



RFID/USN시대의 사생활보호의 법적 문제

정준현
(선문대학교)

목 차

1. 서 론
2. USN사회와 RFID 그리고 문제점
3. USN사회와 개인정보보호법제
4. 결 론

1. 서 론

현대정보화사회는 현실의 생활인이 사회의 변화·발전을 인식하고 그에 상응하는 자신의 생활방식을 타인이 정당한 권리에 대한 충돌없이 합리적으로 결정하게 하는 것을 불가능하게 할 정도로 급변하고 있다. 특히, RFID의 발전·활용에 따라 USN사회로 치닫고 있는 작금의 정보사회에 대한 일반인의 적응력이나 개인인격의 보호문제에 대한 윤리적 내지 법제적 대응이 채 성숙되기도 전에 언제 어디서나 개인의 흔적을 감지하여 전자적 기록으로 남기게 되는 소위 USN사회로의 발전이 도모되고 있어, 개인이 제3자에 의한 전자적 감시로부터 자유로운 공간은 점증적으로 전무하게 될 것으로 예측된다. 요컨대, 정보화가 고도화되면 될 수록 자신의 공개를 통한 실시간 수요의 충족에 대한 의존도는 커질 수밖에 없고 그만큼 개인지배의 문제는 커지게 된다고 할 것이다.

이러한 점에서 자신의 공개를 전제로 하면서도 공개된 자신이 제3자나 국가기관에 의해 불법

적인 목적에 악용될 가능성이 높은 USN사회로부터 국가에 의해 보호되어야 할 개인의 기본적 가치를 헌법적인 관점에서 출발하여 관련된 몇 가지의 개별법적인 문제를 검토해볼 필요가 있다.

2. USN사회와 RFID 그리고 문제점

2.1 유비쿼터스 컴퓨팅 사회

유비쿼터스 컴퓨팅은 “언제 어디서나 존재한다”는 의미의 라틴어인 ‘Ubiquitous’와 컴퓨팅이 결합된 단어로 “언제 어디서든 어떤 기기를 통해서도 컴퓨팅할 수 있는 상태”를 의미하며, 유비쿼터스 컴퓨팅 사회는 이러한 컴퓨팅 시스템에 의존하게 되는 사회를 의미하게 된다.

이처럼 “모든 물건에 컴퓨터를” 또는 “사라지는 컴퓨팅”을 내용으로 하는 유비쿼터스 컴퓨팅 사회는 무한대의 고유식별번호 부여를 가능하게 하는 “IPv6”의 기술개발로 도로·다리·터널·빌딩·건물 벽·천장·화분·냉장고·구두·시계·종이·물 컵·책상 등 도시공간을 구성하는 수많은 환경과 대상물 속에 RFID 칩을 심

을 뿐만 아니라 인간의 인체에도 칩을 이식하거나 입는 컴퓨터를 통하여 인간을 포함한 모든 사물과 대상이 능동화되고 전자공간에 연결되어 서로 정보를 주고받는 현실공간과 사이버공간이 공존하는 사회로 진화될 것이다. 이러한 사회에서는 개인과 개인의 수요를 실시간으로 제공할 서비스제공자는 언제 어디에서나 끊임 없는 접속(Ubiquitous Access)을 하게 되는 결과 개인의 다양한 수요를 충족시킬 뿐 아니라 갑작스러운 병이나 위기로부터 개인구제를 가능하게 하는 등 우리 삶의 질을 획기적으로 발전시킬 수 있는 반면, 개인의 일거수일투족은 서비스제공자의 전자적 기록으로 DB에 수록되어 개인정보를 보유한 서비스제공자는 언제든지 개인지배자로 대두될 가능성 또한 배제하기 어렵다.

