2009-20 | 책임연구보고서

개인정보 침해 분석과 이에 대한 입법적 대응에 관한 연구

치안정책연구소
POLICE SCIENCE INSTITUTE

2009-20 | 책임연구보고서

개인정보 침해 분석과 이에 대한 입법적 대응에 관한 연구

치안정책연구소 생활안전대책연구실

선임연구관 김 학 신

<목 차>

【표 차례】

【그림 차례】

제1장 서 론

제1절 연구목적

정보통신기술의 비약적인 발전에 따른 유비쿼터스(Ubiquitous) 기술 시대가 도래하면서 때와 장소에 구애받지 않고 네트워크에 접촉할 수 있는 세상으로 우리 사회가 급속도로 변해가고 있다. 더불어 디지털 기술에 의해 수집된 정보의 유통은 빠른 속도로 확대되고 있어 개인정보의 유출 가능성도 빠르게 증대하고 있다.

이러한 정보통신 기술의 변화에 따라 최근 들어 대규모의 개인정보유출 및 오·남용 등 개인정보침해 사건이 사회의 큰 이슈로 자주 등장하게 되었고, 국민 대다수의 사회적인 관심은 과거의 어느 때보다도 개인정보의 보호에 대한 필요성을 절실히 인식하게 되었다.

최근의 한 사례로 전자상거래에 사용되는 신용카드에 개인의 신상정보와 금융거래정보를 담은 스마트 칩을 많이 부착하고 있는데, 이 경우 계약의 체결이나 대금 결제시 고객은 자신의 성명, 주민등록번호, 전화번호, 주소, 신용카드번호 등의 개인정보를 디지털 신호로 거래 상대방에게 전달된다. 그 결과 전자상거래업자들은 수많은 고객의 개인정보를 쉽게 수집·축적하여 자신의 영업활동에 활용하거나, 다른 사업자에게 대가를 받고 고객의 정보를 팔기도 한다.

또한 인터넷을 이용한 전자상거래는 누구나 쉽게 접근할 수 있기 때문에 개인정보가 전송·보관되는 동안 제3자에 의해 탈취·유출, 악용 될 경우 개인의 권익이 침해될 가능성이 크다. 특히 디지털로 바뀐 개인정보는 유출되더라도 흔적이 남지 않아 정보유출의 색출이 어려울 뿐만 아

니라, 불법적으로 유용 또는 악용된 후에는 정정 및 피해구제가 곤란하다는 점에서 매우 심각한 문제가 아닐 수 없다.[1)]

결국 이러한 개인정보의 유출, 탈취 및 오·남용은 소비자의 전자상거래 이용을 기피하는 주요한 원인이 되고 있어 전자상거래 성장의 걸림돌로 작용하고 있다. 따라서 인터넷상 개인정보보호는 인터넷을 이용하는 이용자들의 개인정보가 유출되는 것을 막음으로써 이들이 안심하고 인터넷 및 전자상거래를 이용할 수 있게 함으로써 그 이용촉진에도 기여하게 될 것이다.

한편, 개인의 입장에서는 이러한 기업의 개인정보의 유용은 중요한 프라이버시 침해이나, 기업의 입장에서 개인정보는 비즈니스를 수행하는데 중요한 자원이다. 전자상거래를 통해 정보를 전달하고 이를 사업화하려고 하는 민간영역의 활동을 제약하지 않아야 전자상거래가 활성화될 수 있다는 점도 간과해서는 안 될 것이다.

이러한 개인정보 및 신용정보에 대한 유출 우려로 소비자들이 인터넷 쇼핑을 회피하려 한다. 실제로 1차적 거래에서 제공된 소비자의 개인정보가 당사자의 동의 없이 다른 사업자에 이전됨으로써 거래 이후에 소비자에게 원치 않은 광고 또는 스팸메일 전송에 이용되는 경우가 많은 것으로 나타났다. 그러므로 전자상거래를 활성화하기 위해서는 고객의 신상 및 신용 등에 관한 정보가 유출되거나 악용됨으로써 개인의 권익이 침해되지 않도록 개인정보의 수집·처리·이용 및 제공 등이 적절히 통제될 수 있는 입법적인 보호장치가 강구되어야 한다.

이러한 추세에 부응하여 정부는 2008년에 들어와 적극적으로 개인정보보호 강화라는 국민의 시대적인 요구를 반영하고자 개인정보보호에 관한 법률을 제정하기에 이르렀다. 이 법률 안은 공공기관 및 민간기관 등을

1) 金正熙, 「인터넷상 個人信用情報保護에 관한 法的 考察」, 慶熙大學校 碩士學位論文, 2003. 3. 1면 참조.

포괄적으로 규율하는 개인정보보호의 원칙과 이에 대한 처리기준을 정립함으로써, 개인정보의 활용을 보장하고 부당한 침해로부터 정보주체의 권익을 보호하는 것을 목적으로 하고 있다. 이를 위해 개인정보의 수집·이용·제공 등의 처리기준 정립, 정보주체의 열람·정정·삭제 요구권 보장 등을 규정하여 국내 개인정보보호 법제의 획기적인 전환점이 되고자 하였다.

따라서 본 연구의 주된 목적은 개인정보 침해 관련 사례를 분석·조사하여 정보사회에서의 개인정보가 사적인 거래의 대상이 되는 것을 막고자 하는 것이 주목적이며, 현행 법제도하에서 일어나고 있는 개인정보 침해의 경우들을 유형화하면서 이를 통하여 개인정보침해 관련 사례들을 추적하고 그 흐름을 파악하여 일선 수사기관에서 개인정보침해에 대한 구체적인 대처방안을 마련함과 동시에 현행 법률의 미비점을 보완하여 그에 대한 입법적인 대안을 제시하고자 한다.

제2절 연구범위와 방법

2009년 11월 8일 미국 상원 법사위는 '데이터침해 통지법'(Data Breach Notification ACT)과 '개인정보보호와 보안법'(PERSONAL Data Privacy and SECURITY Act)을 속속 통과시켰다고 한다.

현재 우리나라는 세계 최고수준의 첨단 IT 인프라[2]와 국제사회가 인증한 최고의 디지털 정보 시스템까지 정보화의 비약적인 발전과 국가사회 전반의 유비쿼터스의 발전으로 IT기술은 국민생활에 매우 커다란 영

2) 국제적인 설문조사업체인 스트래티지 애널리틱스(Strategy Analytics)의 발표 내용에 따르면, 세계 58개국을 대상으로 인터넷 보급률을 조사한 결과 한국이 1위를 차지하였다. 코리아 포스트, 2009. 6. 23일자.

향을 미치고 있다.

하지만 첨단 인프라 환경 구축을 통한 세계 최고의 정보화 수준에 비하여 정보보호 수준은 상대적으로 미흡하여 해킹과 개인정보 유출, 인터넷을 이용한 유해정보 유포 등 정보화에 따른 역기능을 시급히 보완해야 할 과제로 떠오르고 있다. 그에 대한 대표적이 예가 개인정보유출과 그에 따른 피해이다. 지난 2008년 한해 동안 대규모의 개인정보 유출 사례가 다수 발생하였고,[3] 지금 현재에도 지속적으로 발생하고 있지만, 개인정보보호법은 아직도 국회에 계류 중에 있는 것이 현실이다.

정보가 사회적 · 경제적으로 핵심적인 역할을 하는 지식정보화 사회에서 정보보호에 대한 믿음과 신뢰를 잃는다면 이는 국가 전체에 엄청난 혼란으로 이어질 수 있다. 그래서 국민 개개인이 취급하는 개인정보도 수집 · 보유 · 이용 및 제공 · 파기에 이르기까지 각 단계별로 관리적 · 기술적 · 물리적 요소 등 3차원의 적절한 보호조치가 반드시 지켜져야 할 것이다. 왜냐하면 개인정보가 오 · 남용되어 잘못 사용되면 개인정보를 침해당한 개인에게 치명적인 피해를 입힐 수 있기 때문이다.

따라서 본 연구에서는 최근의 개인정보의 국내·외 현황과 침해 사례를 구체적으로 분석하고, 이에 대한 대응 방안과 더불어 입법적인 대책도 고찰하고자 한다.

이에 대한 구체적인 연구 범위는 다음과 같다.

제1장은 서론으로 이 논문을 쓰게 된 목적을 제시하고, 문제를 제기함으로써 연구방향 및 연구 범위와 방법을 제시하고자 한다.

제2장에서는 개인정보에 관한 일반론으로서 개인정보의 개념을 정의하

3) ① 2008년 2월 해킹에 의한「옥션」고객 1,081만명의 개인정보가 유출된 사고가 있었으며, ② 2008년 9월에는 내부자에 의한 유출로 「GS칼텍스」고객 1,100만명의 개인정보유출이 있었다. ③ 2008년 7월에는 관리소홀로 인한 「다음」고객 53만명 이메일 정보 유출되었으며, ④ 2008년 4월에는 개인정보 오·남용으로 인한 「하나로 텔레콤」고객 600만명의 개인정보 무단 제공 등이 있었다.

고, 이에 대한 분류, 그리고 프라이버시와의 관계를 설명하고자 한다. 또한 개인정보보호에 관한 국내·외 동향으로서 국내의 법제 동향과 더불어 국제기구의 규범과 기타 선진국에서는 개인정보를 어떻게 보호하는지 살펴보고자 한다.

제3장에서는 최근에 발생한 개인정보의 침해 현황과 유형을 분석해 보고, 개인정보 침해사례를 내부자에 의한 개인유출, 개인정보 관리 소홀로 인한 유출, 기술적 보호 조치 문제로 인한 개인정보 유출, 해킹 및 오남용에 의한 개인정보 유출로 나누어 침해 사례를 분석하고자 한다.

제4장에서는 개인정보의 침해 방지와 이에 대한 입법적인 대응으로서 개인정보 침해 대응 방향을 살펴보고, 개인정보 침해 방지 대책을 제시하고자 한다. 2008년부터 개인정보보호법 제정이 제기가 되었지만, 현재까지 국회에 계류 중에 있는 입법안을 구체적으로 검토하고자 한다.

이상과 같이 이 논문의 연구 목적을 달성하기 위하여 다음과 같은 방법으로 연구하고자 한다.

우선 개인정보 유출은 시간이 지날수록 대규모로 발생하는 경향이 있다. 특히, 2008년도에는 대규모 개인정보 유출 사건이 많은 한 해 였다. 따라서 2008년도에 발생한 사례를 중심으로 하여 수사기관의 자료와 언론기관의 자료를 통해 개인정보 침해를 분석하고 이에 대한 문제점을 고찰할 것이다.

두 번째로 개인정보보호 침해 분석을 위하여 선행연구 논문 및 각종 참고자료, 인터넷 웹사이트, 그리고 언론 기사, 각국의 관련 법제 및 동향 등을 정리, 고찰하며, 관련된 문헌분석을 통해 연구하고자 한다.

세 번째로는 최근 국회에 개인정보보호와 관련한 입법안이 다양하게 제기되었다. 각각 제안된 입법안을 심도있게 분석하여 우리 정치 · 경제 · 사회 · 문화 등 현실의 여건에 맞는 입법안을 제시하고자 한다.

제2장 개인정보에 관한 일반론

제1절 개인정보의 개념

개인정보는 생존하는 자연적 사실, 신체나 재산상의 특징, 사회적 지위나 속성에 관하여 식별되거나 또는 식별할 수 있는 정보의 총체를 말한다.

우리나라의 현행 법률상 개인정보의 정의에 관해서 조금씩 차이는 있지만, 그 의미는 거의 유사하다 할 것이다.

우선 「공공기관의 개인정보보호에 관한 법률」제2조 제2호에서는 「개인정보」라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명· 주민등록번호 및 화상 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 말한다고 규정하고 있다. 예를 들면, 심신의 상태인 체력, 건강상태, 신체적 특징, 병력 등과 사회경력인 학력, 범죄경력, 직업, 자격, 소속 정당·단체 등 그리고 재산상황, 소득, 채권채무관계, 성명, 주소, 본적, 출생지, 본관 등을 들 수 있다.

「정보통신망 이용촉진 및 정보보호등에 관한 법률」제2조 제6호에서는 「개인정보」란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다고 정의하고 있다.

「전자서명법」 제2조 13호에서는 「개인정보」라 함은 생존하고 있는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다고 정의하고 있다.[4)]

개인정보라 함은 개인의 정신, 신체, 재산, 사회적 지위, 신분 등에 관한 사실 · 판단 · 평가를 나타내는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보하고 할 수 있다.[5)]

또한 1995년 클린턴 행정부가 창설한 IITF(Information Infrastructure Task Force)가 제시한 '개인정보의 제공과 이용에 관한 원칙'에서는 개인정보를 개인을 식별할 수 있는 정보로 정의하고 있다.[6)]

그리고 경제협력개발기구(OECD) 이사회의 권고안으로 1980년 9월에 채택된 '프라이버시보호와 개인정보의 국가 간 유통에 관한 가이드라인은 개인정보에 관해서 식별되거나 식별될 수 있는 개인에 관한 모든 정보라고 정의하고 있으며,[7)] 유럽연합의 「개인정보 보호지침」에서는 개인정보를 식별된 또는 식별 가능한 사람은 특히 신원증명번호 또는 육체적 · 심리적 · 정신적 · 경제적 · 문화적 · 사회적 정체와 특정하게 연결될 수 있는 하나 이상의 요인에 의해 직 · 간접적으로 식별되는 자연인에

4) 미국「켈리포니아주법」에서는 개인정보를 "개인의 이름, 주민등록번호, 신체외형기록, 주소, 전화번호, 교육정도, 재정상태, 의료기록 및 고용기록 등을 포함하나, 이에 한정되지 아니하며, 개인을 식별시키거나 묘사하는 기관에 의해 보관되는 정보"라고 정의하고 있으며, 유럽연합(EU)에서는 신체, 정신, 심리, 경제, 문화, 사회적 특성의 요소에 의해서 직·간접적으로 식별되는 자연인에 관한 정보를 말한다(제2조(a)). 金正熙, 前揭論文, 7-8면.

5) 2008년 8월 11일 행정안전부 공고 「개인정보보호법」 제정안 제2조 참조.

6) 박창욱, 「인터넷상 개인정보보호법제의 문제점과 개선방안에 관한 연구」, 울산대학교 대학원 석사학위논문, 2008, 7면.

