

사이버 프라이버시는 없다(?)

연재순서	1. 사이버스페이스의 정체
	2. 사이버상의 음란
	3. 사이버상의 명예훼손
	▶ 4. 사이버상의 프라이버시
	5. 사이버상의 저작권
	6. 디지털콘텐츠의 유통과 관련된 법적 문제

명예훼손에서 '사실의 적시'는 사실을 직접적으로 표현한 경우에만 한정되는 것은 아니고, 간접적이고 우회적인 표현에 의하더라도 그 표현의 동기와 의도가 그와 같은 사실의 존재를 암시하고, 또 이로써 특정인의 사회적 가치 내지 평가가 침해될 가능성이 있다면 명예훼손의 요건을 만족시킬 수 있다. 그렇다면 사이버스페이스에서의 명예훼손은 어디까지이고 어떤 표현을 구체적인 명예훼손으로 인정해야 하는지 그 범위와 개념에 대해 알아보고, 사이버스페이스에서의 명예훼손을 방지하기 위한 제도적, 기술적 대책 등에 관해 사례 중심으로 살펴본다.

글 / 성선제 가톨릭대 법학과 교수

프라이버시의 기원은 저 멀리 성경에서부터 찾을 수 있다. 노아의 홍수 후 노아가 포도주를 마시고 취해 벌거벗은 채로 천막 안에 누워 있는 모습을 본 아들 햄이 밖에 나가 형과 아우에게 이야기를 했다. 노아는 술이 깨어 아들 햄이 한 일을 알고 크게 꾸짖었다. 일찍이 성경에서부터 프라이버시를 간접적으로 인식하고 그 중요성을 강조했다고 평가할 수 있다.

프라이버시에 대한 법적 보호는 20세기에 비로서 커다란 이슈가 됐지만 그 인식의 기원은 고대 서구사회의 오랜 사회적 관습 및 규범들에서 찾을 수 있다. 그리스 시대 이후로 서구 사회는 인간의 사회영역을 사적영역과 공적영역으로 구분해 이해해 왔으며 그 구분개념으로 인간의 본성 및 국가와 개인의 적정한 역할을 사용해 왔다.

'공적인 것'과 '사적인 것'의 구분에 대한 오늘날의 인식도 그리스와 로마 시대의 개념과 많은 부분에서 일치하고 있다. 가정 또는 가족이 사적영역의 중심에 있다는 것이 중요한 공통점이다. 가정에서의 프라이버시는 사회적 관습·문화·종교 및 법적

전통에서 서구 역사상 적극적인 가치로 인정돼 왔다. 이것은 '인간의 가정은 그의 성이다'라고 간결하게 표현하고 있는 법언에서도 알 수 있다. 이는 은신처 및 보호의 장소로서 가정을 강조한 것으로 명시적 허락 없이는 누구도 다른 사람의 집에 들어갈 수 없다는 고대법의 원칙을 의미하는 것이다.

프라이버시와 공동체의 관계는 사회의 종류에 따라 적대적이기도 하고 아니기도 하다. 전체주의사회인 경우 그 본질은 사적인 것에 대해 공적인 것을 완전히 확대한다. 그것은 '프라이버시의 모든 면을 청산할' 때까지 전체주의자들이 사회라고 부르지 않는 것과 같다. 이러한 인식에 의하면 프라이버시와 공동체는 완전히 정반대의 모습을 갖게 된다. 반대로 자유민주주의사회에서 프라이버시는 어떤 가치보다도 큰 지지를 받는다. 프라이버시는 개성과 관련이 있으며 개성의 발전은 자유와 연결돼 있으므로 자유주의와 연결되고, 선거의 자유, 결사의 자유 등을 뒷받침하는 것이므로 민주주의와 밀접한 관련을 갖게 된다.

그리고 프라이버시는 복지 및 평등과도 충돌하지 않는다. 이

것은 복지와 평등의 문제가 프라이버시와 공통적으로 인간의 기본적인 권리에 해당하는 것으로 파악하려 하기 때문이다. 다른 한편, 프라이버시 개념이 개인뿐만 아니라 단체도 포함하는 것으로 확대된다면 프라이버시에 관한 주장들은 복지 및 평등의 이념과 충돌할 수도 있다. 이러한 경우 이들을 어떻게 조화시킬 것인가가 문제된다.

한편 프라이버시에 대한 권리인정이 공동체의 설립과 유지를 위협하고 사회적·정치적 무책임을 조장한다는 비판이 있다. 그러나 자립의 정신을 고취시키는 것이 프라이버시와 관련된다고 생각하는 것은 자연스럽다고 할 수 있으나, 프라이버시의 인정과 공동체의 설립과 유지의 위협은 본질적으로 관련이 없는 사회현상으로 이해할 수 있다.

한국인의 프라이버시 관념

우리는 수천년 동안 농경을 위주로 한 공동체 생활을 영위해 왔다. 그래서 전통적인 한국사회에서는 프라이버시라는 관념이 발달할 여지가 거의 없었다. 즉 대가족제도에서 가족 구성원 모두가 협동생활을 했으므로 당연히 프라이버시가 형성되기 어려웠다. 서구의 기준으로는 가장 프라이버시가 요구되는 혼례식 후 첫날밤의 장면을 공공연히 훑쳐보기 위해 창문에 구멍을 내는 일이 전통으로 이어 내려져 온 것을 보면 과연 우리에게 프라이버시 관념이 존재했을까 하는 의문이 든다.

우리의 프라이버시 관념에 대한 문헌을 찾아보기는 쉽지 않다. 하지만 조선 말 개화기 초 우리나라에 들어온 외국인의 눈에 비친 당시의 조선사회는 한국인의 프라이버시 관념을 이해하는데 도움이 될 수 있다. 개화기 초 심지어 비숍 여사가 쓴 기행문에 의하면 그녀가 여관에 투숙했을 때 한 순간에 문의 창호지들이 찢겨지고 사람들이 방으로 들어와 신기하게 생긴 그녀의 얼굴을 만져보고 머리를 잡아당기고 팔을 꼬집으며 그녀를 관찰했다. 그들은 외국인에 대한 호기심을 인정하면서도 한국인의 프라이버시 관념이 희박함을 간접적으로 지적했다.

