장저당제도	새로운 기업동산담보제도
대상기업	－공장이 있는 주식회사	－모든 법인(회사)
담보목적물	－법에 정한 공장: 토지, 건물 및 그에 속한 기계・기구	－독립된 물건(경제적 가치가 있는 기계・기구, 재고자산, 재공품)
피담보채권	－모든 채권	－모든 채권
효 력	－저당권	－채무자가 담보물을 사용・수익하므로 저당권과 비슷
담보권 실행	－일괄 경매	－개별적 경매도 가능
특 징	－一物一權主義의 수정 －공장 전체의 물건을 유기적 일체로서 취급 －목록작성 및 변경절차가 번잡하고 많은 비용 소요	－一物一權主義의 적용 －담보물을 개별적으로 취급

3) RFID를 활용한 담보관리의 기대효과

RFID를 활용하여 담보관리를 하게 될 경우 다음과 같은 이점이 있다. 기술수준의 발달로 기계, 설비와 같은 기업동산이 고성능화, 고가화 되어 가는 추세에 맞추어 이를 담보가치로 활용함으로써 기업 담보관리의 사각지대를 해소할 수 있다. 기계, 설비, 재고자산을 당해 기업이 계속 점유, 사용할 수 있으므로 기업활동에 지장을 주지 않는다. 또한 분리 가능한 모든 부품에 RFID를 부착함으로써 기계, 설비의 종합적인 상태와 가치를 파악하여 기업의 담보가치를 향상시킬 수 있게 된다. 중소기업의 경우에 RFID를 통한 담보관리를 통해 담보여력을 획기적으로 증대시킬 수 있는데, 중소기업이 가진 고가의 기계, 기구, 재고자산을 금융기관에 담보로 제공하고 신규 대출을 받아 사업을 확장할 수 있다. 자산건전성규제(BIS Rule)를 받고 있는 금융기관들도 부동산담보 의존도를 줄이는 한편 중소기업 동산담보를 통한 신규여신을 확대할 수 있을 것이다.

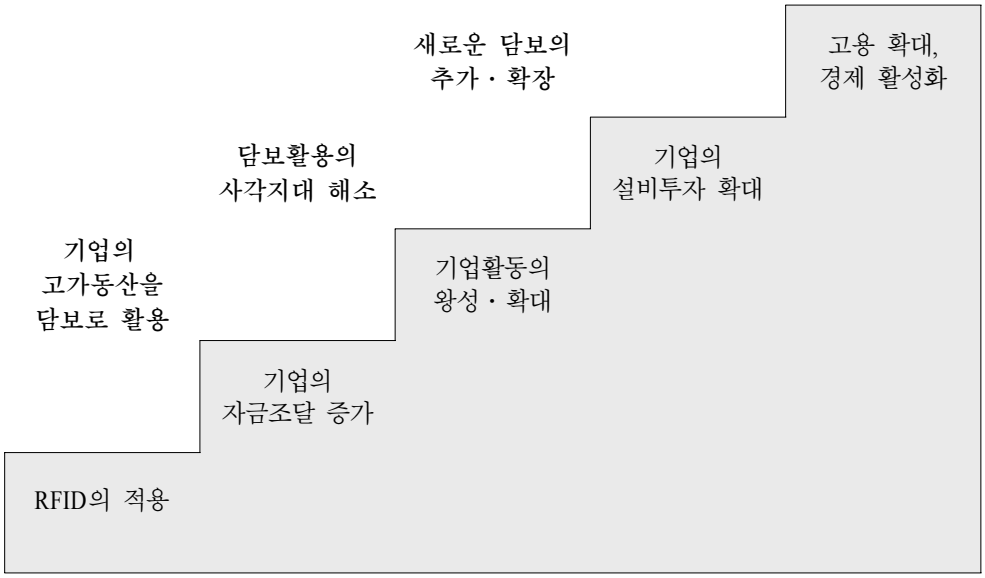
이와 같이 RFID를 통한 담보관리는 기업체뿐만 아니라 금융기관으로서도 효율적으로 담보를 취득하고 관리할 수 있게 된다. 금융기관의 경우에는 기업의 재고자산이나 매출채권 등의 변동을 쉽게 파악할 수 있을 뿐만 아니라 경기변동에 대응한

기업활동에 맞게 여신을 취급할 수 있게 된다. 또한 기계・기구, 재고자산 등 중소기업의 유형재산에 RFID를 부착할 경우 종전의 이중담보의 위험을 원천적으로 불식할 수 있게 되어 보다 효율적인 담보관리가 가능해진다. 그리고 일물일권주의 원칙을 유지하면서 전자적인 공시방법을 갖출 수 있는 범위 내에서 기업의 모든 가치있는 자산을 담보로 제공할 수 있게 된다. 다시 말해서 영미의 부동담보에 필적하는 담보제도의 혁신을 꾀할 수 있는 것이다.