2.2 RFID

RFID 태그는 물체에 부착될 수 있는 소형 안테나에 연결된 미세 칩으로 가장 보편적으로 운용될 것으로 생각되는 방식은 전세계에서 생산되는 모든 상품에 대해 고유식별부호를 갖는 마이크로 칩을 부착하여 인식할 수 있도록 하여, RFID 리더가 전파부호를 송출하면 인근에 있는 태그가 저장된 데이터를 리더에 송출함으로써 프로그램에 따라 반응하게 하는 방식이다. 현재 수동형 RFID 태그의 판독범위는 1인치 이하에서 9미터 이내인 반면 능동형은 보다 먼 거리의 판독능력을 갖는다고 한다.

2.2.1 RFID가 갖는 기본적 자유에 대한 위협

RFID의 유용한 활용이 있는 반면 일부기술을 사생활의 비밀권 등 개인의 기본적 자유를 위협하는 방법으로 오용될 소지가 있다. 이러한 위협의 근거를 이루는 요소로는 ① RFID 태그는 당사자도 알지 못하는 상태에서 물건이나 문서의 내외부에 부착될 수 있다는 ‘태그의 은닉성’(Hidden placement of tags), ② 지상의 모든 물건에 대해 부여되

는 고유식별부호(전자제품부호; EPC)의 사용은 범세계적 상품등록시스템을 가능하게 할 것이고 이 시스템에서는 모든 물건이 판매 또는 이동되는 즉시 식별되어 구매자나 소유자로 연결되게 되는 것을 가능하게 하는 ‘모든 물체에 대한 고유식별부호’(Unique identifiers for all objects worldwide), ③ RFID의 설치에 고유 태그 데이터를 포함한 대량의 DB의 창출을 요구하고 이들 DB는 개인식별데이터로 연결될 수 있다는 것과 관련한 ‘데이터의 대량 수집’(Massive data aggregation), ④ RFID 태그는 사람 또는 상품이 모여 있는 어떠한 환경에서나 보이지 않게 설치될 수 있는 판독기를 통해 가시권 밖에서도 판독될 수 있어 실시간 소비자 등을 검색하게 하는 것을 가능하게 하는 것과 관련한 ‘은닉된 판독기’(Hidden readers) 및 ⑤ RFID 태그 번호를 통해 본인확인이 이루어지면 해당 개인이 인식하지 못한 상태에서 또는 해당 개인의 동의없이 그 개인에 대한 프로파일 및 추적이 가능하게 된다는 것과 관련한 ‘개인추적 및 프로파일링’(Individual tracking and profiling) 등이 제시되고 있다.

2.2.2 RFID의 사용과 사용의 한계

RFID의 사용에 있어서 소비자의 기본적 자유의 보장은 상품의 공급에서 최종 소비과정의 흐름에 대한 사업자의 이익 보다는 중시되어야 한다. 요컨대 소비자의 구매 시점 이후부터는 추적당하지 아니할 개인의 권리가 존중되어야 할 것이다. 개인과 사회에 대한 RFID의 잠재적인 유해성을 완화하고 소비자의 권익을 보호하기 위해 다음의 3가지 원칙이 제안되고 있다.

첫째, RFID에 대하여는 기술평가가 이루어져야 하며 이러한 평가가 있을 때까지 RFID 태그는 개인 소비자의 제품에 부착되어서는 아니된다. 둘째로, RFID의 장착은 개인정보보호와 관련하여 정착된 관행, 예컨대 OECD 8원칙 등에 합치되어야 한다. 끝으로, 다음과 같은 목적의 RFID 사용은 엄격하게 금지되어야 한다. 즉, 소

비자가 구매하는 상품에 태그 부착을 강요하는 행위, 개인에 대해 RFID 태그와 판독기의 탐지를 허용하지 않거나 개인 소유의 물건에 부착된 태그의 활동을 중지시킬 수 없도록 하는 행위, 정보주체의 '설명을 통한 동의'(full informed Consent)나 서면 동의없이 특정개인의 추적을 위해 RFID를 사용하는 행위, 기타 익명성을 제거하거나 완화시킬 목적의 RFID 이용행위 등은 허용되어서는 않된다.