7) 길준규, 「개인정보의 개념과 특징」, 토지공법연구 제18집, 2003, 246면.

관한 정보로 정의하고 있다. 일본의 2003년 「행정기관이 보유하는 개인정보의 보호에 관한 법률」 제2조 제2항에 의하면 “개인정보라 함은 생존하는 개인에 과한 정보로서 당해 정보에 포함되어 있는 성명, 생년월일 기타의 기술 등에 의해 특정의 개인을 식별할 수 있는 것을 말한다”고 정의하고 있다.[8)]

영국의 「데이터보호법」에서는 자연인의 신원을 식별할 수 있는 당해 데이터와 데이터관리자가 보유하거나 장차 관리할 가능성이 높은 기타 데이터나 정보 및 당해 개인에 관한 표현 및 데이터 관리자의 모든 지시사항, 그리고 해당 개인과 관계되는 모든 타인의 견해도 포함한다(제1조 제1항). 독일의 「데이터보호법」에서는 자연인의 신원을 식별하거나 또는 식별할 수 있는 정보주체에 관한 인적 및 물적 환경에 관한 일체의 정보를 말한다(제5조 제1항).[9)]

오늘날 개인정보는 일방적인 공개로부터의 보호를 통한 인격권,[10)] 개인정보를 매개로 한 자유로운 의사소통의 보장과 불가분의 관계를 가지면서도 다른 한편으로는 재산적 가치[11)]을 동시에 갖고 있으며, 현대 정보사회에서 정보통신기술의 발달과 이에 대한 정보보호의 심각한 불균형은 개인과 공공기관 및 민간기관에 의하여 개인정보를 거의 무제한적으로 축적 및 유통시키고 있다. 이러한 형태의 개인정보에 대한 처리과정은 단순한 재산적 피해와 같은 법률상의 이익을 침해시키는 것에 국한되지 않고 인격권, 프라이버시권, 교육권 등과 같은 기본권의 침해로 이어지고 있다.

---

8) 박창욱, 전게논문, 2008, 8면.
9) 金正熙, 前揭論文, 7-8면.
10) 조연상 외 2인, 「기업경영자원으로서의 개인정보이용 및 보호방안 연구」, 한국정보보호진흥원, 2001, 8면 참조.
11) 백윤철, 「헌법상 개인정보자기결정권에 관한 연구」, 법조, 2002, 173면.

제2절 개인정보의 분류

개인정보는 특정 개인을 식별할 수 있는 온갖 종류의 자료들을 지칭하는 것이며, 사회적 구성원으로서 자격을 나타내는 사회적 표식인 주민등록번호, 학번, 군번 등과 재산, 자질, 취미, 구매행동 유형, 심지어 개인의 신용상태나 그 사람이 가지고 있는 사회적 자원인 학연, 지연 등도 개인정보의 구성요소이다.

과거에는 공공부문과 민간부문에서 수집되는 개인정보는 단순히 손에 의한 기계적인 작업으로 정리 · 수행되었으므로 개인정보의 유형이 비교적 좁은 편이었지만, 현재는 정보기술의 발전으로 컴퓨터와 인터넷, 정보통신의 기술이 획기적으로 발전하게 되면서 공공부문과 민간부문에서의 개인정보 수집, 저장, 축적, 관리가 용이해졌으며, 개인정보 조합을 통한 제2차적 자료까지도 생산해 낼 수 있게 됨으로써 개인정보 보유유형도 매우 다양해지고 광범위해졌다.[12)]

다음 [표 1]에 제시된 개인정보는 개인에 대한 사실이나 속성 혹은 그에 대한 제3자의 판단 결과들을 나타낸 것이다. 따라서 이를 통해 역으로 특정개인을 확인하는 것이 가능하다. 하지만 14개의 정보유형들로부터 곧바로 특정 개인을 유추할 수 있는 것은 아니다. 하지만 주민등록번호, 학번, 운전면허번호 등은 배타적인 성질을 지니기 때문에 이로부터 특정 개인을 파악하는 것은 어렵지 않고 그것들로부터 특정 개인의 다른 속성들이나 정보들을 통합할 수 있는 열쇠 역할을 한다는데 더 큰 의미를 지닌다.[13)]

---

12) 고영석, 「전자감시사회와 프라이버시」, 커퓨티케이션북스, 1998, 29면; 金正熙, 前揭論文, 11면 재인용.

13) 한국형사정책연구원, 「개인정보침해에 관한 조사 연구」, 연구보고서, 2001, 75면.

<표 1> 개인정보 유형 및 종류

구 분	유 형
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적 등
가족정보	부모의 이름 및 직업, 배우자의 이름 및 직업, 부양가족의 이름, 가족구성원들의 출생지 및 생년월일, 가족구성원들의 주민등록번호 및 직업 등
교육 및 훈련정보	학교 출석사항, 최종학력, 학교 성적, 기술자격증 및 전문면허증, 이수한 훈련프로그램, 서클활동, 상벌사항, 성격 및 형태보고 등
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대 등
부동산 정보	소유주택, 토지, 자동차, 기타 소유차량, 상점 및 건물 등
동산정보	보유현금, 저축현황, 현금카드, 주식·채권 및 기타 유가증권, 수집품, 고가의 예술품, 보석 등
소득정보	현재 봉급액, 보너스 및 수수료, 기타 소득의 원천, 이자소득, 사업소득 등
기타수익 정보	보험(건강·생명 등) 가입현황, 수익자, 회사차·회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가·병가 등
신용정보	대부·잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록 등
고용정보	현재의 고용주, 회사주소, 상관의 이름, 직무수행 평가기록, 훈련기록, 출석기록, 상벌기록, 성격테스트 결과, 직무태도 등
법적정보	전과기록, 교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세 기록 등
의료정보	가족병력기록(심장병·암·알콜중독·정신병 등), 과거의 의료기록, 정신질환 기록여부, 신체장애, 혈액형 등
조직정보	노조가입, 종교단체 가입, 정당가입, 클럽 회원 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 도박성향 등

* 출처: Weible, Ricky Jay, Privacy and Data; doctoral dissertation, Mississippi State Univ.

이렇게 정보마다 그것이 갖는 의미가 다른 점은 개인정보의 보호와 관련하여 중요한 합의를 나타낸다. 또한 동일한 개인정보라 할지라도 민간부분에서 다루는 개인정보는 공공부문에서 다루는 개인정보와 비교 할 때 [표 2]와 같은 차이점이 나타난다.

<표 2> 공공부문과 민간부문의 개인정보 차이점

구 분	공 공 부 문	민 감 부 문
정보수집처	국가 공공기관	사기업
정보 수집의 방식	개인의사와 무관·강제수집, 개인으로부터 직접 수집	개인의 동의에 의한 제공, 제3자로부터 입수
정보 제공의 방식	국민의무 〉 서비스 혜택	서비스 혜택
정보 제공의 목적	국민으로서 정체성	개인의(경제) 신용이 근간
주된 사용처	일상생활 전반	소비 생활
개인정보 보호를 위한 법률	공공기관의 개인정보보호에 관한 법률	신용정보이용및보호에 관한법률, 형법, 여신전문금융업법, 금융실명거래및비밀보장에 관한법률

[표 2]에서 보듯이 민간부문에서 수집하는 개인정보는 공공부문에서 보유하고 있는 개인정보와 동일한 것도 있으나, 성격면에서 큰 차이점을 가지고 있다.

첫째, 정보수집의 방식에서 볼 때, 공공부문이 공공의 목적을 위하여 국민의 의무로서 개인정보를 수집하는 반면, 민간부문에서는 거래 당사자간의 동의에 의한 계약의 형식으로 이루어진다. 다만 현실적으로 불법적이기는 하지만 제3자로부터 입수되는 경우도 있다. 둘째, 개인이 각 부문에 정보를 제공하는 목적을 현대 사회에서 국가의 서비스를 받기 위해서도 있겠지만, 국가의 의무가 가장 핵심적이다. 반면 민간부문은 철저히 경제적 혜택을 받기 위하여 제공한다.[14]

제3절 개인정보와 프라이버시(Privacy)

인터넷의 급속한 발전은 프라이버시(Privacy)에 대한 많은 문제점을 야기하고 있다. 전자상거래는 전자적 수단에 의하여 이루어지므로 특정 소비자의 구매형태에 대한 정보를 쉽게 축적할 수 있다. 특히 거래에서 획득한 개인정보는 한편으로 정보통신서비스제공자의 영업비밀이 되기도 하지만, 다른 한편으로는 개인의 프라이버시에 대한 중대한 위협이 될 수 있다.[15] 한 예로 정보통신부가 2006년 3월 구글 검색엔진과 주민번호 노출점검 소프트웨어를 이용해 개인정보노출 상황을 점검한 결과 2005년 한해 동안 공공기관, 기업 등 1,900여개 기관 61만 여명의 개인정보가 노출된 것을 확인해 삭제 조치한 바 있다.[16]

개인정보보호는 프라이버시보호와 밀접한 관련을 가진다. 초기의 프라이버시권은 '혼자 있을 권리'인 소극적인 권리로 이해되었으나, 컴퓨터와 정보처리기술의 발달에 따른 정보화 사회가 진전됨에 따라 프라이

14) 김행미,「전자상거래에서의 개인정보보호방안에 관한 연구」, 경희대학교석사학위논문, 2002, 7-8면; 金正熙, 前揭論文, 12-13면 재인용.
15) 정용상, 「전자상거래 입법의 법적 문제」, 상사법연구, 제17권 제3호, 1999, 81면.
16) 사이버경제사회연구소, 「인터넷 개인정보 노출방지 및 프라이버시 보호 방안 연구」, 한국정보보호진흥원, 2007. 12, 6면.

버시의 개념이 이전의 비밀스러운 사생활을 보호하기 위한 개인적인 문제에서 벗어나 사회적인 가치로 부상하게 되었고,[17] 프라이버시의 침해 가능성은 더욱 증대되었다. 이런 배경하에서 소위 '정보상의 프라이버시(imformation privacy)'가 새로운 권리로 부각되고 프라이버시권의 성격도 소극적인 프라이버시의 침해배제로부터 적극적인 내용의 통제로 성격전환을 초래하였다.

'프라이버시'란 매우 광범위한 의미를 갖는 것으로 미국을 중심으로 19C 말에 정립되어 사회적 변화와 지역 · 개인의 사정에 따라 개념을 달리하면 점차 확대 적용되고 있다.

1903년에 뉴욕주가 최초로 Privacy Act를 입법으로 제정하였다. 1905년 Pavesich v. NEW England life Insurance Co. 판결[18]을 통해 조지아주 법원이 프라이버시를 권리로서 인정하기 이르렀다.[19]

또한 1965년 미국 연방대법원은 Griswold v. Connecticut 판결[20]에서 피임약의 사용을 제한하는 코네티컷주법을 개인의 '은밀한 결정권(intimate decision)'을 해치는 위헌으로 판시하면서 프라이버시권을 헌법적인 권리로 인정하였다.

우리 헌법은 제17조에서 '사생활의 비밀과 자유'로 프라이버시권을

17) 최근에는 개인의 은밀하고 비밀스런 정보는 물론, 이름 · 주소 · 전화번호, 성별, 직업, 교육수준, 소득, 가족관계, 건강정도, 취미, 구매형태, 신용정보 등 개인에 관한 모든 정보가 데이터 베이스(data base)화 되어 광고 등의 상업적 목적으로 이용되고 있으며, 더 나아가 범죄목적으로까지 이용되고 있는 실정이다.

18) Pavesich v. NEW England life Insurance Co., 122 Ga. 190. 50. S.E. 68(1904). 원고는 피고의 보험회사에 가입하지도 않았고 사진에 게제도 하지 않았음에도 불구하고 남루한 옷을 입은 병약한 사람의 모습으로 나온 자신의 사진을 게재함으로써 프라이버시권을 침해 받았다고 하여 손해배상을 청구한 사건이다.

19) 정찬모,「개인정보 오·남용 실태와 법제도적 대응방향」, 정보역기능방지대회 공청회 자료, 1999. 9. 8면.

20) Griswold v. Connecticut, 381 U.S. 479(1965). 피임기구의 사용을 금지하는 커네티컷주 법은 결혼에 있어서의 사생활의 권리를 침해하는 것으로 무효화하였으며, 연방대법원은 종래의 수정헌법 제4조에서 보장되었던 것과는 명백히 다른 헌법상의 프라이버시권을 인정한 사건이다. 권건보,「개인정보보호와 자기정보통제권」, 경인문화사, 2005, 24-25면 참조.

규정하고 있는데, 이는 성격상 제10조에 규정된 '인격권'의 한 내포로서 "내용을 공개당하지 아니할 권리, 자신에 관한 정보를 스스로 관리·통제할 권리 등을 내용으로 하는 인격권으로서 오늘날 정보화 사회가 급속히 진전되면서 그 보호가 절실한 권리이고..."로 일관되게 판시하고 있다.

과거에는 프라이버시라는 용어가 주로 사용되었으나, 최근에 이르러서는 프라이버시와 개인정보라는 용어가 혼용되거나 개인정보라는 용어가 자주 사용되는 경향이 있다. 프라이버시는 특정 개인을 식별할 수 있는 개인정보를 보호함으로써 보호될 수 있고, 개인정보보호는 개인정보의 수집·처리·이용에 의한 프라이버시 침해를 예방하거나 구제하는 것이므로 프라이버시보호의 한 부분이라 할 수 있다. 즉 프라이버시는 정보주체가 자신의 개인정보에 대한 보호를 위하여 지켜야할 권리가 강조된 개념인데 반하여 개인정보는 보호되어야 할 대상으로서의 객체적 존재라고 할 수 있으므로 개인정보의 보호는 프라이버시 개념이 그 외연을 확대하면서 새롭게 추가된 문제로서 프라이버시가 개인정보보호 보다 폭넓은 개념으로 이해할 수 있다.[21]

정보화 시대에 개인정보보호가 과거의 프라이버시보호와 구별되는 점을 설명하면 다음과 같다.