게다가 개성공단 등 북한에 진출하는 기업들에 대해서는 또 다른 의미를 갖는다. 예컨대 개성공단에 진출한 기업의 설비와 재고자산에 RFID를 설치하고, 인터넷을 통하여 원격지 모니터링을 할 수 있다면 현재로서는 취급이 어려운 설비・재고자산을 담보로 운영자금 등의 금융지원을 할 수도 있을 것이다. 지금도 북한 소재 공장의 토지이용권, 건물 등에 대하여 저당권을 취득할 수 있다고는 하나 이것만으로는 은행들이 담보부 대출을 취급할 수 없는 형편이다. 나아가 고가의 원재료, 부품 등의 불법반출 통제도 가능할 것이다.

또한 RFID를 활용하여 담보관리를 할 경우에는 담보관리의 안전성・신뢰성 제고를 위한 관련산업의 발전이 크게 촉진될 것으로 기대된다. 예를 들면, RFID의 정보보안 내지 정보보호와 관련된 전문업체의 사업영역이 확대되고, 전국에 산재한 공장들의 기계・기구를 데이터베이스화하여 이를 RFID에 입력하고 담보관리를 대행해주는 업체가 등장하게 될 것이다. 이에 따른 고용창출 효과도 적지 않을 것으로 예상된다. 무엇보다도 RFID 관련기술의 지속적인 발전을 촉진시켜 국내 IT산업이 더욱 발전된 RFID 기술을 구현할 수 있을 것이다. 다만, 금융기관들이 RFID를 활용하여 기업동산을 담보로 취득하고 대출을 해주기 위해서는 몇 가지 선행조건이 필요하다. 담보권의 실행 과정에서 담보가치가 저하되는 것을 방지하고 담보물이 원활하게 거래될 수 있도록 감정평가 전문회사와 중고 기계・기구의 온라인・오프라인 거래를 촉진하기 위한 전문거래소가 설치되어야 한다. 법제도상으로도 담보권의 효력이 확실하고 담보권실행절차가 간편할 뿐만 아니라 그 비용도 저렴하게 할 수 있는 인프라 구축이 필요함은 물론이다.

〔그림 4－2〕 RFID를 활용한 기업동산 담보관리의 선순환 효과



제 5 장 결론 및 정책적 제언

본 보고서는 “유비쿼터스(ubiquitous)”라는 세계적인 IT 기술 방향의 흐름에 맞춰 유비쿼터스 환경의 핵심개념과 핵심 기술을 파악하여 미래 한국사회를 보다 풍요롭고, 안전하게 만들기 위한 법제도적 기반을 마련하는 것이 목적이다. 물론 법제도라는 것이 현 상황에 맞춰 적절한 대안을 찾고, 마련하는 것이 되어야 하겠으나 급속도로 IT의 기술혁신이 진행되는 현시점에서는 다가오는 미래상에 대한 정확한 개념파악을 통해 IT기반의 미래사회를 활성화시키고, 발생가능한 역기능을 최소화할 수 있는 법제도적 기반을 제시하는 것이 적절한 것으로 판단된다. 따라서 본 본고서에서는 우선적으로 유비쿼터스 개념을 파악하고, 유비쿼터스 IT로 구현된 사회환경의 모습을 그려보고 유비쿼터스 IT가 어떠한 핵심 기술들로 이루어지는지를 살펴보았다. 이를 통해 다음과 같은 5가지의 미래사회의 이슈와 법제도적 구현방향을 제시할 수 있다.