지금도 사람들은 모르는 사람으로부터 우편물이 배달됐을 경우 프라이버시 침해로 불쾌감을 느끼는 이는 많지 않다. 예컨대 자신이 한번도 이용하지 않은 백화점의 실명 광고 우편물이 배달됐을 경우 자신의 성명과 주소에 대한 프라이버시 침해에 대한 인식보다 오히려 자신의 사회적 신분이 외부에 공표된 것으로 여기고 이것을 자랑스럽게 여기는 경우가 보통이다. 이런 현상들을 종합해볼 때 우리는 아직도 프라이버시라는 관념이 미약

하다고 할 수 있다.

우리는 전통적으로 단일민족으로서의 삶을 영위해 오면서 공동체로서 타인에 대한 관심이 그 누구보다도 강한 삶을 살아 왔다. 따라서 전통적으로 우리에게서 서구적 의미의 프라이버시 관념이 희박하거나 없었다고 해도 과언이 아니다.

우리에게 프라이버시 또는 사생활 관념이 도입된 것은 근대화 이후의 일이라고 할 수 있다. 그러므로 근대화 이후 최근까지도 우리의 관념은 프라이버시 또는 사생활 침해에 대해 상당히 너그러운 태도를 보이고 있었다. 즉 프라이버시 침해에 대해 관용적인 편이었으며 이에 대한 사회적, 법적 문제제기에 대해서 오히려 별로 대수롭지 않은 것을 가지고 야단법석이나는 등의 반응을 보이곤 했던 것이 사실이었다. 더욱이 프라이버시 침해에 대해 문제를 제기하는 자를 이상하게 여기는 풍토마저 존재하고 있었다.

그러나 우리사회도 점점 프라이버시 또는 사생활의 중요성을 인식하기 시작하면서 프라이버시 관념이 급변하고 있는 시점이라고 평가할 수 있다. 여기에 급격히 도래한 IT 사회는 이제 우리에게도 프라이버시 또는 사생활이 남의 일이 아닌 우리 자신의 중대한 문제임을 인식하게 해 줬다. IT 사회로 급격한 변화중인 21세기 한국 사회에서 프라이버시의 문제가 제기되는 것은 한국인의 타인에 대한 남다른 관심과 이를 손쉽게 가능하게 하는 IT가 그 원인이라고 할 수 있다.

프라이버시의 의의

우리 헌법은 프라이버시를 '사생활'의 비밀과 자유로 파악하고 있으며 별도의 프라이버시라는 용어를 찾아볼 수 없다. 한편 프라이버시에 대해 사생활의 소극적인 면을 뛰어 넘어 적극적인 처분권을 인정하는 견해가 독일 헌법의 영향을 받아 최근에 '정보자기결정권'이라는 개념을 사용하고 있다.

그리고 IT 사회의 도래로 인해 컴퓨터 네트워크를 통한 정보의 집중이 문제시되면서 '개인정보(personal data, 또는 personal information)'라는 개념이 유럽과 OECD를 중심으로 사용되기 시작했고 이것이 우리나라에 도입돼 정보통신망법을 비롯한 개별입법에서 사용되고 있다. 그리고 미국에서는 IT 사회의 도래 전후를 불문하고 전통적으로 '프라이버시'라는 용어를 사용하며 그 범위를 포괄적으로 이해하고 있다. 이하에서는 범위가 포괄적인 프라이버시를 주로 사용하고 실정법이나 특수한 의미를 나타내는 경우에는 적절한 다른 개념을 사용할 것이다.

우리 헌법은 인간의 존엄과 가치, 주거의 평온을 보장하는 주거의 자유, 통신의 비밀을 위한 통신의 자유, 그리고 일반적인 사생활의 비밀과 자유를 프라이버시 보호를 위한 헌법적 근거로 제시하고 있다. 그 중에서 인간의 존엄과 가치는 한 차원 높은 근거이다. 또한 사생활의 비밀과 자유는 헌법의 주거와 통신의 자유를 제외하는 인격권을 비롯한 내밀영역과 비밀영역 및 사적영역 그리고 사회적 영역에 관한 기본권과 자유의 보호로 이해할 것이다.

L. Brandeis는 19세기 말 프라이버시를 개인의 '혼자 있을 권리'로 최초로 정의하며, 민주주의에 반드시 필요한 자유로서 헌법에 반영돼야 한다고 주장했다. 프라이버시는 일반적으로 사생활의 내용을 공개 당하지 아니할 권리, 사생활의 자유로운 형성과 전개를 방해받지 아니할 권리, 그리고 자신에 관한 정보를 스스로 관리, 통제할 수 있는 권리 등을 내용으로 하는 복합적 성질의 권리이다.

이메일, CCTV, 휴대폰 및 휴대폰 카메라는 IT의 발전으로 프라이버시와 관련해 새롭게 등장한 것으로 전통적인 프라이버시 침해에 대체하고 있으며 프라이버시 정의 자체를 바꾸고 있다.



프라이버시 침해 유형

정보프라이버시

정보프라이버시(Informational privacy)는 종래의 공공부분과 민간부분에서 개인정보의 데이터 수집 및 취급과 관련해 법령을 근거로 해서 운용하는 개인정보를 말한다. 우선 공공기관이 수작업이나 컴퓨터에 의해서 수집과 관리 및 이용하는 개인정보가 주요 대상이다. 정보프라이버시는 개인 정보를 수집·개시·이용되는 관계를 통제하기 위한 개인의 요구라고 할 수 있다. 이 정보프라이버시는 개인정보 소유자의 자기정보에 대한

통제권(자기정보통제권)의 측면에서 개인정보를 강조하기 위해 사용된 용어이다.