다만, 인간의 생명이나 건강과 직결되는 치료 약 등은 불법적인 목적에의 오남용 방지나 유효기간의 감시 등을 목적으로 제조시점에서 투약시점까지의 추적을 위한 RFID 태그의 사용이나, 제품이 공급망을 통해 배송되는 과정에서 분실되거나 도난당하는 것을 예방하거나 해당 제품에 적합한 취급을 보장하기 위한 RFID 태그의 사용(이 경우 태그는 상품의 포장외부에 부착하여 소비자에게 인도되기 전에 영구 제거되어야 한다) 또는 재화의 재활용과 특정 유해 폐기물의 무단방치를 방지하기 위한 RFID의 사용 등은 적극 권장되어야 할 것으로 생각된다.

2.3 USN사회의 문제점

종래 빅 브라더로 표현된 개인지배에 대한 위협은 통상 정부에 의한 개인정보의 일원적 관리에 대한 상징적인 표현으로 사용된 것이었다. 그러나 오늘날에는 많은 서비스제공자가 대규모의 개인정보 DB를 구축하고 있는 결과 이들 중에는 정부 기관이 보유한 것 이상의 개인정보를 보유한 기업이 적지 않고, 수집·축적된 개인정보가 당초의 목적과는 별개의 목적으로 이용될 기회도 적지 않은 것이 현실이다.

이러한 현실을 두고 뉴욕주의 사법부장관은 “계약회사가 아무런 관계없이 서점이 보유하고 있는 정보를 입수하는 것을 가능케 할 필요성이나 금융기관이 신용카드 신청서나 구매품목에 관한 정보를 판매할 수 있도록 할 필요가 있는

것인가” 하는 의문을 제기하면서 기술개발에 따라 상용목적으로 개인정보를 수집·분석 또는 이용하는 것이 비약적으로 증가하는데도 연방 및 주에서는 대부분 이러한 정보의 수집이나 이용을 금지하고 있지 않다면서, “현재 내가 두려워하는 것은 빅 브라더(Big Brother)가 아니라 빅 브라우저(Big Browser)” [1] 라고 하여 서비스업자를 경계하였다.

그러나, 유비쿼터스 컴퓨팅 사회는 「드러난 컴퓨팅에 의해 한정된 공간에서 일정한 명령행위에 의해 개인 행적을 어느 정도 분산·디지털화하는」 기존의 정보화 사회와는 달리 「곳곳에 놓여진 RFID를 통해 일정한 명령행위 없이(Just Its) 언제 어디에서나 개인의 행적을 집약적·전자적 기록으로 남기는」, 전자적인 측면에서는 일정한 목적범위 내에서 개인을 완전히 발가벗기는 사회라고 할 수 있고 그 점에서 어느 누구의 적극적 또는 소극적 간섭으로부터 벗어나 자신의 창의와 개성을 자유롭게 발현하는 것을 내용으로 하는 인간의 존엄과 가치의 실현이 위협받는 사회라고 할 수 있다.

3. USN사회와 개인정보보호법제

3.1 USN사회와 개인위협

앞에서 살펴본 바와 같이 USN사회에서는 RFID를 통해 개인은 일정한 목적범위 내에서 완전히 공개되며, 실시간 서비스를 제공하게 될 사업자나 국가기관 등은 개인 데이터를 실시간으로 수집·저장·처리할 수 있게 됨으로써 한정된 재화를 통해 최적생산과 공급 또는 맞춤형 서비스를 제공함으로써 경영이익 내지 효율의 극대화를 꾀할 수 있는 반면, 인간은 컴퓨터에 의해 프로그램화된 생활의 노예 내지는 개인정보를 다량으로 보유한 자에 의한 지배로부터 자유로울 수 없게 될 위험 아래 놓이게 되며, 이는 헌법이 보장하고 있는 인간 본연의 가치에

반하게 된다.