첫 번째는 미래사회 이슈는 디지털 디바이드와 사회적 불평등의 확산 가능성이다. 마크 와이저는 각 개인이 편리한 장소, 시간, 상황에 맞춰 여러 대의 컴퓨터를 사용하게 되는 사회가 바로 유비쿼터스 컴퓨팅 환경이 도래한 사회라고 지칭했다. 여러 기술이 도입되고 통합된 단말기를 통해 다양한 서비스를 이용하게 되는 것이다. 하지만 이러한 유비쿼터스 IT는 경제력에 따라 기술 활용 범위가 달라지게 될 우려가 있다. 초기 기술 도입에 있어 단말기나 서비스 비용은 상대적으로 경제적 우위에 있는 사람들이 사용할 수 있도록 채정되는데, 유비쿼터스 IT는 사회 전방에 분산된 컴퓨터가 사용자의 다양한 상황과 맥락에 따라 서비스를 제공하기 위해 작동되어야 하기 때문에 이에 따른 비용문제는 새로운 디지털 디바이드(digital divide) 양식을 만들어 낼 우려가 있다. 이는 곧 유비쿼터스 사회의 사회복자(welfare)문제로 등장하게 될 것이다. 이에 따라 유비쿼터스 IT가 디지털 디바이드의 심화와 사회적 불평등 확산에 대비한 법제도적 기반이 필요할 것이나 여타 보고서들에서 이들 문

제를 더욱 심도깊게 많이 다루었기에 본 보고서에서는 제외하였다.

두 번째 이슈는 시스템 리스크(system risk)의 발생 가능성이다. 유비쿼터스의 개념에 있어서 유비쿼터스 IT는 언제, 어디서나 도처에 존재하는 IT 기술로 다양하나 종류의 컴퓨터가 사람과 사물, 환경 속에 내재되어 연결되어 있어서 필요한 곳에서 컴퓨팅을 구현할 수 있는 것을 지칭한다, 특히, 많은 유비쿼터스 기술 구현이나 서비스에서 사물(things or objects)에 컴퓨팅 파워(computing power)를 적용시킴으로써 사물이 지능화되는 것에 초점을 맞추고 있다(강홍렬b, 2004). 이러한 사물의 지능화는 우리가 일상적으로 사용하는 책상이나 의자, 컵은 물론 펜, 음식 조리기구, 냉장고, 세탁기 등 모든 사물과 대상을 망라하고 있다. 특히 냉장고를 지능화시켜 냉장고 안에 있는 우유나 채소 등 식품 등에 붙어있는 RFID 태그의 정보를 읽어서 유통기한, 주문장소, 제조방법, 요리방법 등을 자동적으로 사용자들에게 알려주는 형식도 취하고 있다. 이렇게 유비쿼터스 IT는 점차적으로 일상적인 삶(장보기나 요리하기 등)을 기계에 의존하게 되는 방향으로 가게 되어 기계가 정보처리를 하는 과정에 과부하를 주어 기계의 시스템 리스크를 가져올 수 있다. 다시 말하면, 각 기계가 지능화 된다는 것은 각각이 정보를 입력(input), 출력(output)하는 등 정보를 처리하는 과정(information processing)을 거치게 된다는 것을 의미하는데 이는 각 기기마다 걸리는 정보처리 과정 시간이 길어지게 되거나, 입출력 장치가 다양해 지거나, 정보처리 과정이 복잡해 질 가능성이 높아진다. 또한 모든 일상생활을 컴퓨터에 의존하게 된다면 잠깐이라도 일상적 사물의 컴퓨팅의 정보처리가 중단될 경우 일상적인 삶마저 지속이 되지 않게 되는 우려가 생기게 된다. 때문에 유비쿼터스 IT는 인프라의 안전성 문제나 기술적 신뢰문제가 중요하다.

하지만 현행 정보통신법제에서는 아직 '유비쿼터스'라는 개념을 흡수하지 않고 있기 때문에 이러한 유비쿼터스 IT 인프라의 안전성 문제를 법제도적으로 해결할 방안이 없다. 이에 본 보고서에서는 우선 현행 정보화촉진법 제2조제1호상의 정의하고 있는 "정보" 개념을 유비쿼터스 환경에서도 적합하도록 "기록 또는 전자적 방식에 의하여 처리된 사항"으로 포괄적으로 규정하여 수동적인 정보 기록과 지능화된 사물간의 자동처리되는 정보를 포괄하는 개념 규정으로 바꾸어야 할 것으로 제시하