이러한 정보프라이버시는 기존의 프라이버시와 두 가지가 다르다. 첫째, 정보프라이버시는 동시에 두 사람 이상의 사람들에게 공유되고 사용될 수 있다. 둘째, 정보프라이버시는 무제한적으로 다른 목적으로 사용이 가능하다. 이러한 정보프라이버시의 특징은 개인에 대한 전혀 새로운 정보의 창출가능성 및 컴퓨터 등에 개인정보의 잔존가능성 등 컴퓨터 및 인터넷의 특징과 결합해 오늘날 심각한 프라이버시의 침해문제를 제기하고 있다.

예컨대 현행 주민등록법에서 정하는 일반적인 행정정보에 관련되는 성명, 주민등록번호, 주소, 전화번호, 생년월일, 출생지, 본관, 취미와 특기, 국적, 가족관계, 교육과 직업훈련에 관한 정보로서 최종학력과 학적사항, 자격증, 상벌관계, 병역정보로서 계급, 병과와 병종, 특기부여, 군번 등이 있다. 특히 중요한 정보프라이버시는 금융기관의 신용정보로서 은행예금과 거래내역, 증권회사 고객의 증권계좌와 주식거래 내역 등 신용카드회사의 고객 신용정보와 결제내역 등이다. 또한 병원이나 의료기관 환자의 병력과 진료내역 등 개인정보와 의료기관이나 의료보험공단 등이 관리하는 병력과 진료기록 및 치료과정 자료 등이다. 또한 정부가 기록하고 보관하는 범죄인의 개인기록으로서 전과자료, 범죄특성의 기록, 그리고 혼인관계와 성적 취향에 관한 기록은 민감한 사안이다.

이러한 정보프라이버시는 관리주체에 의해서 침해되는 경우가 다수이다. 즉 외부자의 침입보다는 내부자의 불법적인 유출에 의해 침해되는 까닭에 조직내부의 개인정보에 접근을 엄격하게 법적으로 규율하는 것이 무엇보다도 중요한 관건이다.

이 중에 가장 많은 문제점을 노출하고 있는 주민등록번호를 둘러싼 문제를 살펴본다. 주민등록번호에는 한 개인의 생년월일 및 성명 등의 정보가 포함돼 있기 때문에 그 자체로서 프라이버시 침해 위험성을 상당히 내포하고 있다. 원래 행정목적의 주민등록번호는 공공부분에만 한정되지 아니하고 민간부분까지 전체 생활영역에서 특정한 개인정보가 광범위하게 활용되면서 주민등록번호의 오·악용 피해 실태는 중대한 경제·사회적 문제를 야기하고 있다.

현재 우리나라 인터넷사이트는 거의 예외 없이 회원 가입시 개인의 주민등록번호를 필수적으로 기입할 것을 요구하고 있다. 그 결과 자신의 실명을 숨기기 위해 주민등록번호 생성기를 이용해 임의로 생성한 주민등록번호로 인터넷사이트에 회원가입

을 하거나 타인의 주민등록번호를 도용해 인터넷사이트에 회원 가입하는 사례가 빈번히 발생하고 있다.

주민등록번호 도용으로 인해 피해자의 심리적·정신적 불안감을 심각하게 야기한다. 주민등록번호를 도용당한 경험이 있는 피해자들은 누가, 무슨 목적으로 도용했는지 알지 못한 채 또 다른 목적으로 자신의 주민등록번호를 악용할지 알 수 없는 불안감에 시달리게 된다고 하소연하고 있다. 그러므로 주민등록번호 도용이 얼마나 큰 프라이버시 침해가 되는지를 알 수 있다.

주민등록번호 도용의 문제점은 크게 사업자의 주민등록번호 수집관행과 주민등록번호 생성기 등으로 누구나 쉽게 생성할 수 있는 문제로 인해 도용에 대한 원천적인 차단이 어렵고 또한 법제도적인 대처의 한계로 인해 고충해결이 상당히 어렵다.

IT 시대의 사이버공간에서 프라이버시를 보호하려면 현행 주민등록번호제도에 대한 근본적인 재검토가 필요하다. 주민등록번호제도 자체가 프라이버시 침해 요소를 갖고 있을 뿐 아니라 주민등록번호가 흩어져 있는 개인정보를 통합·프로파일링하는 수단으로 작용할 수 있기 때문이다. 사이버공간에서 주민등록번호 도용행위를 방지하기 위해서는 첫째, 인터넷 사업자로 해금 주민등록번호를 수집하지 못하도록 제도화해야 한다. 민간 인터넷 사업자의 경우 주민등록번호를 필수항목으로 수집할 정당한 이유가 없으며, 대금의 결제를 위해 꼭 필요한 경우에도 신용카드 결제나 전자서명 등 공인인증서를 활용하도록 하고 주민등록번호는 요구하지 말아야 할 것이다.

둘째, 주민등록번호 도용에 대한 처벌을 강화해야 한다. 정신적·심리적 피해가 막대한 프라이버시 침해의 경우에는 금전적인 피해가 없는 경우에도 민·형사상 책임을 물을 수 있어야 한다. 또한 공정거래위원회에서 제시하고 있는 '인터넷사이버쇼핑물 표준약관'의 필수수집항목에서 주민등록번호를 시급히 삭제해야 할 것이다.

셋째, 주민등록번호 도용에 따른 피해를 근본적으로 방지하기 위해서는 무엇보다도 타인의 정보를 함부로 도용하거나 오·남용해서는 안 된다는 기본 의식과 나의 정보도 나의 정보와 동일하게 소중히 다뤄야 한다는 의식의 정착이 선행되어야 할 것이다. 그러기 위해서는 나의 정보도 언제든지 도용될 수 있고 자신도 어느 순간 피해자가 될 수 있다는 것을 각인하고 타인의 프라이버시 침해가 얼마나 심각한 범죄인지를 인식시키고 이의 방지를 위한 사이버 윤리교육이 절대적으로 필요하다.

통신프라이버시

통신프라이버시(Communication privacy)는 전화·휴대전화, 이메일 및 인터넷 등의 통신수단을 매개해 수집과 분석 및 가공되는 개인정보로서 새로운 기술을 이용하기 때문에 이것은 오늘날 IT의 발전에 따른 부작용으로서 빈번하게 발생하는 문제이다. 따라서 가해자는 개인정보의 침해의사를 가지고 이동하는 데이터에 접근해서 개인정보를 도청하거나 검열하는 까닭에 그 기술력에 의해서 침해범위가 결정되는 특성을 나타낸다.