첫째로 보호의 대상이 확대되었다는 점이다. 과거의 프라이버시의 보호대상은 비밀스럽거나 개인을 난처하게 할 우려가 있는 사적 정보의 보호가 주된 내용이었다. 그러나 개인정보보호는 개인의 식별이 가능한 일체의 정보를 보호의 대상으로 한다. 아주 사소한 것일지라도 데이터베이스에 저장된 개인정보는 정보통신기술에 의한 분류를 통해 개인에 대한 체계적인 평가를 가능하게 하고, 영구보존이 가능하며, 광범위하게 전달

21) 박창욱, 「인터넷상 개인정보보호법제의 문제점과 개선방안에 관한 연구」, 울산대학교 대학원 석사학위논문, 2008, 9면.

될 수 있기 때문이다. 둘째로 프라이버시보호는 사적 정보에 대해 개인에게 불가침의 영역을 보장하는 소극적 측면의 보호인 반면 개인정보보호는 개인에게 적극적으로 자신에 관한 정보의 수집 · 처 리· 유통 및 제공에 있어서 통제권을 인정하며, 접근권을 부여한다.

제4절 개인정보보호에 관한 국내 · 외 동향

1. 국제기구의 개인정보보호 규범

경제협력개발기구 OECD는 1980년에 「프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침」(Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data),[22] 1981년의 유럽회의(EU) 협약,[23] 1990년 12월 14일 UN총회의 결의로 '컴퓨터화된 개인정보파일의 규율에 관한 지침' 즉, UN 가이드라인(Guidelines for the regulation of computerized personal data files),[24] 1995년 EU

22)「프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침」(Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data) OECD는 1998년 12월 「범세계적 네트워크상의 프라이버시 보호에 관한 각료선언」(Ministerial Declaration on the Protection of Privacy on Global Networks)에서 1980년에 채택한 8원칙이 인터넷 환경에서도 적합하다는 점에 동의하고, 각국이 네트워크 환경에서 효율적인 프라이버시 보호조치를 취할 것을 촉구하였다.

23)「개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의협약」(Council of Europe Convention No.108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data in 1980: CoE 108)은 1985년 10월 1일 발효되었다. 이 협약은 OECD 이사회의 권고에 기초를 두고 성립하였다. 유럽이사회는 1990년 회원국 간의 개인정보보호법의 조화·통일의 방향을 모색하기 위하여 개인정보보호에 관한 입법초안을 제시하였다.

24)「컴퓨터화 된 개인정보 파일의 규율에 관한 지침」(Guidelines for the regulation of computerized personal data files)의 개별 원칙들은 다음과 같다. ①합법성과 공정성의 원칙(Principle of Lawfulness and Fairness)으로 개인에 관한 정보는 합법적으로 수집·처리되어야 하고, UN헌장에 명시된 목적과 원칙에 반해서는 안된다. ②정확성의 원칙(Principle of Accuracy) 정보를 수집·저장하는 사람 및 이에 관하여 책임있는 담당자는 개인정보를 정기적으로 검사하여 수록된 정보가 정확한 정보인지를 검토하여야 한다. ③목적구체성의 원칙(Principle of

개인정보보호지침[25] 등이 국제기구에서 확립된 개인정보보호 원칙이라 할 수 있다. 그 결과 개인정보보호 기준에 관하여는 광범위한 국제적 합의가 형성되어 있는데, 대체로 다음과 같이 요약할 수 있다.[26]

① 정보처리자는 자신이 보유하고 있는 모든 개인정보에 대하여 책임을 져야한다. ② 개인정보의 수집시 또는 그 전에 개인정보처리의 목적을 분명히 밝혀야 한다. ③ (특정 상황에서 예외가 허용되지만) 정보주

---

the Purpose Specification) 개인정보를 수집·처리하는 목적이 구체적이고 정당하여야 한다. ④이해당사자에 의한 접근의 원칙(Principle of Interested-person Access)으로 자신에 관한 정보가 수집되거나 저장된 경우 이해당사자는 이러한 정보가 어떻게 처리·사용되는지에 대하여 알 권리가 있으며, 잘못되거나 정확하지 않은 정보의 삭제권 등 여러 보호권리를 가진다. ⑤비차별의 원칙(Principle of Non-discrimination)으로 개인정보의 주체들은 종교적·인종적·성적 차이나 정치적 견해 등을 이유로 부당하거나 자의적인 차별을 받아서는 안된다. ⑥예외에 대하여 결정할 수 있는 권한(Power of make Exceptions)으로 위에서 열거된 원칙에 대한 예외는 국가안전보장, 질서유지, 타인의 자유와 권리보호 및 반인류적 범죄를 범한 범인 추적 등 그 목적과 근거가 국내법 절차에 따라 정당하게 제정된 법 규정에 구체화된 경우에 한하여 인정될 수 있다. ⑦안전의 원칙(Principle of Security)은 자연재해, 컴퓨터 바이러스, 권한 없는 접근 등으로부터 개인정보파일을 보호하기 위한 적절한 조치들이 행해져야 한다. ⑧감독과 제재(Supervision and A Sanctions)로 모든 국가들은 열거된 원칙들의 준수를 감시할 독립된 기관을 설치하여야 하고, 이 원칙들을 위반한 경우에 대비하는 처벌규정 및 개인정보보호규정들을 만들어야 한다. ⑨국경 없는 정보의 흐름(Transborder Data Flows)으로 개인정보가 한 국가에서 다른 국가로 전달될 경우 사생활 보호에 관한 충분한 보호대책들이 마련되어 있다면, 정보는 관련국가들 내에서 가능한 한 자유롭게 전달, 처리되어야 한다. ⑩적용범위(Field of Application)는 열거된 원칙들은 모든 공적·사적기관에 적용되어야 하고, 컴퓨터 파일 뿐만 아니라 수작업 파일도 적용대상에 포함된다. 박창욱, 전게논문, 16-17면 참조.

25)「개인정보의 처리 및 개인정보의 자유로운 유통에 관한 개인정보보호준칙」(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data). EU의 유럽의회(European Parliament)와 유럽이사회(European Conucil)는 1995년 공동으로 '개인정보의 처리와 개인정보의 자유로운 유통에 관한 개인정보보호준칙'을 채택하였다. EU의 개인정보준칙은 OECD의 개인정보보호지침 보다 그 내용에 있어서 보다 구체적이고 상세하게 규정하고 있으며, 공공·민간 부문에 공동으로 적용되는 강력한 개인정보보호조치를 포함하고 있다. 또한 이 준칙은 법적 구속력을 갖기 때문에 EU 회원국은 이를 준수하야야 한다. 박창욱, 전게논문, 20면 참조.

26) Colin J. Bennett & Rebecca Grant, "Introduction", in Visions of Privacy: Policy Choices for the Digital Age, Colin J. Bennett & Rebecca Grant eds., 1999, 6면; 이인호, "개인정보보호에 대한 국제적 논의방향과 국내 법제의 개선방향",「개인정보보호 국외동향과 한국의 대응방안」, 한국정보보호진흥원 2002년 제2회 개인정보보호 워크샵 자료집, 2002. 7. 26, 8면.

체의 인식과 동의 하에서만 개인정보를 수집하여야 한다. ④ 미리 밝힌 목적에 필요한 한도 내에서만 개인정보를 수집하여야 한다. ⑤ 정보주체의 동의가 있는 경우를 제외하고 미리 밝힌 수집목적 이외의 다른 목적으로 개인정보를 이용하거나 제3자에게 제공해서는 아니 된다. ⑥ 필요한 기간 동안만 개인정보를 보유하여야 한다. ⑦ 수집된 개인정보가 정확하고, 완전하며 최신성을 유지하도록 하여야 한다. ⑧ 적절한 보안장치에 의해 개인정보의 안전성을 확보하여야 한다. ⑨ 자신의 정책과 처리 관행에 관해 공개하고, 비밀리에 처리 시스템을 운영하는 것은 절대 허용되지 아니한다. ⑩ 정보주체에 대하여 자신의 정보를 열람하고 필요시에는 그것을 수정할 수 있는 기회를 제공하여야 한다.

이러한 기본원칙은 범세계적인 네트워크 환경에서도 유효한 것으로 인정되고 있다. 1998년 10월 캐나다에서 열린 OECD 각료회의에서도 1980년 가이드라인에서 제시하였던 8개 원칙[27]을 재확인하고 있으며, 그 산하 위원회들도 전자상거래든지 지적재산권 보호이든지 1980년 가이드라인을 인정하는 범위내에서 이루어져야 함을 강조하고 있다.

또한 2001년의 9·11 테러 사건을 계기로 사이버 공간에서의 보안이 중요 관심사로 대두됨에 따라 OECD에서는 2002년 7월 주목할 만한 지침을 새로 내놓았다. 사이버 테러의 가능성을 방지하고 정보 시스템 및 네트워크에 대한 위협에 능동적으로 대처할 필요가 있다고 보고 OECD 이사회는 7월 25일 「정보 시스템 및 네트워크의 안전을 위한 지침」[28]권고안을 채택하였다.

---

27) ①수집제한(collection limitation)의 원칙 ②정보정확성(data quality)의 원칙 ③목적구체성(purpose specification)의 원칙 ④이용제한(use limitation)의 원칙 ⑤안전성확보(security safeguards)의 원칙 ⑥공개(openness)의 원칙 ⑦개인참여(individual participation)의 원칙 ⑧책임(accountability).

28) OECD Guidelines for the Security of Information Systems and Newworks: Towards a Culture of Security. 새 지침은 1992년 11월 처음 공표 되었던 OECD Guidelines for the Security of Information Systems을 대체하게 된다.

OECD 이사회에서는 정보 시스템 및 네트워크가 전세계적으로 확산되면서 정보에 대한 무단접근, 부당한 이용 · 변경, 악의적인 코드(컴퓨터 바이러스)의 유포, 서비스 거부, 파괴와 같은 위협이 증대되고 있음을 똑바로 인식해야 한다고 강조하고 그에 대처하기 위한 정책과 관행, 조치, 절차가 필요함을 지적하였고, 나아가 이와 같은 행태를 단순한 정보시스템의 보호차원을 넘어 '보안의 문화'(culture of security)로 고양시키고 국제협력을 강화할 것을 촉구하였다. 그렇지만 OECD의 새 지침은 강제적인 것은 아니며 각 회원국이 자발적으로 수용할 것을 권고하는 데 그치고 있다.[29]

2. 주요 국가의 개인정보보호 법률 동향

가. 미 국

개인정보보호 입법방식을 공공부문과 민간부문을 포괄적으로 규율하는 옴니버스형, 별개의 법률로 나누어 규율하는 구분(segment)형, 규제대상을 한정하여 개별법으로 규율하는 영역(sectoral)형으로 구별한다면[30] 미국은 세 번째 유형에 속한다. 예를 들어 연방행정기관의 개인정보취급에 관하여는 「프라이버시법」(Privacy Act of 1974),[31] 예산관리국(Office of Budget Management)의 정보수집에 관한 「정부문서업무

29) 한국정보보호진흥원, 「2002 개인정보보호 백서」, 2002, 참고.
30) 岡村久道 · 新保史生, 「電子ットフ-クと 個人情報保護- オンラインプライバシ-法入門」, 經濟産業調査會, 2002, 93面.
31) 미국은 1974년에 프라이버시법을 제정하였다. 미국 정부기관이 보유한 기록을 보호하는 것을 목적으로 하고 행정기관의 개인정보이용에 대한 제한으로서 사적정보의 공개요건 및 방법을 규정하고 있다. 김재광,「영미법계 국가의 개인정보보호법제 동향 및 함의」, 공법학 연구 제6권 제2호, 2005, 120면; 권태웅,「미국의 전자정부법제와 추진전략」, 법제, 법제처, 2004, 25면.

감축법」(Government Paperwork Elimination Act of 1980),[32] 연방 데이터베이스의 비교·합성에 관한 「컴퓨터 연결 및 프라이버시법」(Computer Matching and Privacy Protection Act of 1988) 등이 시행되고 있다. 그 밖에 개인정보는 「케이블통신정책법」(Cable Communications Policy Act 1984),「비디오 프라이버시법」(Video Privacy Protection Act 1988), 「텔리커뮤니케이션법」(Telecommunications Act 1996) 기타 주법과 판례에 의하여 보호되고 있는 실정이다.[33] 일찍이 프라이버시권을 인정하였던 미국은 정부 차원에서도 연방거래위원회(Federal Trade Commission)는 온라인 프라이버시에 관한 자율규제 및 기술적 해결을 모색하였고, 상무부(Department of Commerce)에서도 정보통신업계가 자율적으로 개인정보보호를 추진하도록 하였다. 1999년 11월에 제정·공포된 「금융 서비스 근대화법」(Financial Modernization Services Act 1999)에서는 금융기관에 보다 엄격한 개인정보보호 의무를 부과하고 있다.[34]

이후 2002년 12월에 부시행정부는 시민 중심적이고 결과 지향적이며 시장에 기반을 둔 연방정부를 만들기 위한 조치의 하나로 전자정부 서비스 및 절차의 관리 및 향상을 촉진하기 위하여 「전자정부법」을 제정하였다. 이 법은 전자정부를 정부가 국민·단체 및 그 밖의 정부기관의 정부정보 및 서비스에 대한 접속 및 이들에 대한 정부정보 및 서비스의 제공 원활화 또는 정부업무의 효과성과 효율성 그리고 서비스의 질 또는 변화가 포함된 개선을 도모하기 위하여 일정한 절차와 결합된 웹 기반

32) 미국은 1980년에 정부문서업무 감축법을 제정하였으며, 당시 지나친 문서작성과 유통으로 인한 시간 및 비용이 행정의 생산성을 저하시키고 국민에게 불편을 주게 되어 정보자원관리의 필요성이 제기되었다. 이 법은 정보의 자원으로서의 중요성을 확인하고 각 기관의 업무수행 과정에서 정보기술의 활용도를 향상시키기 위하여 연방법에 정보자원관리의 개념을 도입한 것이다. 이후 이 법률은 1986년, 1995년 1998년 개정을 하였다. 권태웅, 상게논문, 36-37면; 임지봉, 「미국의 전장정부법제」, 한국법제연구원, 2001, 14-15면 참조.

33) 松井茂記, 「アメリカ-プライヴァシ-保護法制の展開」, 法律時報, 72卷10號, 200. 9, 26面.

34) 金正熙, 上揭論文, 31-32면 참조.