였다. 이를 통해 보다 안전한 정보통신 인프라를 마련할 수 있을 것이며, 정보 제공업자, 정보통신서비스제공자 또한 규정할 수 있을 것이다. 특히 RFID가 부착된 제품의 판매가는 현행법상 정보통신서비스제공자의 영역에 포함시키기 어렵다는 문제점이 있다. RFID가 고도로 발달하게 될 경우 하나만으로도 정보처리과정이 가능한 하나의 컴퓨터화 될 수 있으므로 RFID 제조업자는 물론 이를 부착한 상품 판매자를 “유비쿼터스 관련 정보서비스 사업자(가칭)”로 분류하여 RFID를 통한 정보서비스에 대한 권리 및 책임을 지게 할 수도 있을 것임을 제시하였다.

세 번째 유비쿼터스 IT로 인한 미래사회 이슈는 센싱이나 태그 확대로 인한 개인정보보호 및 프라이버시(privacy) 문제이다. 유비쿼터스 환경을 구성하는 핵심적인 기술 개념 중의 하나로 센싱과 태그를 설명하였다. 기존의 바코드와 달리 더욱 소형화되고 지능화된 RFID의 경우에는 일정한 정보를 기억하거나 상황을 인식하고 리더기를 통해 정보를 내보낼 수 있는 컴퓨터의 역할을 한다. 유비쿼터스에서 논의되고 있는 센싱(sensing)은 좁은 의미에서는 주변상황인식(context aware)을 하는 것이지만, 보다 넓게는 사물이나 사람, 시설물 등을 확인하고 그에 대한 정보를 저장할 수 있게 된다. 또한 지리적인 위치나 사물이나 사람들의 위치를 파악하는 역할도 수행한다. 이러한 센싱 기술의 특성상 유비쿼터스 사회는 사용자의 상황에 맞는 서비스 출현이 가능하게 되며(예컨대 LBS나 health care 등), 본 보고서에서 유비쿼터스 활성화 방안 중의 하나로 RFID를 통한 기업담보관리를 제시한바 있다. 물론 센싱이 보다 소형화되고 저가화, 저전력화가 되어야 널리 보급되고 일상생활 속에서 사용되게 된다. 하지만, 센싱이나 태그들이 일상생활 속에 널리 사용되게 되면 모든 일상생활을 인식하고, 확인할 수 있게 되는 가능성 또한 높아진다. 즉, 센서가 부착된 개인 주변환경에 대한 인지(context aware)나 확인(identification), 개인의 위치 및 이동 지역 확인을 통해 개인의 프라이버시를 침해할 위험성이 높아진다는 것이다.

프라이버시의 경우 기존에 정부 권력으로부터 나의 일상을 보호받을 권리였다면 점차 기술의 발달로 인해 여러 상업적 권력이나 타인에 의해 나의 일상이 침해받지 않을 권리 또한 중요해 졌다. 특히 본 보고서에서 개인 프라이버시 문제와 관련지어 살펴본 것은 현재 시행되고 있는 CCTV사례와 소비제품에 부착되는 RFID 사례

이다. CCTV는 직접적인 센싱 사례는 아니지만 이것이 좀더 소형화 되고 센서화 될 경우를 염두해 둔다면 개인 일상을 감시할 수 있는 도구가 될 수 있다. 하지만 아직 전자감시자비의 설치와 이용에 관한 적절한 법적 규율이 이루어지고 있지 않기 때문에 전자감시장비 설치의 주체, 설치장소, 장비의 종류, 운영방침, 절차 등에 대해 포괄적으로 규정하는 특별법을 제정할 필요성으르 제시하였다. 또한 미국이나 일본, EU 등에서는 옷이나 식품 등에 부착되는 RFID가 제품 구매 후에도 지속적으로 원격 리더기와 정보를 주고 받음으로써 소비자 감시, 식별을 통해 프라이버시가 침해될 우려가 있음을 시민단체 등에서 주장하여 정부적 차원에서 법안이나 가이드라인을 제정한 것을 살펴보았다. 현재 우리나라에는 RFID 도입 초기라 사업・서비스 차원에서는 이를 활성화 시킬 필요도 있기 때문에[154] 외국의 사례를 참고하여 자율규제형식으로 가되 기존의 개인정보보호법을 고려하여 적절한 지침이나 권고 형식의 연성법적 접근을 시도할 필요가 있음을 주장하였다.