치열한 논쟁의 대상은 이메일의 검열과 전화의 도청이다. 이것은 우선적으로 당해 개인의 동의가 필요하고 동의가 필요하지 않은 부분은 적법절차에 의한 절차적 정의의 문제가 중요한 이슈가 될 수 있다. 즉 전화통화, 하드디스크 또는 디스켓에 저장한 데이터에 대한 강제수사가 필요할지라도 법원의 영장발부가 필요하다.

최근 급증하고 있는 회사 내 이메일 검열에 대한 사례로 2002년에 발생한 스카이라이프 사건을 언급할 수 있다. 이 사건은 회사의 기밀을 보호할 목적으로 직원의 이메일을 검열한 경우에도 통신의 비밀 위반으로 유죄판결을 했다. 비록 하급심 판결이지만 IT 사회가 도래한 이후 사이버공간에서의 이메일이 문제된 최초의 사건이라는 입장에서 앞으로 이 분야에 대한 논의를 예측하는데 시금석이 될 수 있을 것이다.

최근 수사기관의 통신기록 조회가 남발되고 있다는 목소리가 높아지고 있다. 휴대전화, 인터넷 등 세계 최고 수준의 통신 인프라가 역으로 국민 감시의 수단으로 활용되고 있다는 지적이다. 디지털 통신의 발달로 유무선, 데이터 통신 등 모든 통신기록이 컴퓨터 데이터로 남기 때문에 개인이 국가로부터 자신을 보호하기 위해 할 수 있는 방법은 사실상 없다. 그러므로 프라이버시 침해를 막기 위한 통신기록 조회에 대한 견제 장치 마련이 시급하다.

수사기관이 아닌 단체나 기업에 의한 개인정보 유출도 위협 수위다. 이처럼 서비스나 판매업체의 고객정보 남용 사례는 갈수록 늘고 있지만 관련법에는 규제조항이 없어 대형 사고의 가능성도 높아지고 있다. 그러므로 민간기업이 인터넷 등 다양한 경로로 수집한 정보를 자의적으로 남용하는 것을 막기 위한 명확한 기준 마련이 시급하다.

신체프라이버시

신체프라이버시(Biometric privacy)는 IT 발전으로 가능해진

유전자 또는 DNA 테스트, Drug 테스트, 지문 인식, 홍채 인식 등을 통해 인체상의 중요한 정보를 수집하는 것이다. 제2차 세계대전을 겪으며 인류는 인간 그 자체는 지구상의 그 무엇과도 바꿀 수 없는 고귀한 존재라는 것을 깨달았지만 얼마 안 있어 도래한 IT 사회는 신체의 본질에 기초한 개인의 유전적인 특성과 비밀을 종래의 공권력만이 아니라 민간부분에 의해서도 더욱 더 요청받고 있다. 또한 과거에는 불가능하거나 현실적으로 어려웠던 것이었지만 이제는 IT의 발전으로 저렴한 비용으로 용이하게 신체상의 정보를 수집할 수 있게 됐다. 이제 인체로 대표되는 인간의 프라이버시가 여러 가지 이유로 침해되기에 이르렀다. 그럼으로써 IT 사회의 도래는 결국 인간의 신체를 존엄한 대상으로서 IT의 실험 대상으로 전락시켜 버리고 있다.

인간의 존엄과 가치의 대상으로서 인간의 신체는 DNA 테스트나 유전자 데이터베이스가 일반화되면서 기업이 적임자를 선발하기 위해서 널리 사용하는 공통수단이 되고 있다. 유전자 테스트가 비록 직업병의 예방을 위해서 합법적일지라도, 기업이 현재 또는 장래의 종업원을 차별하기 위해서 이러한 유전자 테스트를 이용하는 것은 심각한 위험을 야기할 수 있다. 법적 개입이 없이 기업이 종업원의 질병이나 직무태만 등의 경향이 있는지 여부를 식별하는 정보가 종업원을 차별하는데 이용될 수 있기 때문이다. 유전자 테스트는 개인의 인격을 구성하는 핵심요소에 관련되는 프라이버시의 외적 침해이다.

공간감시프라이버시

공간감시프라이버시(Territorial or Spatial privacy)는 일정한 공간에 외부 침입을 방지하거나 감시하기 위해 IT에 의해 가능해진 자기 장치나 CCTV 등을 통해 개인의 프라이버시를 침해하는 것을 말한다.

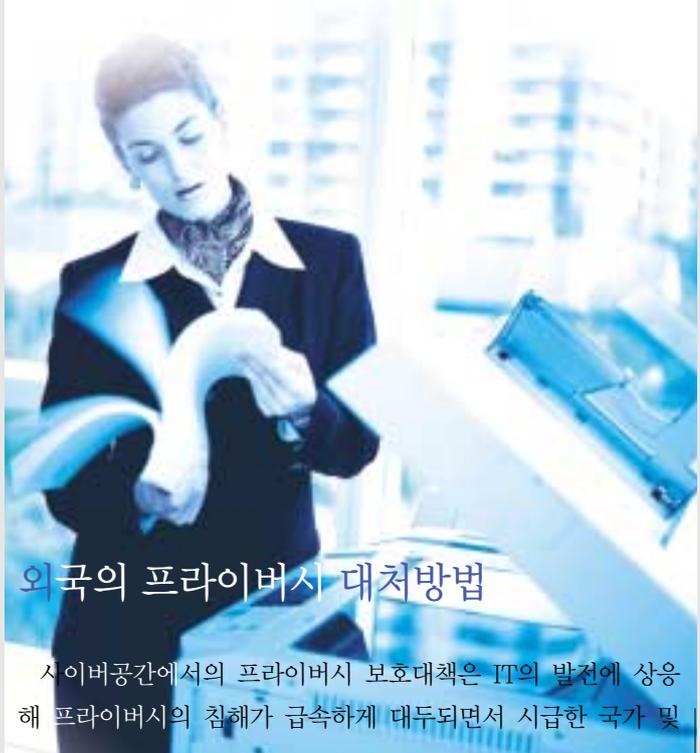
최근 각종 납치사건이 잇따르고 있는 서울 강남구 일대에 강남경찰서와 강남구가 CCTV를 설치하기로 한 것을 놓고 인권침해 논란이 일고 있다. 특히 범죄예방을 위해서 ‘CCTV 촬영지역’이라는 표지판을 달지 않을 방침이어서 ‘몰래카메라’ 논란도 일고 있다. CCTV는 각종 최신 범죄예방 및 통제기법의 공통된 수단이며 가장 효과적인 도구 중 하나로 각광받고 있다. 하지만 본인의 동의 없이 무차별적으로 사람의 모습을 촬영, 저장한다는 측면에서 프라이버시 침해라는 비판의 대상이 되고 있다.