3.2 헌법상 인간의 존엄과 가치

우리 헌법 제10조는 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다”고 먼저 규정한 다음 헌법 제11조의 평등권에서 제36조의 양성평등을 기초로 하는 혼인 및 가족생활권 등에 이르기까지 인간의 존엄과 가치 및 행복을 보장하기 위해 필요한 각종 기본권을 규정하고 마무리로 제37조제1항에서는 열거되지 아니한 자유와 권리도 경시되어서는 아니한다는 점을 명시하고 있다.

그런데 USN사회는 개인의 공개를 전제로 한다는 점에서 헌법 제17조의 사생활비밀권을 필두로 제18조의 통신비밀권을 침해할 가능성이 높으며 그밖에 헌법 제21조에 내포되어 있는 표현자유권과 표현의 자유의 한계로서 타인의 명예권 등을 침해할 가능성 또한 배제할 수 없게 된다. 이러한 USN 사회의 위협으로부터 개인의 존엄과 가치를 구현하기 위해 국가는 헌법 제10조와 제37조에 의거하여 국가기관에 대해서는 국가안정보장을 위해 법률로 정한 필요한 최소한의 범위에서 이들 권리를 제한할 수 있는 입법을, 그리고 개인정보를 보유한 사인에 대해서는 개인정보의 수집·저장·처리 및 이용의 각 단계별로 이들 권리가 침해되지 아니하도록 하여 질서를 유지하고 공공복리를 실현하기 위해 필요한 최소한의 규제를 행하는 입법을 각각 조치할 책무를 부담하게 된다.

3.3 USN사회의 위협과 인격권

3.3.1 인격과 인격권

인격과 인격권에 대한 사전적 의미를 찾아보면, 인격은 “인간에게서 비교적 일관되게 나타나는 성격 및 경향과 그에 따른 독자적인 행동

경향” [2] 을 의미하는바, 구체적으로는 특정 개인의 사회·경제·문화 등 다양한 방면에 있어서 지속적인 생활양태나 습관 또는 언행 등으로 이해할 수 있다. 이것은 정보사회의 관점에서는 개인에 관한 신상정보나 거래정보 또는 각종 취미활동정보 등 개인화작업을 통해 개인을 특정시킬 수 있는 개인정보로 이해할 수 있을 것이다. 다른 한편, 인격권이란 “권리의 주체와 분리할 수 없는 인격적 이익을 내용으로 하는 권리 즉, 생명·신체·자유·정조·이름 등을 목적으로 하는 사권(私權)으로서 현행 민법은 타인의 신체·침해하면 불법행위를 구성한다고 규정(751조)함으로써 소극적으로 그 보호를 규정할 뿐이고 그 이상의 규정은 없다”고 설명하고 있어, 정보사회에 합치될 수 있는 가분적이고 적극적 통제의 대상이 되는 개인정보에 대해 현행 법제는 별도의 인격권을 관념하고 있지 않다[3].

3.3.2 개별법상의 인격권

우리 법상 인격권을 명문으로 규정하고 있는 예는 없고 인격권의 의미에 대하여도 다의적이지만[4] 주로 생명·신체·건강 등의 신체적 측면과 명예·초상·사생활비밀 등 정신적 속성의 보호이익으로서[5], 그 자유로운 발전을 위하여 제3자에 의한 침해에 대해 보호되어야 할 이익의 총체라고 할 수 있다. 그런데 명예, 프라이버시, 초상 등 인격적 이익을 이루는 이들 개별적 보호법익에 대한 침해는 주로 타인이 제3자에 향하여 전파한 정보 또는 본인에 대해 발하여진 정보에 의하여 야기된다. 그러한 점에서 개인의 생활습관이나 병력, 기호 등 개인에 관련된 모든 정보는 일단 해당 개인의 일신전속적 人格材로서 전적으로 정보주체의 자기결정권의 지배를 받게 된다고 할 것이다[6].