인터넷 응용 및 그 밖의 정보기술을 이용하는 것으로 정의하고 있다.[35]

이러한 관점에서 미국 정부는 EU측과 국경을 넘는 정보유통(transborder data flow : TBDF)에 관한 협상을 하면서 민간자율에 무게를 두고 '세이프하버 원칙'(Safe Harbor Principles)이라는 색다른 접근방법을 제시하였다.

EU지침은 역외로 전송되는 개인정보에 대하여 국가적인 적절한 보호를 요구하고 있으나, 미국은 개인정보보호에 대한 자율규제와 정부규제를 혼합한 세분화된 접근방법을 취하여 관련기업들이 세이프하버 원칙을 자발적으로 준수하겠다고 상무부에 신고할 경우 그 혜택을 받을 수 있게 한 것이다.

EU 개인정보보호작업반에서는 수 차례에 걸쳐 세이프하버 원칙의 범위를 좀더 명확히 하고 예외 사유를 줄이며, 공공기관이 분쟁의 해결 등을 책임지고 관장하게 하는 등 일부 내용을 보완하도록 의견을 제시하여 집행위원회가 미국과의 협상을 타결할 수 있게 하였다.

이 방식에 대하여 프라이버시 주창자들과 소비자단체에서는 반대를 하였지만, 미국 정부는 EU측에 로비를 벌여 이를 관철시켰다.[36] 미국의 세이프 하버 원칙과 그와 관련된 질의응답 사례집(FAQs: frequently asked questions)의 골자를 살펴보면 다음과 같다.

①고지(Notice): 세이프하버 원칙의 적용을 받고자 하는 조직(organizations)은 정보주체인 개인에 대하여 정보수집·이용 목적과 용도, 제3자 정보제공, 고충처리 방법, 정보의 이용제한 방법을 고지하여야 한다. ②선택(Choice): 조직은 개인정보의 제3자 제공, 목적외 이용에 대하여 정보주체가 선택적으로 배제할 수 있게 하고, 인종, 정치적 신조, 노조활동,

35) 박창욱, 전게논문, 28면.

36) EPIC & Privacy International, Privacy & Human Rights: An International Survey of Privacy Laws and Developments, Electronic Privacy Information Center Washington, DC, 2001. p.17.

성생활 등의 민감한 정보는 명백하게 선택하게 하여야한다. ③제3자 전송(Onward Transfer): 제3자 정보 제공시 고지 및 선택의 원칙을 따르고, 제3자가 세이프하버 원칙을 준수하는 조건으로 이를 허용한다. ④안전성(Security): 조직은 개인정보를 생성, 유지, 이용, 보급함에 있어 손실과 오용, 무단접근, 공개, 변경, 파기로부터 보호할 수 있는 조치를 취하여야 한다. ⑤정보의 무결성(Data Integration): 개인정보는 사용목적과 연관이 있어야 하며, 당초 정보주체가 동의한 목적과 양립할 수 없는 방법으로 정보를 처리할 수 없다. ⑥접근(Access): 정보주체는 조직이 보유한 자신의 정보를 열람하고 부정확한 정보는 수정하거나 삭제할 수 있어야 한다. 다만, 국가안보·공공의 안녕질서 등 공익에 반하는 경우에는 정보접근을 불허할 수 있다. ⑦실행(Enforcement): 프라이버시 보호 원칙을 위반한 데 따른 손해를 배상하고 세이프하버 원칙을 따르지 않을 경우에는 제재를 가해야 한다.

세이프하버 원칙은 미국과 EU의 합의일 뿐 국제적인 협약은 아니지만, 별도의 입법없이 업계의 자율규제를 통하여 개인정보를 보호한다는 점에서 국제적인 정보이전에 있어서 중요한 기준이 될 것으로 보인다.[37]

나. 캐나다

캐나다의 경우 EU 집행위원회는 2001년 12월 20일 캐나다「개인정보보호 및 전자문서법」(Personal Information and Electronic Document Act : PIPED Act)이 EU 개인정보보호지침 제25조 제6항의 기준에 합치된다고 인정하였다. 캐나다법은 클로벌 스텐다드에 맞추기 위해 2000년 4월 13일 제정되었는데 민간부문의 조직·기관이 개인정보를 영업활동과 관련하여 수집·이용·공개하는 경우에 적용된다.[38]

37) 金正熙, 上揭論文, 32-33면 참조.

이 법은 또한 각주의 입법권을 존중하여 주별로 이와 실질적으로 유사한 프라이버시법을 시행할 경우에는 주법의 적용을 받는 조직이나 사업활동(Organizations or Activities)에 대하여 연방법의 적용을 면제할 수 있다고 규정하였다(PIPED Act 제26조 2항). 그럼에도 주간의 또는 국제적인 개인정보의 수집·이용·공개행위에 대하여는 이 법이 적용된다.

캐나다는「OECD의 개인정보보호 가이드라인(1980)」및「국제적인 개인정보유통 가이드라인(1984)」을 준수하고 유엔의 개인정보 전산파일에 관한 가이드라인(1990)을 줄곧 지지해 왔다. 이에 따라 PIPED법이 비록 중요한 공공이익을 보호하고 공공의 영역에 속하는 정보를 인정하는 예외나 한계는 있지만 개인정보를 적절한 수준으로 보호하는데 필요한 기본원칙을 모두 망라하고 있음을 국제적으로 인정받은 것이다. 이러한 기준을 적용함에 있어서 사법적으로 구제 받을 수 있고 위반행위에 대하여는 민사책임을 물을 수도 있으며, 위반행위를 조사하고 이를 중지시킬 수 있는 권한을 가진 독립된 감독기구(Federal Privacy Commissioner)가 있다는 것도 좋은 평가를 받았다.

다만, EU 집행위원회는 투명성을 확보하고 EU 회원국의 개인정보보호 감독기관이 개인정보 처리와 관련하여 필요한 조치를 취할 수 있도록 특정 정보의 캐나다 이전을 정지시킬 수 있는 예외적인 상황을 명시할 필요가 있다고 보았다. 다시 말해서 캐나다 정보보호 감독기관이 캐나다의 정보수신자가 정보보호기준을 위반하였다고 판단한 경우, 또는 그러한 보호기준을 저촉할 가능성이 큼에도 캐나다 당국이 적시에 적절한 조치를 취하기 어렵다고 믿을 만한 사유가 있고, 계속적인 정보의 이전이 정보주체에 중대한 위해를 야기하고 EU 회원국 감독기관이 캐나다 측의 당

38) Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. [http://europa.eu.int] 참조.

사자에게 통보를 하여 시정할 기회를 주는 경우가 이에 해당한다.

캐나다는 EU로부터 개인정보를 적절한 수준으로 보호하고 있다는 인정을 받았지만, 동 법의 적용을 받지 않는 캐나다측 당사자에게 정보를 이전할 때에는 EU가 인정하는 표준계약을 체결하는 등 적절한 보호조치(safeguards)를 강구하지 않으면 안 될 것이다.[39]

다. 일 본

일본에서 개인정보의 근원이 되는 프라이버시 권리는 "연희의 그림자 사건"[40]에서 관한 동경지재판결(東京地裁判決)[41]이다. 이 판결을 통하여 프라이버시 권리를 '사생활을 함부로 공개하지 안니할 법적 보장 내지 권리' 즉, '홀로 있을 권리' 라고 정의하였다.[42] 일본에서의 프라이버시보호에 관한 논의는 1974년부터 중앙정부 차원으로 시작한 이래 행정관리청에 설치된 행정관리위원회에서 연구를 착수하였고, 1976년에는 '전자계산기 처리 데이터 보호관리 준칙' 을 제정하여 시행하였다. 민간부문을 대상으로 한 개인정보보호는 지장자치단체별로 '프라이버시 보호에 관한 조례' 에 의해서 보호되고 있었으나, 포괄적인 법률이 존재하지 않아 정부지침과 고시 및 자율규제에 의존하였다.[43]

일본은 개인정보보호가 공공부문과 민간부문으로 나뉘어 서로 다른 법

39) 金正熙, 上揭論文, 34-35면 참조.

40) '연희의 그림자 사건' 은 동경도지사 선거의 후보자였던 인물과 그의 처간의 애정문제를 묘사한 삼도유기부의 소설 '연희의 그림자' 를 둘러싸고 소설의 모델이 된 전 외무대신이 프라이버시 침해를 이유로 손해배상과 사죄광고를 청구한 사건으로 법원은 프라이버시를 '사생활을 함부로 공개하지 안니할 법적 보장 내지 권리' 라고 정의하고, 그 불법침해에 대하여 법적 구제를 부염함에 있어서 가장 중요한 인격적인 이익으로 위자료의 지불을 명하였다.

41) 東京地裁判決, 소39 · 9 · 28 판시 385호 12혈.

42) 백윤철 외, 「개인정보보호법」, 한국학술정보(주), 2008, 158-159면; 박창옥, 전게논문, 33면 재인용.

43) 황상철, 「일본의 개인정보보호를 위한 입법동향」, 법제, 2003, 65면, 박창옥, 전게논문, 33면 재인용.

규에 이루어지고 있는데, 공공부문의 개인정보보호는 1988년 12월에 제정된「행정기관이 보유하는 전자계산기처리에 관한 개인정보의 보호에 관한 법률」이 근거법이다. 전국의 지방자치단체들도 기준에 맞추어 개인정보보호 조례를 시행하고 있다.

민간부문에서는 개인정보의 신용정보의 보호에 관해서는 '할부판매법'과 '대금업의 규제에 관한 법률', '취업안정법' 등 일반적인 개인정보보호법이 없이 부분적인 개별입법이 마련되었으며,[44] 통산산업성, 우정성의 개인정보보호지침[45] 사업자단체의 가이드라인이 시행되어 왔다.

한편 1994년부터 총리가 위원장인「고도정보통신사회추진본부」하에 개인정보보호검토부회 및 개인정보보호법제화전문위원회를 중심으로 개인정보보호 입법을 추진해 온 일본정부는 민간부문 전체를 망라할 수 있는 개인정보보호 법제를 마련하고, 또 향후 예상되는 對 EU 협상에서 고지를 점하기 위해 2001년 공공부문과 민간부문을 아우르는 일반법 형태의「개인정보의 보호에 관한 법률(안)」을 국회에 상정되고,[46] 2003년 5월 23일 개인정보보호 관련 5개 법률[47]이 가결되었고, 2005년 4월 1일

44) 이자성, 「일본 개인정보보호제도에 있어서 운영현황 및 법적구성에 관한 고찰 -개인정보보호법 및 행정기관의 개인정보보호법을 중심으로-」,자치정보화조함 지역정보연구단, 국제지역학회, 2007, 962면 참조.

45) 일본 통산성은 1997년 3월「민간부문에서의 전자계산기 처리에 관련된 개인정보보호 가이드라인」을 마련하고, 전자상거래실증추진협의회(ECOM)는 1998년 3월「전자상거래 개인정보보호 가이드라인」을 제정하였다. 한편, 통산성에서는 1999년 3월 공업규격(JIS Q 15001)으로「개인정보보호 실천준수계획을 위한 규칙」을 제정하였다.

46) 일본「개인정보의 보호에 관한 법률(안)」은 제1장 總則, 제2장 基本原則, 제3장 국가 및 지방공공단체의 책무 등, 제4장 개인정보의 보호에 관한 시책 등, 제5장 개인정보취급사업자의 의무 등, 제6장 잡칙, 제7장 罰則 등으로 구성되어 비교적 글로벌 스탠더드에 맞게 만들어졌다는 평가를 받았다. 岡村久道・新保史生, 前揭書, 180-248面; 金正熙, 上揭論文, 36面 參照.

47) 개인정보보호 5개 법률은 '개인정보의 보호에 관한 법률', '행정기관이 보유하는 개인정보의 보호에 관한 법률', '독립행정법원등이 보유하는 개인정보의 보호에 관한 법률', '정보공개·개인정보보호 심사회 설치법', '행정기관이 보유하는 개인정보의 보호에 관한 법률 등의 시행에 따른 관계 법률의 정비' 등에 관한 법률이다. 그 중 '행정기관이 보유하는 개인정보의 보호에 관한 법률'은 기존에 '행정기관이 보유하는 전자계산기 처리에 관한 개인정보의 보호에 관한 법률'을 전면 개정한 것이다. 이자성, 전게논문, 962-963면 참조.

부터 시행되었다. 이 법률은 개인의 권리이익의 침해를 예방하며 이를 위해 행정기관에 있어서의 개인정보의 취급에 관한 기본적인 사항을 정하는 것을 그 목적으로 한다.[48]

일본은 개인정보보호제도를 추진하기 위하여 내각부와 총무성의 2개 부처를 두었다. 내각부는 공공·민간부문을 총괄하여 일본의 국가 전체적인 관점에서 개인정보보호제도를 추진하는 관점에서 국민생활심의회 소속으로 개인정보보호부회 및 정보공개·개인정보보호 심사회를 설치하고 있다. 개인정보보호부회는 국민생활심의회를 설치하여 공공단체, 사업자단체에 대한 개인정보보호 관련 가이드라인 및 기본방침 제정, 개인정보보호 운영상황 및 실태조사 수행, 인터뷰나 공청회 등을 통한 의견수렴을 수행하도록 하고 있으며, 정보공개 · 개인정보보호심사회에서는 법률이 규정한 정보공개의 결정, 정정결정 또는 이용정지결정 등에 대해 불복이 있는 경우 제3자적 입장에서 공정하고 중립적인 조사·심의를 수행하기 위하여 설치되었다.

한편 총무성은 행정기관 및 독립행정법인 등의 개인정보보호의 전체적인 총괄을 담당하고 있으며, 중앙행정기관의 경우 행정관리국의 행정정보시스템기획과에서 지방의 경우 자치행정국 지역정보정책실이 관장하고 있다. 중앙행정기관의 행정관리국은 주로 ‘행정기관이 보유하는 개인정보보호에 관한 법률’, ‘독립행정법인등이 보유하는 개인정보보호에 관한 법률’ 등을 제정 및 관리하며 가이드라인 및 규정의 제시와 매년 법률의 시행상황 조사 및 결과 공표 등을 수행하고 있다. 지방의 자치행정국의 지역정보정책실은 자치단체의 개인정보보호 뿐만 아니라 정보보안대책 추진, 가이드라인 정비, 정보보안감사 등의 제도정비 및 시책을 추진하고 있다. 특히 개인정보보호에 관해서는 2003년부터 5개 법률 등이 제정됨에 따라 개인정보보호 조례 제정 및 검토 등의 요청, 시 직원 등

48) 황종성, 「국외 개인정보보호법제 분석 및 시사점」, 한국전산원, 2004, 54-55면 참조.