네 번째 유비쿼터스 사회 이슈는 컴퓨팅(computing)이 서로 네트워크화 되어 컴퓨팅 파워의 폭발 시대가 올 것이라는 것이다. 유비쿼터스 IT는 기존의 IT제품(컴퓨터나 통신기기 등)은 물론 생활기기(냉장고, 세탁기, 청소기 등)는 물론 일상적으로 사용하는 사물(펜, 컵, 거울 등)등에 일정한 수준의 정보처리가 가능하도록 하는 컴퓨터 기능을 부여하게 된다. 따라서 이러한 컴퓨터 기능을 가진 사물들은 서로 네트워크화되어 정보처리를 하게 되는데 이러한 컴퓨팅 시스템이 외부로 네트워킹 되면서 개인의 정보를 외부에서 컨트롤이 가능해 질 수 있다. 다시 말하면, 네트워크화된 기기들의 정보를 외부 기업 등에서 소유하여 내부 기기들의 정보처리 과정을 통제하게 될 우려가 있다. 따라서 개인 정보를 개인이 소유하게 될 가능성이 희박해짐에 따라 유비쿼터스 환경에서는 개인정보보호문제가 더욱 중요해진다.

현행 개인정보보보법제는 텔레매틱스나 홈네트워킹 등 유비쿼터스 환경의 새로

154) 기업의 입장에서는 RFID를 도입하여 물류확인비용을 절감시키고 물류의 효율성을 높일 수도 있다, 또한 본 보고서에는 RFID 활성화를 위해 기업동산 담보물에 RFID를 부착시켜 담보관리의 효율성을 증진시킬 수 있도록하는 법제도적인 기반 마련을 주장하였다.

운 서비스의 정보 수집, 사용 유형 등을 포괄하지 못하고 있기 때문에 이 분야에 적용할 수 있는 정보보호원칙을 담은 가이드라인이나 지침을 제시하는 것이 바람직하다. 또한 센싱 기술의 발달로 소비자가 모르는 사이에 정보가 외부에서 읽혀질 수 있는 경우 정보주체의 권리강화를 위해 정보획득의 동의 획득은 물론 개인정보 안전성 확보를 위해 정보서비스 사업자들에게 관리적, 기술적 조치 의무를 부과하거나 사업자들에 대한 모니터링 체계를 규제하는 방안이 모색되어야 한다.

마지막 다섯 번째는 유비쿼터스 IT로 인해 자본이나 기계 등의 생산과정이 전개됨에 따라 노동의 사회적, 제도적 역할 변화가 불가피 할 것이라는 점이다. 유비쿼터스 IT는 단순노동뿐만 아니라 복잡한 정보처리, 조작, 시행이 가능해 짐에 따라 노동 구조의 변화가 예상된다. 예를 들면, 로봇을 통한 수술과 같은 복잡한 시행과정 뿐만 아니라 현재 시범적으로 실시되고 있는 RFID를 통한 도서관 자료 정리, 반납, 대출이 가능해지고 쇼핑 계산도 상품에 RFID가 부착되어 있으면 자동적으로 되기 때문에 도서관 사서나 계산원과 같은 단순 노동직업은 많이 사라질 것이다. 또한 본고에서 인용한 바와 같이 사업적 측면에서 RFID를 통한 물류관리는 관리시스템의 변화를 가지고 와서 단순관리업무직종의 감소가 예상된다. 본고에서는 유비쿼터스 사회의 도래에 따라 노동구조의 변화에 어떻게 대응할 것인가와 같은 상세한 설명이나 예시는 들지 않았지만 단순노동비율이 줄어들면서 지능을 기반으로 한 업무, 예를 들면 RFID 데이터 베이스 관리, 전자적 방식에 의한 기업담보관리 대행업체 등 새로운 직종의 고용창출효과도 발생할 것으로 예상된다는 점을 지적하였다.