3.3.3 판례상 인격권

판례가 “... 개인의 명예나 사생활의 자유와

비밀과 같은 사적 법익도 보호되어야 할 중요한 가치를 가지는 것이고, 인격권으로서의 개인의 명예의 보호와 표현의 자유의 두 법익이 충돌하는 경우 … 더욱이 오늘날의 보도기관이 영리추구의 입장에서 공·사인의 프라이버시에 속하는 사항을 즐겨 보도하는 경향이 있는 점 등을 고려하여 개인의 인격권 보호라는 이익을 최대한 배려하여야 할 것이다”[7]고 한 것이나 명예훼손을 이유로 한 손해배상청구사건에서, “… 헌법 제9조 후단에서는 ‘모든 국민은 … 행복을 추구할 권리를 가진다’라고 하여 생명권, 인격권 등을 보장하고 있어 어떤 개인이 국가권력이나 공권력 또는 타인에 의하여 부당히 인격권이 침해되었을 경우에는 인격권을 이유로 그 침해행위의 배제와 손해배상을 청구하여 그 권리를 구제받을 수 있도록 하고 있다. … 표현의 자유는 가끔 개인의 명예나 사생활의 자유와 비밀 등 인격권의 영역을 침해할 경우가 있는데 표현의 자유 못지않게 이러한 사적 법익도 보호되어야 할 것이므로 인격권으로서의 개인의 명예의 보호(헌법 제9조 후단)와 표현의 자유의 보장(헌법 제20조제1항)이라는 두 법익이 충돌하였을 때 그 조정을 어떻게 할 것인지는 구체적인 경우에 사회적인 여러 가지의 이익을 비교하여 표현의 자유로 얻어지는 이익, 가치와 인격권의 보호에 의하여 달성되는 가치를 형량하여 그 규제 폭과 방법을 정해야 할 것이다”라고 판시[8]한 것은 모두 개인정보의 인격성을 인정한 예라고 할 것이다.

3.4 현행 개인정보법제의 특징과 문제점

개인정보보호를 규정하고 있는 「정보통신망이용촉진 및 개인정보보호에 관한 법률」 등 현행 개인정보보호법제는 대부분이 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특

정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)”로 규정하여 개인에 관한 정보 중 해당 개인을 식별할 수 있는 정보로서 개인의 인격권 중 사생활비밀권 및 명예권의 보호를 위한 정보자기결정권을 규정하고 있다. 그 결과 개인정보를 이용한 분배의 최적화나 DB산업의 발전가능성을 비롯한 유비쿼터스 컴퓨팅 사회의 발전을 위한 방향제시규범은 전무한 상태에 놓여 있다.

다시 말하자면, 사생활비밀권이나 명예권 등 인격권의 외형적인 보호에만 치중한 결과 개인 지배의 수단이 되는 주민등록번호나 이름 등을 익명화한 그러면서도 본인확인인 공적 증명력을 갖춘 대체수단을 규율하는 법제정비가 없는 결과 사업자는 수집된 개인정보를 활용할 수 없게 되어 DB산업의 활성화와 USN사회의 구현이 장애를 겪고 있는 것이다. 정보사회에 있어서 정보주체와 정보보유자의 ‘원-원전략’ 차원에서 수집 단계에서부터 식별할 수 없는 그러나 해당 개인에 대해서는 실시간 서비스가 가능한 개인정보의 수집·처리 법제를 구상할 필요가 있다. 이러한 점에서 현재 온라인의 익명성 내지 비대면성을 극복하기 위한 수단인 동시에 개인지배의 수단으로 지목되고 있는 ‘주민등록번호’를 대체할 본인확인수단에 대한 대안입법이 화급하다[9].