을 위한 개인정보보호 핸드북 제작·배포, 2006년에는 과잉반응에의 대응 요청, 누설방지 등의 요청, 체제정비 등의 요청 등을 수행하고 있다.[49]

라. 홍 콩

홍콩 행정특구(Hong Kong SAR, China)에서는 개인정보(프라이버시)조례(Personal Data(Privacy) Ordinance)에 의하여 공공부문과 민간부문에서의 개인정보가 보호되고 있다. 온라인 상거래 역시 개인정보를 취급하는 경우 웹사이트를 운영하는 서버가 홍콩 내에 존재하고 홍콩에서 정보를 수집, 보관, 처리, 이용하거나 홍콩에 주된 영업소를 가진 조직이 정보를 관리하고 있다면 개인정보령의 적용을 받는다.

홍콩의 인터넷상에서의 개인정보 이용에 관한 가이드라인에 따르면 개인정보를 웹사이트를 통하여 수집하는 경우 당해 웹사이트의 운용주체를 명시하여야 하며, 그 운영자는 프라이버시 정책을 이용자가 알아 볼 수 있게 게시하여야 하며, 개인정보를 수집할 때에는 '개인정보수집 안내'(personal information collection statement: PICS, 收集個人資料聲明)에 링크시켜 이용자가 정보수집의 목적을 알 수 있게 하여야 한다. 다이렉트 마케팅에 이용될 경우에는 이를 명시하고 이용자가 그 선택을 배제(opt-out)할 수 있도록 해야하며, 민감한 정보는 암호를 사용하거나 암호를 사용하지 않을 경우에는 불안전함을 고시하여야 한다. 위 가이드라인을 위배한 경우에는 민사상의 손해배상책임은 물론 프라이버시 감독관의 조사결과에 따라서는 시정명령을 받게 된다. 감독관은 동 가이드라인을 구체화한 개인정보보호 책임자의 행동강령(codes of conduct)을 제정하기도 하는데, 현재 개인식별장치의 이용에 관한 규칙과 소비자 신용정보에 관한 규칙이 시행중이다. 홍콩의 개인정보감독기관에서는 인

49) 이자성, 전게논문, 965면; 박창욱, 전게논문, 34면 재인용.

터넷상에서 활동하는 기업들이 뜻하지 않은 제재를 받지 않도록 개인정보보호 규칙의 준수여부를 자가진단 할 수 있는 “프라이버시 세이프”라는 도구(PC kit)를 만들어 보급하고 있다.[50]

3. 국내 개인정보보호 법제 동향

개인정보보호는 오늘날 국제사회의 공통적 가치와 관심사가 되고 있다. 이미 국제연합(UN), 경제협력개발기구(OECD), 아시아·태평양경제협의체(APEC), 국제노동기구(ILO) 등이 개인정보의 적절한 보호와 합리적 이용을 보장하기 위한 원칙들을 제시한 바 있다.

이들 국제규범은 강제력은 없지만, 개인정보의 보호 및 이용에 관한 현대사회의 보편적 기준이 되고 있으며, 특히 이들 국제규범은 개인정보의 보호 뿐만 아니라 개인정보의 합리적 이용권도 보장되어야 함을 강조하고 있다.

이에 따라 국제적인 흐름에 맞추어 개인정보의 보호와 활용을 조화롭게 이끌어갈 수 있는 종합적인 개인정보보호법을 제정해야 한다는 사회적 요구가 증대되고 있는 것이 현실이다. 이하에서는 현재 국내 개인정보법제 동향을 살펴보고자 한다.

우리나라에서는 1989년 12월 개인정보보호법시안을 마련하였고, 1991년 5월 국무총리훈령 제250호로 ‘전산 처리되는 개인정보보호를 위한 관리지침’을 제정·시행하였다. 그 뒤 OECD 개인정보보호 가이드라인에 따라 1994년에 먼저 공공부분에서의 개인정보보호를 먼저 규정하였다. 예를 들면, ‘공공기관의 정보공개에 관한 법률’, ‘공공기관의 정보 공

50) 홍콩의 개인정보관련 법규는 한국정보보호진흥원이 APT(Asia-Pacific Telecommunity) 회권국을 대상으로 개인정보보호 실태를 조사한 결과를 참고하였다. 金正熙, 前揭論文, 38-40面 재인용.

개에 관한 법률 및 행정정보의 공동이용에 관한 규정' 등이다. 공공기관의 정보공개에 관한 법률은 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호하기 위하여 제정되었다. 공공기관의 정보 공개에 관한 법률은 공공기관이 보유·관리하는 정보에 대한 국민의 공개청구 및 공공기관의 공개의무에 관하여 필요한 사항을 정함으로서 국민의 알권리를 보장하고 국정에 대한 국민의 참여와 국정운영의 투명성을 확보하기 위해 제정되었다.이 외에도 공공부문에 있어서의 개인정보와 관련된 법률은 '주민등록법', '공직자윤리법', '민원사무처리에 관한 법률' 등이 있다.

민간부문에서는 '금융실명 거래비밀 보장에 관한 긴급재정 경제명령권', '신용정보의이용및보호에 관한법률', '통신비밀보호법', '전기통신사업법', '정보화촉진기본법', '전자서명법', '전파법', '정보통신기반보호법' '전자상거래등에서의 소비자보호에 관한 법률', '대부업의 등록 및 금융이용자 보호에 관한 법률' 등 그리고 2001년 들어서야 민간부분에서의 개인정보보호를 위한 일반법으로「정보통신망 이용촉진 및 정보보호등에 관한 법률」을 제정·시행하고 있다. 또한 1995년 12월 29일 개정된 형법은 사이버스페이스의 범죄행위를 컴퓨터 범죄로 명명하고 컴퓨터등사용사기, 업무방해(동법 제347조의 2, 제314조 제2항)등을 처벌하는 규정을 두고 있다.[51]

현재 국내 개인정보보호 체계와 관련 법률 및 규정을 정리해 보면 아래 [표 3]과 [표 4]와 같다.

51) 백윤철, 전게서, 50면.

<표 3> 국내 개인정보보호 체계[52)]

	분야	주요 법률	기타 개인정보 관련법	기타 업무상 비밀준수 규정
헌법	공공행정	공공기관의 개인정보보호에 관한 법률	· 공공기관의정보공개에관한법률 · 전자정부법, 주민등록법, 호적법 · 국정감사및조사에관한법률, 통계법 등	· 변호사법 · 법무사법 · 세무사법 · 관세사법 · 공인노무사법 · 외국환거래법 · 공증인법 · 은행법 · 근로기준법 · 노동위원회법 · 직업안정법 · 공인중개사의업무및부동산신고거래에관한법률 · 형법 제317조 등
	정보통신	정보통신망이용촉진및정보보호 등에관한법률	· 통신비밀보호법 · 위치정보의보호및이용등에관한법률 · 정보화촉진기본법,정보통신기반보호법	
	금융신용	신용정보의이용및보호에관한법률	· 금융실명거래및비밀보장에관한법률 · 방문판매등에관한법률 · 전자상거래등에서의소비자보호에관한법률 · 전자거래기본법, 보험업법, 증권거래법 등	
	의료	보건의료기본법, 의료법	· 장기등이식에관한법률 · 생명윤리및안전에관한법률 · 인체조직안전및관리등에관한법률	
	교육	교육기본법	· 초중등교육법 · 교육정보시스템의운영등에관한규칙 등	

<표 4> 국내 개인정보보호 관련 법률 및 규정

52)「개인정보보호법안 」에 대한 공청회 자료집, 국회행정안전위원회, 2009. 4. 23, 227면.

연 도	개 인 정 보 보 호 관 련 법 및 규정
1983	·전기통신기본법 ·전기통신사업법
1986	·전산망보급확장과이용촉진에관한법률
1989	·전파법 개정(1962년 제정)
1991	·무역업무자동화에관한법률
1993	·통신비밀보호법 ·금융실거래및비밀보장에관한긴급제정경제명령
1994	·공공기관의개인정보보호에관한법률·정보통신설비에관한안전신뢰성기준 ·공업및에너지기반조성에관한법률
1995	·컴퓨터 범죄대응 규정에 관한 형법(1953년제정)개정 ·정보화촉진기본법 ·신용정보의이용및보호에관한법률
1997	·공공기관의정보공개에관한법률 ·금융실명거래및비밀보장에관한법률
1999	·전산망보급확장과이용촉진에관한법률(개정)정보통신망이용촉진및정보보호에관한법률 ·공공기관의개인정보보호에관한법률 개정
2000	·개인정보보호지침
2001	·정보통신망이용촉진및정보보호에관한법률(개정) ·전자정부구현을위한행정업무등의전자화촉진에관한법률(제정)
2002	·개인정보보호지침· 정보통신망이용촉진및정보보호에관한법률(개정)
2003	·전자정부구현을위한행정업무등의전자화촉진에관한법률(개정)·정보통신망이용촉진및정보보호에관한법률(개정)
2004	·공공기관의정보공개에관한법률(개정) ·주민등록법(일부개정)· 정보통신망이용촉진및정보보호에관한법률(개정)
2005	· 정보통신망이용촉진및정보보호에관한법률(개정)
2006	·주민등록법(일부개정) ·정보통신망이용촉진및정보보호에관한법률(개정)
2007	· 공공기관의 개인정보보호에 관한 법률(개정) ·공공기관의 정보공개에 관한 법률 ·주민등록법(전부개정) ·전자정부법(일부개정) · 정보통신망이용촉진및정보보호에관한법률(개정)
2008	·공공기관의 정보공개에 관한법률 ·주민등록법(일부개정) ·공공기관 CCTV관리 가이드라인 · 정보통신망이용촉진및정보보호에관한법률(개정)
2009	·주민등록법(일부개정) ·공공기관의 개인정보파일 관리지침 · 정보통신망이용촉진및정보보호에관한법률(개정)

공공부문에서는 개별 법률들을 인터넷 시대에 부응하는 입법적 미비사

항들이 많이 존재하며, 특히 민간부문에서의「정보통신망 이용촉진 및 정보보호등에 관한 법률」은 인터넷과 전자거래에 대응하여 개인정보보호 장치를 마련함에 있어서 정보사회에서 인터넷과 전자상거래를 활성화시키기 위한 입법적 대응이다. 동법은 OECD의 개인정보보호원칙에 맞추어 인터넷 등에서의 개인정보를 보호하기 위하여 이용자의 동의에 기초한 개인정보 수집·이용·처리·제공, 이용자의 권리보장을 규정하고 있다.

현재 우리나라의 개인정보보호법제는「공공기관의 개인정보보호에 관한 법률」과「정보통신망 이용촉진 및 정보보호등에 관한 법률」[53]이 가장 대표적인 법률로서 이 두 법률에 의하여 개인정보보호가 이루어지고 있다. 전자는 공공기관에 한정되어 있고, 후자는 정보통신서비스제공자에 한정된다.「공공기관의 개인정보보호에 관한 법률」에서의 프라이버시보호는 개인정보의 보호를 의미하고, 동 법은 OECD의 가이드라인의 일반원칙을 그대로 수용하고 있다. 그리고「정보통신망이용촉진및정보보호등에관한법률」은 민간부분에서의 정보통신 이용자의 개인정보를 효과적으로 보호하기 위하여 시행되었다.

따라서 우리나라의 현행의 개인정보보호법제는 형법상 규정된 '비밀침해죄'와 전기통신에 대한 도청을 금지하고 있는「통신비밀보호법」상의 보호규정을 제외하면「공공기관의 개인정보보호에 관한 법률」이 주축으로 자리 잡고 있다. 그런데 이 법은 명칭에서 알 수 있는 바와 같이 공공기관이 취급하는 개인정보를 중심으로 규제하고 있다. 현재 민간부문 개인정보를 규제하는 포괄적인 일반 법률은 없으며, 분야별로 관련 조항이 존재하고 있다. 이처럼 우리나라의 개인정보보호관련 법규는 공공기관에 적용되는 일반 법률이 존재하는 반면, 민간부문에 있어서는 개별조항으로 산재하고 있는 실정이다.

53) 정보통신망법은 유비쿼터스 시대에 각종 컴퓨터 범죄와 사생활 침해 등 부작용을 수반하게 되었고, 이에 대한 대처로 1994년 1월 법률 제4734호로 동법을 공포하였다.

제3장 개인정보 침해의 현황 · 유형 및 사례 분석

제1절 개인정보 침해 현황

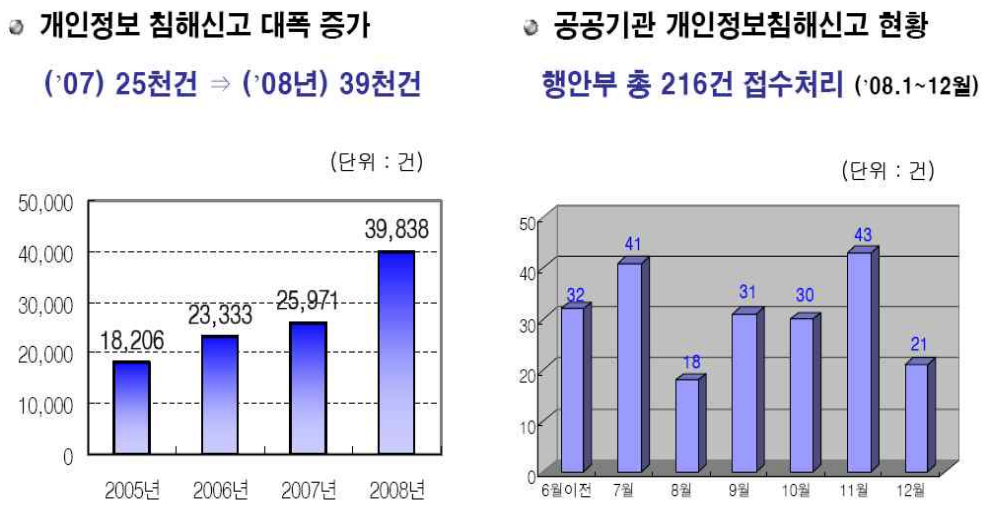
현재 우리나라는 전자정부를 통해 정부 혁신을 이룬 대표적 국가로 인식되고 있다.[54] 이는 2007년 8월 미국 브라운 대학이 발표한 세계 전자정부 평가결과 우리나라가 2006년에 이어 198개 국가중에서 1위를 차지하였으며, UN 전자정부평가에서도 우수한 성적을 거두는 등 세계 정상의 전자정부 수준을 공고히 하고 있다고 할 수 있다. 그러나 전자정부를 가능하게 했던 다양한 행정정보의 활용이 개인정보 침해 사고로 이어지는 경우가 발생되고 있다.