강력범죄 예방을 위해 CCTV로 24시간 거리를 촬영하는 ‘감시시스템’ 도입은 개인의 동의를 받지 않은 무차별한 개인정보

의 수집이며, 해당개인의 승낙이나 동의 없이 수집·저장하는 것은 그 자체로 프라이버시의 침해에 해당한다. 개인정보의 비밀 수집은 자신의 개인정보 처리를 자신만이 결정할 수 있는 자기결정권을 침해하는 것이며 따라서 개인정보는 해당 개인에 대한 사전고지 및 그로부터의 동의 및 승낙을 전제로 해 수집되어야 한다. 공공장소에서의 초상권도 사적 공간에서의 권리만큼 강하게 지켜지지는 못하는 측면이 있지만 보호돼야 할 권리임은 분명하다. CCTV 촬영을 하면서 이러한 사실을 도로의 입구에 사전에 고지하더라도 사전에 통행자의 동의 및 승낙을 모두 받기는 불가능하기 때문에 초상권 내지 프라이버시권의 침해에 해당한다.

CCTV의 설치가 주민의 동의 하에 그리고 명시적으로 설치되는 경우에도 관리운영방식 등의 문제로 CCTV의 효과에 대해 우려의 목소리가 높은 만큼, 범죄취약지 등 특정지역 CCTV 설치 의무화 등 CCTV 설치 확대를 통한 범죄감소 목적을 달성하기 위해서도 CCTV의 성능 및 제원, 설치 및 운영 주체와 자격 및 방법, 기록물의 보관과 활용 및 이에 대한 감독 등에 대해 국제적 수준에 부합하는 엄격한 가이드라인이 설정돼야 한다.

국민들에게 CCTV가 제한된 원래 목적의 한계 내에서 책임 있는 당국의 엄격한 관리 하에, 부실이나 악용의 우려 없이 운영된다는 확신을 심어줘야 할 것이다.



외국의 프라이버시 대처방법

사이버공간에서의 프라이버시 보호대책은 IT의 발전에 상응해 프라이버시의 침해가 급속하게 대두되면서 시급한 국가 및

국가 간의 중요한 과제가 됐다. IT의 확산 및 이전에 따른 정보 공유 체제가 등장하면서 데이터 이동에 따른 지리적 장애를 제거한 세계화와 국가 간의 기술적인 장애를 제거하면서 체제 수렴의 현상 그리고 다양한 데이터를 수집한 것을 다른 형태로 전환해 이용할 수 있는 멀티미디어의 통합은 프라이버시의 침해를 촉진한다.

세계적으로 볼 때 민간부분은 공공부분에 비해 다소 늦게 입법화되고 있는 실정이다. 민간부분의 프라이버시 보호법제는 공공부분과 별도로 제정됐다가 점차 양자가 통합되고 있다. 최근 각 국의 프라이버시 보호법제의 특색은 공공부분과 민간부분의 개인정보보호를 위한 법집행기관이 통일되거나 또는 프라이버시 침해에 따른 권리구제의 방식도 전통적인 법원재판에 보충해 당사자주의에 의한 분쟁조정과 화해방식을 널리 채택하는 추세로 나타나고 있다. UN은 세계인권선언(1948)에서 프라이버시의 보호를 선언하고 있다. 또한 UN은 1990년 컴퓨터 처리의 개인화일 규율의 가이드라인을 제시했다. 개인의 프라이버시 보호에 관한 국제적인 입법 동향은 개별국가의 관련 입법에 직·간접적으로 영향을 미치고 있다.

미국의 보호방법

미국은 Brandeis와 Warren이 1890년 'The Right to Privacy'에서 프라이버시 보호에 대해 선구적으로 주장한 이후 Olmstead 판결을 통해 연방대법원에서 프라이버시 보호를 다루기 시작했다. 미국은 전통적으로 '프라이버시'라는 용어를 사용하고 왔다. 그리고 헌법상 이념적으로 연방정부 및 주정부는 시민의 적이라는 관념이 지배적이었기 때문에 유럽에 비해 프라이버시가 침해될 소지가 적었다. 그러나 IT 사회의 도래로 인해 사이버공간상의 프라이버시 보호가 사회적 이슈로 부각되고 컴퓨터에 의한 정보처리와 개인정보의 보관이 가능하게 되면서 프라이버시를 보호하는 일반법을 제정하지 않고 그 대신 문제가 되는 분야별로 수시로 법을 제정·시행하고 있다.

미국의 개별적 입법의 주요 예를 들면 Cable Communications Policy Act(1984), Electronic Communications Privacy Act(1986), Video Privacy Protection Act(1988), Employee Polygraph Protection Act(1988), Telephone Consumer Protection Act(1991), Driver's Privacy Protection Act(1994), Telecommunications Act(1996), Children's On-Line Privacy Protection Act(1999) 등이 있다.

OECD 및 EU의 보호방법

EU는 사이버공간에서의 프라이버시를 보호하기 위해 공공부분의 개인정보, 민간부분의 개인정보, 온라인 및 오프라인 정보를 통합해 규율하는 방식을 취하고 있다. 이러한 EU 모델의 논거는 과거의 프라이버시의 침해에 대한 철저한 권리구제, 전자상거래를 촉진하기 위해서, 또 EU 법체계의 통일을 기하고자 단일한 개인정보감독기구의 설치를 전제로 하고 있다. 권리구제 방식도 법원에 의한 구제가 아니라 옴부즈맨과 같은 독립기구에 의해서 신속하고 사법비용이 적게 들기 때문에 매우 유리한 구제방안이라고 할 수 있다.