각 나라의 IT 발전 특성에 따라 사용하는 용어들에 다소 차이가 있긴 하지만 유비쿼터스는 세계적인 IT의 흐름에는 분명하다. 유비쿼터스 IT는 지금과는 다른 사회적 패러다임을 가지게 될 것이며, 이에 따라 생활양식과 문화의 변화를 가져온다. 센싱이나 태그, 네트워크 커뮤니케이션, 사용자 인터페이스, 정보보안 기술과 같은 것은 단순한 기술 자체에 머무는 것이 아니라 사회전체에 퍼져서 이러한 사회 변화를 일으키는 구심점이 된다. 또한 이러한 기술적 발전들은 지속적인 경제발전, 기업 효율화를 위해 활성화시킬 필요도 있지만 사용계층을 제한시키는 디지털 디바이드나, 프라이버시 침해, 개인정보보호 등 역기능을 가져오기도 한다. 따라서 본 보고

서에서는 유비쿼터스 기술들이 가지고 올 사회문화적 변화를 살펴보고 이를 위해 필요한 법제도적 개념을 설정하고 대응방안을 살펴보았다. 본 보고서에는 거시적인 유비쿼터스 IT의 흐름을 파악하고 이에 따른 법제도적 방향을 포착하는 것에 초점을 두고 있기 때문에 세부적인 법제도적 제정이나 조항은 제시하지 않았지만 향후 진행될 u-Korea 전략에서 유비쿼터스 사회의 도래와 기술변화에 따른 법제도적 기반을 마련하는데 기초자료로 활용될 수 있을 것이다.

참 고 문 헌

강홍렬a. 2004. “국가전략수립을 위한 유비쿼터스의 의미”, KISDI 이슈리포트 04－23

강홍렬b. 2004. “유비쿼터스 논의에서 읽는 IT의 기술혁신방향”, KISDI 이슈리포트 04－26

권수갑. 2002. “Ubiquitous Network 구축전략”, ETRI 정보화기술연구소 산업전략연구부

_____. 2003. Ubiquitous Computing 개념과 동향. 전자부품연구원 전자정보센터

김동환. 2003. “유비쿼터스 공간의 경제와 경영전략”, Telecommunication Review. 13권, 1호

김완석・김정국・김효기・김창석・구홍서・이상범・박태웅・이성국. 2003. “유비쿼터스 컴퓨팅 기술과 인프라 그리고 전망”, 한국정보처리학회 유비쿼터스 컴퓨팅 특집 제10권 제4호

김완석. 2003. “유비쿼터스 컴퓨팅과 IT 메가트렌드”, 한국전자통신연구원(ETRI) 자료.

김재윤. 2003. “유비쿼터스 컴퓨팅: 비즈니스 모델과 전망”, 삼성경제연구소. 2003. 12.16.

김창환, “유비쿼터스 IT 최근 동향”, 전자부품연구원 전자정보센터

_____, “유비쿼터스 컴퓨팅 동향 분석”, 전자부품연구원 전자정보센터

김철수,『헌법학개론』, 박영사, 2000.

다카토 나츠이.2002. “상업적 목적 및 프라이버시 보호를 위한 위치기반서비스”, 2002 개인정보보호 국제 컨퍼런스 발표문, 2002. 11. 28.

렉 휘태커/이명균・노명현 역. 2001.『개인의 죽음』, 생각의 나무, 151면 이하 참조.