개인정보는 과거부터 다양한 형태로 존재하고 있으며, 최근들어 세상의 이목이 더욱 집중되고 있다. 이는 현대 자본주의의 발전, 시민사회의 성장, IT기술의 눈부신 진보에 기인한다. 현대의 기업들은 고객 정보가 기업 활동의 중요 요소라는 것을 알게 되었으며, 많은 관심을 기울이게 되었다. 국민은 국가와 기업에 의해 자신들의 사생활이 쉽게 감시당 할 수 있다는 사실을 알게 되었으며, 이러한 침해 위험성은 자신의 개인정보 침해 위험성은 자신의 개인정보와 프라이버시(Privacy)에 대한 침해가 그 어느 시대보다 높은 우려감을 나타내게 되었다. 또한 급격히 발전

54) 2009년 9월 28일 서울에서 세계 42개 도시 CIO(최고정보화책임관) 및 도시대표들이 참석한 가운데 열린 '세계도시 CIO 포럼' 실무회의에서, 에서 합의된 사항을 살펴보면 창립총회는 오는 2010년 10월 서울에서 개최하며 창립총회의 원활한 운영을 위해 임시의장은 서울시장이 수행하기로 했다. 서울시가 세계도시 전자정부 협의체의 핵심에 있음으로써 서울시의 창의적인 전자정부 서비스를 벤치마킹하려는 해외도시는 더욱 증가할 것으로 보이며, 2010년에는 60~70개 도시 대표단들이 대거 방문할 것으로 예상된다. Newdaily, 2009. 9. 29 일자.

하는 새로운 유비쿼터스의 기술은 특정영역이 아닌 사회 전반에 급속도록 파급되어지고 정보 유통이 점차 확대되고 있어 개인정보의 유출 가능성도 그 만큼 증대하고 있다. IT기술의 발전은 인간에게 인터넷이라는 새로운 기회를 제공해 주었으나, 개인 자신보다 자신의 개인정보를 더욱 정확하고 세밀하게 수집 · 분석하게 해주어 활용 여부에 따라서는 개인의 프라이버시 침해에 가장 커다란 적이 될 가능성을 제공하고 있다. 이에 개인정보보호는 선진 전장정부를 추진해 나가는 동시에 과도한 개인정보의 수집 및 이용을 방지하고 정보주체의 권리가 보장되도록 해야한다. 결국 개인정보를 취급함에 있어 공공업무의 적정한 수행과 동시에 국민의 권리와 이익을 보호해야 한다.[55]

<그림 1> 2008년도 개인정보 침해사고 현황



※ 출처 : 행정안전부

55) 2009 국가정보보호백서, 국가정보원·방송통신위원회·행정안전부·지식경제부, 2009. 4, 102면.

제2절 개인정보 침해 유형

최근 국내에서는 대규모의 개인정보유출 및 오· 남용 등 개인정보침해 사건이 사회의 큰 이슈로 등장하고 있어, 국민 모두가 개인정보의 보호에 대한 필요성을 인식하고 있으며, 정보통신의 발달에 따른 유비쿼터스의 기술은 개인정보의 유출 가능성도 증대시키고 있다.

더불어 모바일을 통한 행정서비스, T-Gov(IPTV) 등 신기술이 접목된 행정서비스의 등장으로 인하여 보호가 고려되어야 할 개인정보의 범위가 확대되고 있는 것이 현실이다.[56]

지난 2008년 한해 동안 발생했던 대표적인 대규모 개인정보 유출 사례를 살펴보면, ① 2008년 2월 해킹에 의한「옥션」고객 1,081만명의 개인정보가 유출된 사고가 있었으며, ② 2008년 9월에는 내부자에 의한 유출로 「GS칼텍스」고객 1,100만명의 개인정보유출이 있었다. ③ 2008년 7월에는 관리소홀로 인한 「다음」고객 53만명 이메일 정보 유출되었으며, ④ 2008년 4월에는 개인정보 오·남용으로 인한 「하나로 텔레콤」고객 600만명의 개인정보 무단 제공 등 2008년 한해에도 공공기관 및 민간기관을 가릴 것 없이 개인정보가 불법 유출, 판매되는 등의 충격적인 침해사고가 지속적으로 발생하였다.

2008년 12월 한국정보보호진흥원에서 개인 인터넷 이용자들(1,184명)을 대상으로 실시한 정보보호 실태조사에서 개인정보 및 프라이버시 침해 피해의 주된 유형은 다음과 같다.

첫째, '사업자의 관리 소홀로 개인정보가 유출된 경우(72.5%)'를 꼽은 응답이 가장 많았다. 즉, 관리부주의로 인한 개인정보 유출이 가장

56) 행정안전부, 「공공기관 개인정보보호 이해와 해설」, 행정안전부 개인정보보호과, 2008, 25면.

높은 것으로 나타났다. 2007년에는 관리자의 부주의로 고객 개인정보 190만건이 노출되는 사건과 2008년 발생했던「다음」고객 53만명 이메일 정보 유출(′ 08. 7)도 역시 대표적인 관리 소홀로 인한 개인정보 유출 사례이다.

둘째, ‘사업자가 귀하의 동의 없이 개인정보를 본래 목적 이외의 용도로 이용하거나 제3자에게 제공한 경우(58.4%)’ 및 ‘사업자가 귀하의 개인정보를 무단 수집하여 텔레마케팅 목적으로 이용하거나 무단으로 회원 가입시킨 경우(51.7%)’ 즉, 사업자의 고객 개인정보 무단이용으로 인한 개인정보침해라고 볼 수 있다. 2007년 초고속인터넷 사업자가 고객의 개인정보 730만 건을 부가서비스 무단가입 시키는 사건이 있었다.

셋째, ‘ID 및 비밀 번호 도용으로 게임 아이템, 사이버 머니, 캐릭터 등을 도난 당한 경우(26.3%)이다.

넷째, ‘주민번호 도용으로 웹사이트에 회원가입이 되지 않았거나 경제적인 피해를 입은 경우(22.9%)’ 순으로 나타났다. 즉, 외부의 공격, 해킹 등을 통한 개인정보 유출로 위의 해킹에 의한「옥션」고객 1,081만명의 개인정보 유출사고가 대표적인 사례이다.

2008년 한 해동안 한국정보보호진흥원의 개인정보침해신고센터와 개인정보분쟁조정위원회에 총 39,811건의 개인정보관련 피해, 상담, 신고가 접수되었는데, 이는 2007년 25,965건에 비하여 약 35%가 증가한 수치이다.[57]

개인정보 피해구제 상담 및 신고 접수 유형을 분석해 보면 신용정보침해 등의 정보통신망 이용촉진 및 정보보호등에 관한 법률 적용 대상 이외의 개인정보침해 관련 건수가 전체의 60.7%(24,144건), 주민등록번호 등 타인 정보의 훼손 · 침해 · 도용이 25.5%(10.148건)으로 전체 접수 유형의 86.2%를 차지하고 있다.

57) 2009 국가정보보호백서, 국가정보원·방송통신위원회·행정안전부·지식경제부, 2009. 4, 103면.

특히 2007년과 비교해보면, 정보통신망법 적용대상 이외의 개인정보침해 관련 접수건수가 전년대비 48% 증가한 24,144건을 차지하고 있다. 이는 2006년도 하반기부터 발생한 공공기관 또는 금융기관을 사칭한 전화사기가 2008년까지 지속적으로 증가하였기 때문이다. 또한 기술적 · 관리적 보호조치 미비로 인한 개인정보 누출, 주민등록번호 등 타인정보의 훼손 · 침해 · 도용 관련 접수 건수가 각각 전년 대비 61%, 48% 증가한 11,469건을 나타내고 있다. 반면, 이용자의 동의없는 개인정보 수집, 개인정보 수집 시 고지 또는 명시의무 불이행 관련 접수 건수가 각각 3%, 17% 감소했다. 이는 개인정보 관련 법제 강화 및 사업자 대상 개인정보보호 인식제고를 위한 다양한 교육활동 등이 주요한 원인으로 판단된다.[58]

<그림 2> 개인정보 유출에 따른 피해 유형[59]

피해 구분		이용정보	피해 유형	피해 가능성
명의 도용	인터넷 회원가입	성명 주민번호	• 회원가입 가능한 사이트에 타인명의 회원가입 • 사이버머니 취득 후 판매	높음
	기존회원 자격 도용	ID,비밀번호, 성명,주민번호	• 회원자격 도용 • 타인명의 비망글 게시	중간
	신분증 위조	성명, 주소, 주민번호	• 타인명의 각종 신분증 위조 • 위조신분증으로 타인명의 부동산 절취 • 불법취업 등 신분 위장	낮음 (위험 ↑)
	오프라인서비스 명의 도용	성명, 주소, 주민번호, 계좌번호	• 타인명의 금융계좌 및 휴대폰 개설 • 증권사 CMS 계좌이체로 금전탈취 • 보이스피싱용 대포통장 판매 • 타인명의 대포차 할부구매후 판매	낮음 (위험 ↑)
개인정보 불법 유통	개인정보 불법 유통	전 개인정보	• 통신사 영업점, 스팸발송업자, TM업자 등에게 판매되어 이용	높음
	인터넷 유포	전 개인정보	• 개인정보 판매 목적	중간
스팸	불법 스팸발송	이메일 전화번호	• 불법스팸 및 TM 발송에 이용	높음
피싱	보이스 피싱	성명, 주민번호	• 기관사칭 전화사기, 납치사칭 전화사기 등에 이용	높음

* 출처: 행정안전부

58) 2009 국가정보보호백서, 국가정보원·방송통신위원회·행정안전부·지식경제부, 2009. 4, 104면.
59) 행정안전부, 2009년도 개인정보보호 정책 방향, 행정안전부 정보화전략실 개인정보보호과, 2009, 4. 24.

제3절 개인정보침해 사례 분석

현재 개인정보 침해 신고는 지속적으로 증가하는 추세이며, 개인정보 침해에 대한 양상도 내부자에 의한 개인정보 유출, 사업자의 무단이용과 더불어 관리자의 부주의, 해킹[60] 및 웜 바이러스[61] 등 외부 공격에 의한 유출 등 다양하게 변화하고 있다.

<그림 3> 개인정보 침해 신고 및 침해양상의 변화

* 출처: 방송통신위원회(2008. 4. 24)

60) 해커의 자기 과시나 네트워크 · 시스템 마미 목적에서 개인정보 탈취 목적의 해킹이 증가하였는데, 2007년 해킹신고 건수는 21,732건으로 2006년 대비 18. 9% 감소했으나, 개인정보 탈취 등 '침입시도' 해킹(4,316건)은 오히려 16.3% 증가하였다. 방송통신위원회, 「인터넷상 개인정보 침해방지 대책」, 2008. 4. 24, 2면.

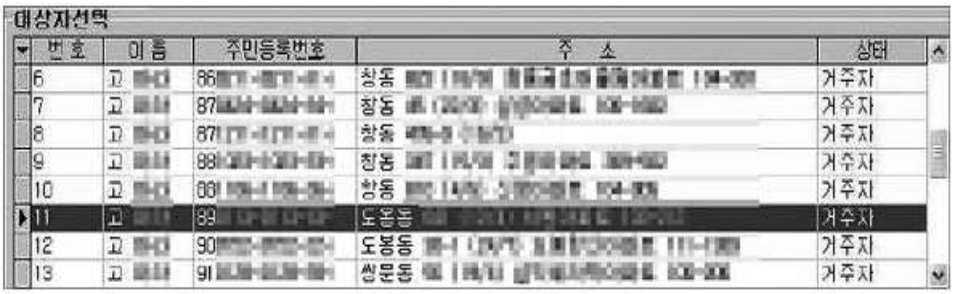
61) 스팸메일 발송, DDos 공격 등 시스템 통제 목적에서 개인정보 탈취를 목적으로 하는 유형이 증가하였다. 2007년 웜바이러스 피해신고는 총 3,639건 발생했으며, 이 중 ID · 비밀번호 등 개인정보 유출 목적의 Online game Hack 등은 전년 대비 71.7%가 증가하였다. 방송통신위원회, 상게논문, 2면.

1. 내부자에 의한 개인정보 유출

가. 주민등록 전산망을 통한 주민번호 인터넷 노출

2008년 8월 12일 정부의 주민등록 전산망을 통해 특정인(고씨)의 이름· 주민등록번호· 거주지를 조회한 화면 캡처(아래 그림)가 인터넷에 올라와 일주일여 동안 노출이 되었다. 이 화면에는 고씨와 이름이 같고 서울 도봉구에 사는 19명의 개인정보가 실려 있다.

<그림 4> 개인정보를 조회한 화면



전 국민의 주민등록 정보가 담겨 있는 주민전산망은 전국 3500개 읍· 면· 동 사무소에서 아이디를 부여받은 주민등록 업무 담당 공무원들만 접근이 가능한 행정통합 전산망의 하나이며, 주민전산망 조회 화면이 공개적으로 노출된 것은 이번이 처음이다.

이 사건은 베이징 올림픽 유도경기에서 은메달을 딴 왕기춘 선수에 대한 욕설을 인터넷에 올린 고씨에 대해 누리꾼들이 집단적으로 사이버 공격을 하는 과정에서 발생했다. 누리꾼들은 고씨의 개인정보인 사진은 물

론 인터넷 사이트의 ID, 게시글과 상담내역, 주민등록번호, 현 주소와 소속 대학, 전화번호 등을 유포시켰다. 이 과정에서 주민전산망을 통해 고씨의 정보를 조회한 화면이 인터넷에 노출이 된 사건이다.[62]

이 사건은 앞으로 개인정보보호위원회 같은 독립적인 기구를 설치하여 각종 개인정보를 수집· 관리하고 있는 정부부처 및 공공기관에 대한 감독, 집행, 징계권의 필요성을 보여준 대표적인 사례라고 할 수 있다.