OECD는 1980년 정보화 사회의 도래와 국가 및 민간부분이 타인의 개인정보 취득이 전과 비교할 수 없을 정도로 용이해지는 상황에 심각한 우려를 표명하고 프라이버시 가이드라인 8원칙을 공표했다. 이것은 여타 국가의 국내 개인정보 보호입법에 지침으로 작용했다. OECD 프라이버시 가이드라인은 프라이버시 보호에 시금석이 되는 중요한 국제사회의 첫걸음이자 기준이 되고 있다. ①데이터 수집제한의 원칙, ②데이터 특성의 원칙, ③목적 특정화 원칙, ④사용제한의 원칙, ⑤비밀보호의 원칙, ⑥공개의 원칙, ⑦개인 참여의 원칙, ⑧책임성 원칙을 들고 있다.

또한 유럽이사회는 1981년 프라이버시 협약(Council of Europe Convention on Privacy)을 제정해 프라이버시에 관한 일반적인 원칙을 표명했다. EU 회원국의 프라이버시 보호법제는 이상과 같은 기본원칙을 국내법의 차원에서 입법해 시행하고 있다. 이와 같이 EU는 프라이버시 협약(1981), EU데이터보호 지침(1995), 유럽연합 전화통신부문의 프라이버시 보호지침(1997), 인터넷의 익명성(1997) 등을 제정해 사이버공간상의 프라이버시를 보호하고 있다.

우리나라의 프라이버시 보호방법

우리나라에서도 '정보통신망이용촉진및정보보호에관한법률'과 '공공기관의개인정보보호에관한법률' 등 IT를 기초로 한 프라이버시의 보호 및 개인의 자기정보통제권 보장을 위한 각종 법제도적 수단들이 마련돼 있고 그 보호를 위한 행정체제도 구축돼 있기는 하지만, 국민 개개인에게 프라이버시의 안전을 보장해 줌으로써 사이버공간 자체의 생명력과 성공적 발전을 뒷받침해 주는 신뢰인프라의 구성요소가 되기까지는 아직도 미흡하다.

공공기관의 개인정보보호에 관한 법률

‘공공기관의개인정보보호에관한법률’은 개인정보 보호에 관한 일반법적인 성격을 갖는다. 이 법은 공공기관의 컴퓨터에 의해 처리되는 개인정보의 보호를 위해 그 취급에 관해 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다. 여기에서 말하는 국민의 권리와 이익은 일반적으로 프라이버시를 뜻한다. 공공기관이 보유하고 있는 정보는 국민의 알권리에 의해서 공개를 청구할 수 있지만, 그 정보가 개인의 사생활에 관한 정보인 경우에 사생활의 비밀과 자유를 근거로 공개가 면제될 수 있다.

IT의 발전으로 컴퓨터가 없는 국가는 상상할 수 없게 됐다. 프라이버시가 특히 문제된 것은 이 모든 컴퓨터가 네트워크화 돼 있기 때문에 개인정보의 유출과 부작용의 위험이 매우 컸다. 따라서 보호되는 개인정보는 컴퓨터에 의해 처리한 개인정보에 한정하고 있다. 상대적으로 수기에 의한 개인정보는 유출과 그 부작용이 작으므로 프라이버시가 침해될 가능성이 적다고 봤다.

개인정보라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함돼 있는 성명·주민등록번호 등의 사항에 의해 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합해 식별할 수 있는 것을 포함한다)를 말한다. 법인과 사자(死者)의 개인정보는 제외된다.

공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집해서는 안 된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시돼 있는 경우에는 그러하지 아니하다. 또한 개인정보의 보유기관의 장은 처리정보를 정보주체이외의 자에게 제공하는 때에는 그 수령자에 대해 사용목적·사용방법 기타 필요한 사항에 대해 제한하거나 처리정보의 안전성확보를 위해 필요한 조치를 강구하도록 요청해야 한다. 그리고 다른 법률에 의해 보유기관의 내부에서 이용하거나 보유기관 외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화의 보유목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공해서는 안 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

우리나라는 아직 민간부분에 대한 일반법은 없으나 2001년 ‘정보통신망이용촉진및정보보호등에관한법률’을 제정해 시행하고 있다. 정보통신망법의 의의는 첫째, 정보통신망의 이용을 촉

진해 정보통신서비스이용자의 개인정보의 보호를 강화하고 유해정보로부터 청소년보호를 강화하는 것이다. 둘째, 정보통신서비스제공자가 개인정보의 수집·처리·관리 등을 타인에게 위탁하는 경우에 그 타인의 개인정보보호 위반행위에 대해 책임을 부과하고 있다. 이와 같이 IT 환경의 급속한 발전에 의해서 이전보다 디지털 정보형태가 온라인 서비스의 중요한 거래객체로서의 의의를 강조하는 국제적인 추세를 반영한 것으로 평가된다.

개인정보는 생존하는 자연인에 관한 성명이나 주민등록번호 등과 같이 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(다른 정보와 결합해 식별 가능한 경우도 포함)를 말한다. 컴퓨터나 전자기기에 의한 개인정보만을 한정해 적용되기 때문에 오프라인의 수기에 의한 개인정보는 보호객체에서 제외된다. 특히 이 법은 민간부분의 개인정보에 관해서 정보통신망에 의해서 개인정보를 수집하고, 이용 및 처리하는 경우에만 적용된다.

정보통신서비스제공자가 이용자의 개인정보를 수집하는 경우 그의 동의를 필요로 한다. 동의를 얻기 위해서는 개인정보관리책임자의 신원 등과 수집목적 및 이용목적, 제3자에게 제공할 경우에 그 제공목적과 그 정보의 내용 및 수령자 그리고 그의 권리와 행사방법을 고지하거나 이용약관에 명시해야 한다. 또 정보통신서비스제공자는 그 이용자의 동의에 의해서도 고지범위를 초과해서 제3자에게 제공할 수 없고 또한 그 개인정보를 제공받은 자도 제공목적 이외로 이용하거나 제3자에게 제공하지 못한다.