4. 결론

유비쿼터스 컴퓨팅 사회가 개인의 사생활비밀을 포함한 인격권을 보호하지 못하는 전체주의적 사회로 흘러 모든 사람의 행동이나 생각이 다른 사람에게 투명하게 되는 결과 자신의 생각이나 감정 또는 내적 생활을 더 이상 자유롭게 가질 수 없게 된다면 개인의 자율과 조화를 바탕으로 하는 우리 헌법의 기본적 틀인 자유민주적 기본질서는 파괴될 수밖에 없을 것이다. 이러한 이유에서 헌법 제10조와 헌법 제37조 그

리고 개인과 기업의 경제상의 자유와 창의를 존중함을 기본으로 경제질서를 규정한 헌법 제119조로부터 자유민주적 기본질서를 구성하는 개인의 인격권을 침해하는 각종 불법행위에 대하여는 시장자율규제에 대한 보충적 규제로서 최소의 정부규제를 해야 할 국가의 기본적 책무를 발견할 수 있다. 이러한 헌법 정신을 종합할 때, 한편으로는 개인의 공개 없이는 성립될 수 없는 유비쿼터스 사회가 공개된 개인정보를 토대로 개인을 유린하는 전체주의사회가 되지 아니하도록 하는 개인보호와 아울러 다른 한편으로는 수집·처리된 다종다양한 개인정보가 갖고 있는 재화가치의 극대화를 통한 복리증진과 재화의 적정배분이라는 두 가지의 목적을 달성하기 위해 공적 증명력이 있는 그러나 식별하기 어려운 본인확인수단(공인된 주민번호대체수단)을 도입하는 법제의 개발이 시급하다고 할 것이다.

참고문헌

[1] John Caher, "Big Browser has replaced Big Brother", NYAG Says(January, 24, 2000) <<http://www.nylj.com/stories/00/01/012400a2.htm>>.
 [2] <http://100.naver.com/100.php?id=129066> <2005.5.15. 접속>.
 [3] 송영민, "첨단의료와 인격권", 인권과 정의, 제345호, 30쪽 이하 참조.
 [4] 金炯坤, 자연법이론의 기본적인권예의 수용에 관한 연구, 경남대 박사학위논문, 1990, 126면.; 洪春義, 인격권의 보호에 관한 연구, 전북대박사학위논문, 1990, 9면; 星野英一, 私法における人間, 基本法學(1), 岩波書店, 1983年 참조.
 [5] 19세기의 프랑스·독일 등의 근대 민법전은 인격권을 명시적으로 인정하지 않았고 1907년 스위스민법 제28조에서 처음으로 명시적으로 인정하였다. 학설로는 19세기말 독일

에서 주장되고 제2차세계대전 후 판례를 통하여 일반적으로 승인되었다.

[6] 독일의 경우 연방정보보호법은 일반적인 인격권에서 나오는 독자적 정보권(Recht am eigenen Datum)을 보호한다는 견해와 일반적인 인격권만을 보호하는 것이 아니라 4개의 이익영역, 즉 ①개인정보의 처리에 대한 통지이익, ②정보의 정정에 대한 이익(정보의 정확성과 완전성), ③개인정보의 목적에 적합한 처리의 이익 및 ④사적 영역을 보호한다는 견해로 나누어진다. Diethelm, "Deliktsrechtliche Problem des Datenschutzes", Betriebs - Berater 1983, S.414.
 [7] 서울민사지방법원 1989.7.25, 88가합31161 판결. 언론중재 1989. 가을, 175면 참조.
 [8] 대법원 1988.10.11, 85다29 판결.
 [9] 이와 관련하여는 한국정보보호진흥원, "인터넷 상의 주민번호 대체수단 정책워크샷", 2005. 7.28. 및 정준현, "개인정보보호법제 현황과 법제정비의 필요성", 민간부문의 개인정보보호에 관한 법률 제정 공청회(2004.5.21.) 등 참조.

저자약력



정준현

1982년 성균관대학교 법률학과(학사)
 1984년 성균관대학교 법학과(석사)
 1991년 고려대학교 법학과(박사)
 1986년~1996년 법제처 법제연구담당관
 1997년~현재 선문대학교 법학과 교수
 관심분야: 지방자치법, 행정작용법, IT개인정보보호법제, 사이버테러방지법제