나. 국방부 전산망에서 5만명 개인정보 유출

2008년 4월 국방부 전산망에서 예비군 명단과 주민등록번호 등 개인정보가 대량으로 유출되어 온라인 도박 사이트에 넘겨졌다. 육군 50사단 헌병대는 7월 18일 국방 동원 정보체계 시스템에 접근해 대구· 경북 지역 예비군 가운데 5만여명의 명단과 개인 정보를 빼내 온라인 '바다이야기' 도박 사이트를 운영하는 자신의 사촌형에게 건넨 혐의(정보통신망이용촉진 및 정보보호 등에 관한 법률 위반 등)로 대구 지역 한 예비군동대 상근 예비역 김모 상병을 검거했다. 또 온라인 도박사이트 홍보 등에 사용하기 위해 김모 상병한테서 명단과 개인 정보를 넘겨받은 사촌형 도 같은 혐의로 검거하였다.

<그림 5> 국방부 전산망 정보유출 과정

62) 한겨레 신문, 2008. 8. 20 일자.

국방부 헌병대의 조사 결과에 의하면, 김상병은 4월 초 사촌형 김씨의 부탁을 받고 자신의 상관인 중대장의 ID와 비밀번호를 알아낸 뒤 국방부 전산망에 접속해 예비군들의 개인정보를 USB 메모리를 이용하여 유출하였다. 김상병이 사촌형에게 넘긴 파일에는 예비군 5만여명의 소속 읍·면· 동대와 이름, 주민등록번호, 주소, 군번, 휴대전화 번호, 집 전화번호 등 다량의 개인정보가 담겨 있어, 이 유출된 개인정보를 통한 2차 피해가 우려되었다. 사촌형 김씨는 이렇게 빼낸 자료 가운데 일부로 인터넷 포털사이트 게시판 등에 자신이 운영하는 인터넷 사행성 게임 사이트의 광고용 블로그를 제작해 게시하였다.

김상병이 접근한 국방부의 국방동원 정보체계 시스템은 병무청의 전산망과 달리 일반 국민이 접근할 수 없고, 군부대나 국방부, 예비군 중대 등에서 허가된 예비군 중대의 중대장급 이상만 열람이 가능한 정보로서

내부 사람만이 접근할 수 있었다.[63] 특히, 국방동원 정보체계 시스템은 ID와 비밀번호만 입력하면 별도의 신분확인 절차 없이 열람이 가능한 것으로 알려져 국방부의 허술한 서버시스템에 문제가 제기되었다.[64]

다. 건강보험공단, 유명 연예인 정보 무단 열람·유출

2009년 4월에는 보건복지가족부가 실시한 '2008년 개인정보보호 실태점검'에서 보건복지부 본부와 소속 및 산하기관 11개 중에서 국민건강보험공단은 개인정보관리감독 등 4개 분야에서 1위로 선정되었다.[65]

국민건강보험공단에서 공개한 자료에 따르면, 2002년부터 2008년 5월까지 불법으로 개인정보가 열람된 건수는 무려 12,033건이며 이중 유출된 것만 1,885건에 이른다. 특히 무단 열람된 기록중에는 인기 연예인들과 유명 정치인의 기록도 다수 포함되었다. 보험공단 직원들이 불법으로 무단 열람한 이유는 단지 호기심 때문이라 하였다.[66]

특히 건강보험공단의 경우 남성스타와 관련된 여성의 낙태경험, 아파트 윗층 거주자의 신분 등 구체적인 개인정보까지 무단 열람하였다. 심지어 자신의 학위논문 작성을 위해서 장애인 정보 5천여건 활용하여 설문조사 하기도 하고, 근로자 570여명의 건강검진정보 활용하기도 하였다.[67] 이처럼 건강보험공단이 축적하고 있는 건강정보에는 주민등록번

63) 한겨레 신문, 2008. 7. 19 일자.
64) 시사1번지 폴리뉴스, 2008. 7. 20 일자.
65) 매일경제신문, 2009. 10. 8 일자.
66) LA타임스의 보도에 따르면 로스앤젤레스 캘리포니아주립대(UCLA) 병원의 내부직원들이 유명 연예인 진료내역 정보를 무단 검색 · 유출되었다고 한다. 캘리포니아 주 공중보건국의 조사결과 127명에 달하는 직원이 지난 2004년 1월부터 2년여 기간에 걸쳐 할리우드 스타 등의 유명 인사에 대한 진료기록을 무단으로 열람한 사실이 확인되었다. 유코피아뉴스, 2008. 8. 7일자.
67) 이외에도 집나간 아들을 찾기 위해 아들친구 주소를 검색하고, 회의참석자의 분실물 반환을 위하여, 군대후배와 동명이인 검색, 대학동기나 연락이 끊긴 지인의 연락처 조회, 동호회에서 알게 된 지인의 말이 사실인지 또는 지인의 사업내역 확인차 열람하고, 자신의 청첩장을 전하

호는 물론 질병과 치료 및 투약에 관한 정보까지 포함하고 있으므로 건강정보가 유출될 경우 프라이버시 침해를 넘어 치명적인 피해를 야기할 수 있다.

이와 관련하여 건강보험공단의 일부 내부 직원들이 업무와는 관계없이 개인 건강정보를 무단 열람하거나 유출하여 받은 징계 현황 즉, '건강보험공단 직원 징계조치 현황' 자료에 따르면, 2007년에는 53명에 달하는 공단 내부 직원이 정치인과 유명 연예인의 개인정보를 무단열람하거나 유출해 개인정보를 대부업체에 팔아넘긴 사례가 적발되어 징계를 받았으며, 2008년 22명의 직원이 개인정보 무단열람 및 유출, 업무목적 외 개인정보 불법열람 등의 이유로 징계를 받았다.

또한 2009년 현재까지 8명의 직원이 개인정보 불법열람 및 장기요양기관에 개인자료 제공, 업무목적 외 동료직원 개인정보 불법조회, 수급자 개인정보 유출 및 알선유인 등의 불법행위로 인해 징계를 받았다. 징계를 받은 직원은 1급부터 6급까지로, 징계 내용으로는 '업무목적 외 개인정보 불법열람' 의 경우 대부분 견책에 그쳤고, 일부 직원의 경우는 '개인정보 무단열람 및 유출' 에 대해 감봉 1개월에서 정직 3개월에 그치는 등 약한 처벌만 이뤄지고 있어 재발의 문제가 제기되고 있다.

따라서 개인의 건강정보 유출 문제 해결을 위해서는 약한 처벌도 한 요인으로 꼽히고 있기 때문에 징계 수위를 크게 높여서 함부로 부정행위에 손대지 못하게 해야 할 것이다. 또한 건강정보 유출을 막기 위해 이중삼중의 보안체계를 갖추면서 사용이 끝난 정보는 쌓아두지 말고 즉시 폐기하는 방안의 강구되어야 할 것이다.

그리고 국민의 신상정보를 일상적으로 취급하는 공공기관은 개인정보 보호에 만전을 기해야 할 것이며, 공공기관에서 개인정보 무단 열람, 유출행위를 근절할 수 있는 법률적 근거를 정비해야 할 것이다.[68]

기 위해서 지인의 주소를 열람 하는 등 업무 외 목적으로 개인정보를 조회하였다.

특히, 개인정보보호에 취약한 의료 관련 법령도 문제인데, 현행 의료법은 환자의 건강정보를 기록한 진료기록부 등에 대해 환자의 요구가 있거나 법령으로 허용되는 특정한 경우를 제외하고는 원칙적으로 타인의 열람을 금지하고 있다. 하지만 건강보험공단 등 외부기관들이 보험료 청구심사 등의 목적으로 개인건강정보를 수집한 것을 기회로 환자 동의를 구하지 않고, 목적 이외의 용도로 사용해도 이를 명백하게 규제할 조항이 없어 개인건강정보의 무분별한 유출이 사실상 현실화 되고 있는 실정이다. 따라서 공익의 목적이라 하더라도 개인건강정보의 활용에 대해 원칙적으로 환자의 동의를 구하고, 제한된 목적으로만 사용하도록 하는 등 입법적인 보완이 시급하다.

라. GS칼텍스 고객 1,100만명 개인정보 유출

2008년 서울 강남구 역삼동의 유흥가 뒷골목에서 1천125만여명의 개인정보가 담긴 CD 1장과 DVD 1장이 버려진 채 발견되었다. 이 중 DVD에는 3.1GB(기가바이트) 크기의 `GS 칼텍스 고객정보'라는 제목의 폴더 아래 1천125만여명의 개인정보가 담긴 76개의 엑셀파일이 있고, CD에도 샘플용 개인정보 파일이 일부 저장돼 있었다. 이 DVD는 정부 부처의 고위 관계자들이 포함된 전국 시도의 한국 국적자들의 이름과 주민등록번호, 이메일 주소 등을 출생연도별로 일목요연하게 담고 있다.[69]

1,100만여명의 단일 사건으로는 역대 최대 규모의 개인정보 유출사건을 일으킨 용의자들은 GS칼텍스의 고객정보 데이터베이스(DB)에 접근할 수 있는 권한을 가진 내부 직원들로 이들 4명은 GS 칼텍스 콜센터에 근무하여 고객정보 DB 접근 권한이 있는 정모씨 등 자회사 직원 2명과 정

68) 소비자가 만드는 신문, 2008. 8. 5일자.
69) 프라임 경제, 2008. 9. 6일자.

씨의 고교 동창, 그리고 강남 유흥가 뒷골목에서 개인정보가 담긴 DVD를 주웠다며 언론사에 제보한 김모씨이다.

이들이 지난 7월부터 직원 아이디로 고객정보를 빼내 이를 엑셀파일로 변환하여 유출하였으며, 개인정보를 팔아 개인적인 빚 등으로 돈이 필요해 범행을 공모하였다. 특히 피의자들은 GS칼텍스 전산시스템이 정보의 유출 여부를 제대로 확인하지 못한다는 점을 노렸다.

이 사건은 GS칼텍스 본사도 아닌 자회사 직원이 마음만 먹으면 얼마든지 고객정보를 통째로 빼낼 수 있다는 점에서 대기업의 허술한 개인정보 관리 실태를 여실히 보여주었다.

또한 전산시스템이 정보의 유출 여부를 제대로 확인하지 못한다는 점을 이용했다는 것을 기술적인 보안의 문제로 고객정보 데이터 베이스를 암호화하는 등의 조치가 필요할 것이다.[70] 또한 고객정보를 다루는 대기업 직원의 도덕불감증과 정유사의 고객정보 수집과 관리는 뚜렷하게 감독할 곳이 없다는 것도 하나의 원인으로 제기되었다.

이후 국내의 각 기업들은 내부정보 유출 방지에 대해 높은 관심을 보이기도 했고 또 실질적인 보안강화를 위한 보안 시스템 정비, 장비의 추가도입 등으로 이어졌다. 특히 고객정보 등 데이터베이스(DB)를 암호화해주는 수준을 넘어 최근에는 누가 언제 DB에 접근했는지를 추적하고 USB메모리나 이메일, 프린터 등을 활용한 유출 시도 즉시 이를 즉각 차단해주는 최신 기술들이 새롭게 조명을 받았다.

한편 2008년 11월 초 미국 '오픈 시큐리티 파운데이션(Open Security Foundation)'이 공개한 세계에서 가장 규모가 컸던 10대 개인정보 사건 순위 중에서 GS칼텍스의 고객 개인정보 유출 사건은 전 세계에서 일어난 대규모 개인정보 유출사건들 중 가장 규모가 큰 10개 사건에 포함

70) 서울경제신문, 2008. 9. 7 일자.

됐다는 발표도 있었다.

이 발표에 따르면 GS칼텍스 사건은 아시아권에서는 가장 큰 규모였으며, 2008년 5월 약 1,250만 명의 주민번호 등이 노출된 미국 뉴욕 멜론 은행, 아치브 시스템에 이어 8위를 기록했다. 또 1위부터 7위까지는 모두 미국과 유럽권의 기업·기관으로 나타나 GS칼텍스 사건은 아시아권 기업에서 발생한 개인정보 유출 사건 중 가장 큰 규모가 됐다.

불명예스런 1위는 미국 소매유통 업체 TJX 컴퍼니로 이 회사는 지난해 1월 무려 4,570만 고객의 신용카드 번호와 거래 기록을 해킹 당했다. 이 순위에는 유명 해외 기업들이 다수 포함되어 있어 날로 발전하는 해킹 공격 방법, 보안의식 부재, 각 기업의 허술한 보안 수준이 우리나라 뿐만 아니라, 전 세계적인 보안 이슈임을 알 수 있는 조사결과였다.[71]

마. 국가전산망에서 개인정보를 빼내 채권추심에 활용

채권추심업체 직원인 이모 씨 등 75명은 2008년 1월에서 4월 사이 채무자의 주민등록번호를 이용해 국가 전산망인 정부기관 사이트에서 개인정보를 유출한 혐의인 주민등록법 위반으로 검거 되었다. 이 중에는 공공기관인 한국자산관리공사(KAMCO) 내부 직원도 2명도 포함된 사건이다.

이들 수많은 채무자 가운데 돈을 빨리 회수할 수 있는 사람을 골라내기 위해 직장정보를 활용했는데, 이들의 범죄수법은 2008년 1~4월 채무자 1만여 명의 주민등록번호로 노동부 산하기관인 한국고용정보원의 직업정보종합전산망에 회원으로 가입해 채무자들의 직장 정보 등을 알아내어, 회원 가입 이후 자기능력개발카드를 작성하면 자동으로 직장 정보가

71) 월간 정보보호21c 통권 제100호; 보안뉴스, 2008. 12. 12 일자.