정보통신서비스제공자등은 타인에게 이용자의 개인정보의 수집·취급·관리 등을 위탁할 경우에 그 사실을 사전에 이용자에게 고지해야 한다. 이는 개인정보의 처리자를 서비스제공자의 이행보조자로 명시함으로써 개인정보의 침해에 따른 분쟁에서 이용자의 입증책임을 완화하고자 함이다. 따라서 처리자의 손해배상책임에 있어서 서비스제공자와의 내부관계를 고려해 부진정연대책임 또 사용자의 책임을 물을 수 있기 때문에 정보주체의 손해배상을 용이하게 해결할 수 있다. 정보통신망의 이용자가 금지행위를 위반한 경우 형벌을 부과할 수 있다. 누구든지 정보통신망에 의해 처리, 보관 또는 전송되는 타인의 정보를 훼손하거나 비밀을 침해, 도용 또는 누설해서는 안된다.



프라이버시 보호를 위한 방안

정부규제의 강화

IT의 급속한 발전으로 사이버공간이 탄생했다. 사이버공간은 우리에게 이전에 상상할 수 없었던 장미빛 공간을 제공하기도 하지만 프라이버시가 여지없이 침해되는 암흑의 공간으로 전락하기도 한다. 이제 우리가 직면한 긴급한 과제는 이러한 프라이버시 보호를 위해서 시장규제와 정부규제 중에서 어떤 방안을 선택하는 것이 우리사회의 실정에서 정당하고 효율적인가의 문제이다.

개인정보의 이용에 관련된 경제적 논의와 기술이 근본적으로 변하면서 개인정보의 이용을 규율하는 제도 또는 메커니즘도 변하지 않을 수 없게 됐다. 오늘날 개인정보의 보호는 대다수 산업 전반에 걸쳐서 제기되고 있다. 시장모델은 소비자의 기호에 따른 제한으로서 대다수 소비자가 기업의 프라이버시 정책에 기초해 그들의 소비의사를 기꺼이 변경하면, 그만큼 기업은 시장변화에 따르게 되고, 기업의 프라이버시 관행에 대한 공표에 따른 제한을 전제로 하고 있다. 기업이 소비자의 기호를 충족시키고자 충실하게 고지하면 소비자의 선택을 촉진한다. 이러한 시장모델은 중요한 요소로서 소비자의 기호와 기업의 행위가 프라이버시에 대한 관심과 이해를 제고시킨다는 점이다. 미국이나 EU와 같이 상대적으로 시장이 합리적으로 기능하는 곳에서 시장규제는 효율적이고 그 정당성을 찾을 수 있을 것이다. 그렇다면 시장이 제대로 기능하지 않는 곳에서는 어떻게 해야 할 것인가?

한편 정부규제방식은 시장규제가 개인 프라이버시 보호에 매우 취약하다는 가정에 기초해 개인의 프라이버시의 보호는 정부에 의한 보다 강력한 정책과 법 집행에 의해서 실현되는 것이다.

즉 프라이버시 규범이 법령, 규제기관, 법원의 판결에 의해서 정해지는 것이다. 특히 현대사회의 특징 중의 하나인 시장의 실패와 기업과 소비자 사이의 권력의 비대칭 관계를 고려할 때 시장에서 기업 또는 개인이 자율적으로 타인의 프라이버시 보호를 실현하기는 기대하기 어려우며 또한 상당히 어렵다. 민간부분 또는 개인에 의한 개인정보의 수집은 기업과 소비자사이의 계약관계에서 시장의 실패를 여실히 보여준다. 프라이버시에 대한 시장실패의 원인은 정보 및 협상 비용에서 기인한다. 정보비용은 기업과 소비자사이의 정보가 비대칭이기 때문에 발생한다.

정부규제의 성과는 법규범이 시장, 기술 및 프라이버시 보호의 변화에 대처할 수 있는 역량에 달려있다. 미국이나 EU와 같이 상대적으로 시장이 합리적으로 기능하는 곳과는 달리 시장의 실패할 가능성이 보다 큰 곳에서, 그리고 기업과 소비자 사이의 권력이 불균형일수록 시장에서 기업 또는 개인이 자율적으로 타인의 프라이버시 보호를 실현하기는 기대하기 어려우며 또한 상당히 어렵다. 이 때문에 프라이버시의 침해 위험이 높아지면서 강행규범이 이전보다 훨씬 많이 필요하다는 결론에 이르고 있다. 즉 시장규제가 개인의 프라이버시 보호에 매우 취약하기 때문에 프라이버시의 보호는 정부에 의한 보다 강력한 정책과 법 집행에 의해서 실현되어야 한다.

하지만 정부규제만이 민간의 개인정보를 효율적으로 보호하는 수단이 아니다. 온라인 환경에서 개인정보는 정보주체, 정보제공자, 정보처리자 등에 의한 개인정보의 오·남용의 억제는 온라인에서 정보유통에 따른 침해를 용이하게 포착할 수 없다. 때문에 개인정보보호를 위한 정부규제의 보충방안으로서 자율규제도 적극 권장하는 정책이 중요하다. 사업자가 자율적으로 적절한 수준의 개인정보지침을 실천함으로써 시장신뢰를 구축할 수 있다. 따라서 정부와 민간 모두가 프라이버시보호의 자율규제를 병행하는 동시에 프라이버시의 보호기술개발도 활성화해야 한다.

전자정부 - 분산에 의한 안전 확보

정보인권, 특히 정보프라이버시의 관점에서 보았을 때, 전자정부의 진전은 위협의 증대인이 아니면 21세기 고도정보사회와 전자정부에 있어 인간의 존엄과 가치를 재발견할 수 있는 각성의 계기가 될 것인가. 전자정부를 구현함에 있어 우리가 직면하는 가장 기본적인 딜레마는 정보의 집적·중앙처리를 통한 효율의 극대화 요구와 정보수집·관리의 분산을 통한 프라이버시의

안전 보장에 대한 요구의 상극관계에서 비롯된다.