박승창. 2003. “유비쿼터스 IT의 2030년 사용자 시나리오(1)～(7)”, 전자부품연구원 전자정보센터(EIC)정보지

박세진. 2003. “유비쿼터스 사회실현을 위한 인간중심적인 접근,” 유비쿼터스 IT 포

럼 2003년 10월 3일 발표자료
박영충・정광모, “이동 Ad-hoc 네트워크 기반의 유비쿼터스 네트워크 기술동향 및 적용방안”, 전자부품연구원 전자정보센터
박우출・이석필・조위덕, “유비쿼터스 컴퓨팅 연구의 현황 분석”, 전자부품연구원 전자정보센터
박훤일,「남북경협의 확대에 대비한 북한 담보제도의 정비방안」, 집문당, 2004
_____, “미국의 부동담보제도－우리나라의 담보법제에 대한 시사점”,「비교사법」 제10권 4호, 2003. 12.
_____, “개정 미 동산담보법의 국내 담보법제에 대한 시사점”,「경희법학」 제37권 제1호, 2002. 12.
성낙인 외,『개인정보보호를 위한 정책방안 연구』, 정보통신부, 1999.
윤훈주. 2004. 유비쿼터스 컴퓨팅 & 네트워크, 2004년 7월 22일 KISDI 발표자료
_____, 2004.「유비쿼터스」, UBiU 강좌교재
이근호. “무선식별(RFID)기술”, TTA 저널, 제89호.
이석희. 2003. 정보통신미래포럼 조찬세미나 발표자료, 2003. 9. 30
이희욱, “세계는 지금 RFID행 Gold Rush”,「Economy21」, No.227, 한겨레이엔씨, 2003. 12. 7.
전황수. 2004. “중요국의 유비쿼터스 관련정책”, ERTI 정책지원자료
_____. 2003. “u-Korea 구축 추진방안”, ERTI 정책지원자료
최남희. 2002. “유비쿼터스 혁명이란 무엇인가?”, 2002년 8월 u-Korea 포럼 준비반 워크샵 발표자료
_____.2003. “유비쿼터스 정보기술을 활용한 물리공간과 전자공간 간의 연계구도와 어플리케이션 체계에 대한 연구”, Telecommunications Review・제13권 1호
하원규. 2003. “u-Korea 구축전략과 행동계획: 비전, 이슈, 과제, 체계”, Telecommunication Review. 13권, 1호
CEO Report. 2003. IT의 뉴패러다임 ‘유비쿼터스’
사카무라 겐 지음, 최윤식 옮김,「유비쿼터스 컴퓨팅 혁명」, 동방미디어(주), 2002, 8

－11면.

RFID조사연구회, 2003.「전자태그의 고도활용을 위한 대처방안」

한국소프트웨어감정연구회,「S/W 등 디지털정보재산권 가치평가 및 담보제도 도입에 관한 연구」, 프로그램심의조정위원회, 2002. 11.

한국전산원. 2004.「e-비즈니스 동향」, 2004. 10.

Andrew Sparrow.1998. “Car Tagging May Help Cut Theft, Say Minister,” Daily Telegraph (London), Oct. 17.

FCC, 1999. *Third Report and Order in the Matter of Communications Assistance for Law Enforcement Act*, Aug. 26, 1999.

Francis S. Chlapowski. 1991. “The Constitutional Protection of Informational Privacy,” 71 *Boston University Law Review* 133.

Hansjürgen Garstka, “Data Protection and Freedom of Information,” 2002 개인정보보호 국제 컨퍼런스 발표문, 2002. 11. 28.

Paul M. Schwartz. 1999. “Privacy and Democracy in Cyberspace,” 52 *Vand. L. Rev*. 1609

Mark Weiser. 1991. “The Computer for the 21th Century”, Scientific American, 265(3), pp.94～104

Mark Weiser. 1993. “Hot topic; Ubiquitous Computing”, IEEE Computer.

Margaret M. Russell. 1995. “Privacy and IVHS: A Diversity of Viewpoints,” 11 *Santa Clara Computer & High Tech. L. J.* 145

Michael Froomkin. 2000. “The Death of Privacy,” 52 *Stanford Law Review* 1461.

Roger Clarke. 1987. “Information Technology and Dataveillance,” Version of November 1987.

S. Engel-Flechsig 1997. “IuKDG vom Budestag verabschiedet. Änderungen des TDDG und des SiG,” *DuD*

日本ユビキタスネットワーク時代における電子タグの高度利活用に關する調査研究會,「電子タグの高度な利活用に向けた取組」(最終報告書), 2004. 3.

日本 企業法制研究會(擔保制度研究會) 報告書,「不動産擔保から事業の收益性に着目

した資金調達へ」, 経済産業省, 2003. 1.

http://www.theorator.com/bills108/hr2405.html.

http://www.fcc.gov/Bureaus/Engineering_Technoloy/Orders/1999/fcc99230.wp.21

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_billf:s1164is.txt.pdf

http://www.securitydirect.co.uk/en-gb/dept_101.html

http://www.informationcommissioner.gov.uk

http://news.bbc.co.uk/1/hi/england/manchester/3043931.stm

http://e-privacy.or.kr/mailing/Mailimg/newsletter/200401/B/pds/CCTV.pdf

http://e-privacy.or.kr/mailing/Mailimg/newsletter/200401/B/pds/CCTV.pdf

http://www.fcc.gov /Bureaus/Engineering_Technoloy/Orders/1999/fcc99230.wp.

http://www4.law.cornell.edu/uscode/47/551.html

http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html