전자정부에서 프라이버시의 보호문제는 종종 시스템개발자들의 기술중심적 또는 기술결정론적 사고에 의해 소홀히 다뤄지거나 아예 무시되는 경우가 적지 않다. 시스템에 입력돼 관리되는 개인정보에 대한 접근 또는 이용 제한이나 장애가 없어야 그 분석, 결합 등 다양한 정보처리방식에 의한 정보처리의 효율성이 극대화될 수 있으므로 개인정보가 무차별적으로 공유되도록 하는 것이 바람직하다고 판단할 수도 있다. 정보주체의 동의를 묵시적으로 의제하거나 그 예상되는 처리양상을 알리지 않은 상태에서 제한적으로 요구함으로써 필요한 정보를 취득한 상태에서의 동의가 아니라 무지상태의 동의를 유도해 낼 수도 있으며, 아예 정보주체의 동의 여지를 배제하고 정보처리단계를 연계해 나갈 수도 있다. 그러나 이러한 극단적인 형태의 현실성과는 달리, 정보프라이버시와 같은 정보인권적 측면에 대한 감수성, 즉 정보감수성은 정보처리의 효율성 극대화를 추구하는 시스템개발자들에게 결여되거나 미흡한 경우가 빈번히 나타난다.

인간의 존엄과 가치가 존중되는 자유민주주의적 헌법질서 또는 자유사회의 헌법모델을 전제로 할 때, 국가가 개인의 동의여부를 불문하고 수집 또는 접근할 수 없는 프라이버시의 최소한의 영역은 존재해야 한다. 아무리 대다수의 사회구성원이 합의를 하거나 다수결 등 민주적 의사결정방법을 통해 그 같은 합의가 이뤄진다고 해도 합부로 접근하거나 침해할 수 없는 최소한의 프라이버시를 인정해야 마땅하다.

전자정부는 더이상 과거와 같은 대면적 방식이 아니고 익면적 방식이다. 그러므로 그 무엇보다도 사이버공간 시스템에 대한 신뢰와 프라이버시가 중요하다. 그러므로 정보처리의 효율성을 어느 정도 놓치더라도 정보의 분산을 통해 국민의 신뢰를 얻고 안전을 확보하는 것이 IT의 발전으로 우리에게 다가 온 전자정부의 사명이다. 사이버공간에 걸맞는 진정한 전자정부는 국민의 신뢰와 안전을 최고의 목표로 해야 할 것이며 이를 위해서는 정보처리의 분산을 통한 프라이버시의 보호와 안전 확보가 필수적이다.

프라이버시 영향평가제도의 도입

IT 환경에 걸 맞는 프라이버시 영향평가제도(Privacy Impact Assessment)의 도입이 필요하다. 최근 NEIS 구축 및 인터넷 게시판 실명제의 추진 과정에서 나타난 바 있듯이, 정부가 정보화 정책이나 사업을 추진함에 있어 사전 계획수립 단계에서부터

프라이버시 또는 개인정보에 대한 영향평가를 실시하도록 해 그 결과를 정책이나 제도에 미리 반영하도록 하는 제도가 필요하다는 주장이 폭넓은 공감을 얻고 있다.

이를 제도화함으로써 예기치 못한 사회적 갈등과 행정비용의 낭비를 미연에 방지하자는 것이다. NEIS의 구축에 수백억원의 예산이 투입됐지만 결국 제대로 사용할 수 없어 엄청난 예산낭비를 초래하고 국민의 부담만 가중시킨 예는 프라이버시 영향평가제도가 필요함을 극단적으로 잘 보여주고 있다. 그렇다면 이러한 제도가 필요하다면 어떠한 방향으로 도입해야 하는가.

특히 전자정부사업 추진시 기획 및 설계단계에서 개인정보침해영향 사전평가제를 반드시 실시해야 할 것이다. 그럼으로써 개인정보 침해를 방지할 수 있는 조치나 수단의 강구, 그 침해영향을 일정 기준이하로 감축할 수 있도록 하는 등의 내용을 사업 또는 정책 내용에 반영하도록 할 수 있다.

유비쿼터스 프라이버시

‘모든 물건에 컴퓨터’를 내용으로 하는 유비쿼터스 컴퓨팅 사회는 도시공간을 구성하는 수많은 환경과 대상물 속에 보이지 않는 컴퓨터를 심을 뿐만 아니라 인간의 인체에도 칩을 이식하거나 입는 컴퓨터를 통해 인간을 포함한 모든 사물과 대상이 지능화되고 전자공간에 연결돼 서로 정보를 주고받는 현실공간과 사이버공간이 공존하는 사회가 될 것이다.

이러한 사회는 개인과 물건이 언제 어디서나 제한 없는 접속을 하게 되므로 개인의 다양한 수요를 충족시킬 뿐만 아니라 갑작스러운 병이나 위기로부터 개인구제를 가능하게 하는 등 우리 삶의 질을 획기적으로 발전시킬 수 있는 반면, 본인의 동의 없는 ‘개인정보의 과도한 집적’의 문제를 안게 된다. 이러한 현실을 두고 뉴욕시의 사법부장관은 “현재 내가 두려워하는 것은 빅 브라더(Big Brother)가 아니라 빅 브라우저(Big Browser)”라고 해 정보통신서비스업자를 경계했다.

유비쿼터스 사회는 사람을 비롯한 모든 물건에 숨겨진 컴퓨팅에 의해 일정한 명령행위 없이 언제 어디서나 개인의 행적을 집약적·전자적 기록으로 남기는 것이다. 전자적인 측면에서 한편으로는 자신의 다양한 수요를 충족시키기 위해 일정한 목적 범위 내에서 자신을 공개하면서도 다른 한편으로는 자신의 행적을 타인의 권한 없는 적극적·소극적인 관여로부터 보호해야 하는 사회임을 감안할 때 프라이버시권의 보호가 가장 중요한 역할을 하게 될 것임을 명심해야 할 것이다. 