노출된다는 점을 이용하였다. 직장 정보가 노출된 것은 이 전산망에 근로복지공단의 고용보험 자료가 연동돼 있었기 때문이다.[72]

2. 개인정보 관리 소홀로 인한 유출

가. Daum, 고객 53만명 이메일 정보 노출

2008년 7월 22일 다음커뮤니케이션의 대형 포털사이트인 'Daum'의 서비스 중 이메일서비스에서 회원의 개인정보가 대량으로 노출되는 사고가 발생했다. 이 사건은 이날 약 50분간 로그인시 자신의 계정이 아닌 타인의 계정으로 로그인되어 타인의 메일함, 메일 목록 뿐만 아니라 일부 내용과 첨부파일도 무작위로 노출되는 문제가 발생하였다.

그러나 다음(Daum) 회사 측은 사고 직후 홈페이지를 통해 서비스 업그레이드 과정에서 나타난 문제라고 해명하면서 회원의 메일함에서 이메일 제목만 노출됐다고 밝혔다. 하지만 사고 이틀 뒤 다음(Daum) 회사의 대표는 "사고 당시 55만 명이 로그인했지만, '한메일 익스프레스'를 제외한 일반 '한메일' 이용자 43만 명의 이 메일함이 노출된 것으로 확인됐다"고 밝히면서 내용까지 노출됐다고 말을 바꾸었다.

결국, 다음(Daum) 측은 공지를 통해 '한메일 익스프레스'에서도 장애가 발생하였다고 발표하였다.

이후 다음측은 이 사건과 같은 유사사고에 대비하기 위해 신규 서비스 배포 전후 보안시스템 강화, 트래픽 과부하 상황에서의 강도테스트 및 보안기술 도입, 강력한 데이터 저장 및 복구 시스템 구축하였다. 다음의

72) 동아일보, 2008. 10. 30 일자.

이메일 노출 사고는 개인정보 노출 사고에서 대응의 투명성을 확보하지 않았을 때, 기업의 신뢰도에 큰 영향을 미치는 결과를 여실 없이 보여준 사고였다.[73]

현재 국민들은 인터넷 포털 이메일을 누구나 갖고 있으며, 업무용으로 사용하는 이용자들도 많다. 더불어 위의 다음 사례처럼 이메일 장애에 따른 피해는 유 · 무형으로 상당하다. 이는 단순히 장애에 그치지 않고 개인정보라도 유출될 경우 심각한 문제를 야기할 수 있다.

따라서 개인정보 관리자는 개인정보 유출 및 노출에 따른 제2차 범죄를 예방하기 위해서라도 보안강화에 적극적이어야 할 것이다.

나. 예비군 4,500명 개인정보 무더기 유출

서울대학교 재학생과 교수, 예비군 등 4천500명 개인정보 인터넷을 통해 무더기로 유출되었는데, 이 대학교 불어불문학과에 따르면, 2008년 5월 학과 인터넷 홈페이지 게시판에 예비군 훈련을 공지하면서 `대학명단.xls'라는 이름의 문서도 함께 게재하였다. 이 문서에는 불문과 소속 학생과 교수 뿐 아니라 예비군 훈련 대상자인 서울대 재학생과 교수 등 4천500여명의 이름과 소속, 연락처, 생년월일, 군번 등의 개인 정보가 고스란히 담겨 있었다.

이는 예비군연대에서 받은 것으로 예비군연대 측은 "훈련 대상자에게 휴대전화 문자메시지로 훈련을 통지하는데 요새 번호 이동이 잦아 3분의 1 정도가 기존 번호와 다르다"며 "각 대학에 훈련을 공지하면서 연락처 수정을 요청하느라 연락처가 포함된 명단을 보낸 것"이라고 하였다.

뒤늦게 학내 구성원의 개인 정보가 인터넷을 떠돌아다닌다는 사실을

73) 보안뉴스, 2008. 12. 31일자.

파악한 불문과 측이 이달 초 해당 게시물을 삭제했으나, 이미 이들의 개인 정보는 6개월 가량 인터넷 상에 무더기로 노출된 뒤였다.

서울대 지구환경시스템공학부도 지난 5월 `2008년도 1학기 관악캠퍼스 예비군훈련 안내'라는 공지 사항을 올리면서 예비군 훈련 대상자 중 소속 학생 100여명의 명단을 별도로 첨부하여 이들의 이름과 연락처 등을 장기간 홈페이지에 게시하여 개인정보를 노출시킨 것으로 확인되었다.[74]

<그림 6> 예비군 훈련 대상자 명단을 캡처한 화면('08. 11. 10 연합뉴스)

이 사건은 개인정보 관리자의 관리 소홀로 인하여 다수의 개인정보를 그대로 노출되도록 장기간 방치했다는 점에서 관리자의 안일한 개인정보 보호인식에 문제점이 있다. 행정안전부의 발표에 의하면, 개인정보 노출 사례의 50%는 관리자의 부주의나 자료게시자의 인식부족으로 인하여 발생한다고 한다. 따라서 위 사건에서 처럼 개인정보의 장기간 방치로 유출된 개인정보를 통하여 2차적인 피해 발생할 수 있다는 점에서 개인정

74) 연합뉴스, 2008. 11. 10 일자.

보 관리자는 반드시 유념해야 할 것이다.

3. 기술적 보호 조치 문제로 인한 개인정보 유출

가. 유가환급금 신청시 개인정보를 컴퓨터에 자동 저장

2008년 유가환급 신청대상은 원천징수 의무자 129만개 업체, 사업소득자 443만개 업체, 전체 유가환급금 지급 신청 대상자가 1650만명인데, 모 업체가 구축한 국세청의 인터넷 세무신고 사이트인 '홈택스'(refund.hometax.go.kr)에 유가환급금을 신청했을 때, 신청자의 개인정보를 자동으로 컴퓨터 하드디스크에 저장해 노출되도록 하는 보안상 결함문제가 있는 것으로 나타났다.

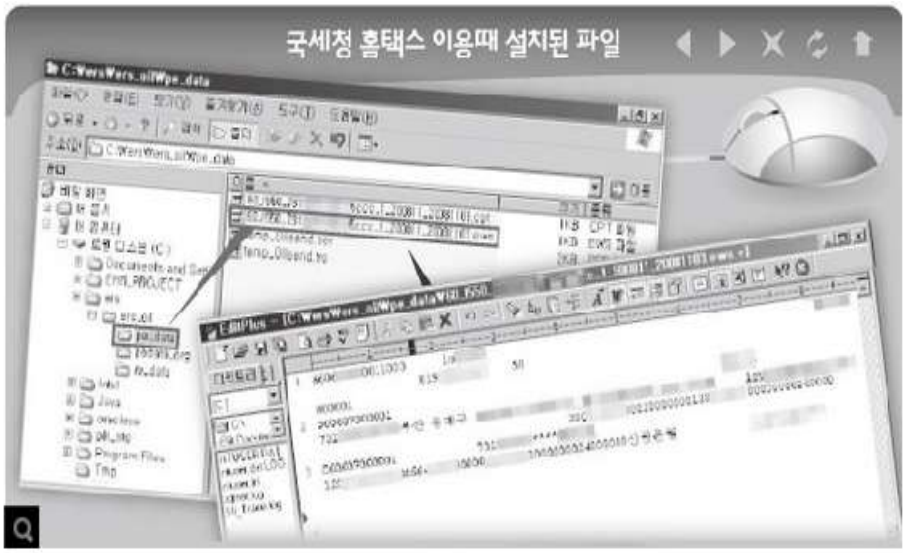
즉, 해당 사이트에 들어가 유가환급금을 신청하면 사용한 컴퓨터의 메인 하드디스크에 'ERS'라는 폴더가 생성되며, 여기에 신청자의 이름, 아이디, 주민등록번호, 주소, 전화번호, 회사명, 은행계좌 등 정보가 자동으로 저장된다.[75]

이 경우 개인 컴퓨터가 아닌 회사나 PC방 등 여러 사람이 함께 이용하는 컴퓨터를 사용하면 개인정보 유출 가능성이 높다.

이는 기술적인 보호 조치 문제로 인하여 개인정보 유출이 발생할 수 있는 대표적인 사례라 할 수 있다.

<그림 7> 국세청 홈텍스 이용때 설치된 파일

75) 보안뉴스, 2008. 11. 10 일자.



출처: 한겨레 신문[76]

나. 암호화 처리 등 보안조치 없이 개인정보 제공

2008년 10월 국회 보건복지가족위원회의 국정감사 자료에 따르면, 국민건강보험공단이 외부 조사기관에 산하 건강보험연구원이 2006~2007년 환자 본인부담금 실태 설문 조사 등을 수행하면서 개인정보유출에 대한 아무런 방책도 없이 가입자들의 개인정보를 넘겨주었다. 건강보험공단은 조사기관에 가입자 개인정보를 최대 150만명의 개인정보를 제공하였기 때문에 모두가 유출됐다고 추정하고 있으나, 정보 제공 과정에서 어느 기관에 어떤 정보를 줬는지에 대한 기록이 전혀 남아있지 않아 유출 건수는 더욱 많다고 한다.

또한 국민건강보험공단은 연구 또는 조사 목적으로 대량의 개인정보를

76) 한겨레 신문, 2008. 11. 11 일자.

외부에 제공할 경우 '개인정보제공 심의위원회' 심의를 거치도록 규정하고 있으나, 연구원측은 가입자 개인정보를 20차례 제공하면서 16번이나 아무런 심의 절차를 거치지 않았다.

20차례 모두 비밀번호, 사용기간 제한 등 정보에 대한 암호화 처리가 이뤄지지 않아 파일 복제에 전면 노출된 상태로 개인정보가 넘겨졌다.

심지어 '전자우편 용량 부족', '시디 라이터 미지급' 등의 이유로 이동식저장장치(USB)에 정보를 담아 인편에 리서치업체에 건네거나 포털사이트 계정 전자메일로 전송, 해킹이나 정보도용 가능성에 노출됐던 경우도 14차례에 달했다.

이와 함께 정보 사용 뒤 제공 자료를 폐기했음을 증명하는 확인서를 받게 돼 있으나 연구원측은 대부분 문서를 받지 않고 구두로 폐기를 지시했다.

이처럼 산하 기관의 가입자 개인정보 보안이 허술했음에도 불구하고 국민건강보험공단은 보건복지가족부가 9월 달에 발표한 '개인정보 보호 우수기관'으로 선정됐다.[77]

만약 "정보를 넘겨받은 외부 조사기관이 악의적으로 국민 개인정보를 유출 · 도용했다면 어떤 결과가 빚어졌을지 모를 것이다.

국민건강보험공단이 취급하는 개인정보는 국민의 병력 등 개인 프라이버시와 관련된 내용이 대다수이기 때문에 특별히 개인정보가 관리가 되어야 한다.

4. 해킹 및 오 · 남용에 의한 개인정보 유출

77) 중앙일보, 2008. 10. 20 일자.

가.「옥션」고객 1,081만명 개인정보 유출

2008년 2월 초 중국인 해커가 옥션 데이터베이스인 고객지원시스템(eNomix)에 저장된 고객의 개인정보를 해킹하여 유출된 사례가 발생하였으며, 또한 개인정보가 유출된 회원의 수가 국민의 1/4인 1,081만 명으로 확인 확인되었다. 옥션 가입자 중 60%의 정보가 빠져나간 것이다. 개인 정보가 유출된 1,081만 명 중 90%에 해당하는 약 900만 명은 이름과 아이디(ID), 주민등록번호(일부 회원은 은행계좌번호가 포함되었다)가 유출되었다. 그러나 다행스럽게도 비밀번호나 신용카드번호는 미유출되었다. 더불어 명의도용, 불법유통, 스팸발송 보이스피싱(전화금융사기) 등 제2의 후속 피해가 우려되기도 한 사건이었다.

이 사건에서 사용된 해킹 프로그램은 기존 안티바이러스 프로그램으로 확인 불가한 악성 변종프로그램이었고, 해외 IP를 사용한 것까지 확인되었다.[78]

이 사례에서 나타난 문제점은 서비스 제공과 무관하게 개인정보를 과다하게 수집하는 관행이 개인정보의 침해에 주요 원인이 되고 있으며,[79] 고객의 개인정보를 마케팅, 업무편의 등을 위한 수단으로 이용하는 반면, 정보보호에 대한 투자 및 경영자의 관심은 부족하였다. 또한 사업자, 단체 등의 자율적 개인정보보호 활동은 미흡한 반면, 정부 규제 및 단속에 대해서만 소극적으로 대응하는 수준이었다.

그리고 해킹에 대한 대응력 부족도 하나의 문제점으로 지적되었다. 개인정보 탈취를 위한 해킹은 네트워크, 사업자 서버, 이용자 PC에서 발생

78) 한국경제신문, 2008. 4. 17 일자; 한겨레 신문, 2008. 4. 17 일자; 동아일보, 2008. 4. 17 일자; 중앙일보, 2008. 4. 17 일자; 조선일보, 2008. 4. 17 일자 참조.

79) 국내 사이트의 73% 이상이 주민등록번호를 수집하고 있다. 그러나 야후, MSN, 아마존 닷컴 등 외국의 주요 사이트는 성명, 이메일, 생년월일 등 기본정보만 수집을 하고 있다. 정방송통신위원회, 전게논문, 4면.

하였는데, 사업자의 정보보호 투자 및 전문가 부족으로 해킹 사실을 조기 인지하지 못하거나 신속한 초동 대응력이 미흡하였다.[80]

이 사건으로 추진되었던 대책으로는 인터넷에 유출된 개인정보가 명의도용, 회원자격 도용에 악용 되는 것을 막기 위하여, 주요 포털사들은 유출 개인정보에 대한 모니터링을 강화하고,[81] 회원자격 도용방지를 위한 비밀번호 변경 캠페인, 인터넷사업자의 휴대폰 등을 이용한 본인확인 절차의 도입도 확대되었다. 또한 스팸과 관련해서 통신사업자의 불법스팸 발송자에 대한 관리 강화 및 대출· 성인· 대리운전 등 3대 악성 스팸에 대한 집중관리도 추진하였다.

인터넷상의 주민등록번호 수집을 제한하는 방안을 정부 등 관계부처와 협의하여 추진하고, 현재 선언적 성격이 강한 개인정보의 필요 최소한의 수집 의무 규정의 실행력 확보를 위해 벌칙을 규정하고, 통신, 인터넷 사업자의 개인정보보호 책임성을 강화하며, 개인정보 해킹에 대한 기술적 대책을 추진하는 등 제도개선을 추진하였다.

나.「하나로텔레콤」고객 600만명 개인정보 무단 제공

2008년 4월 23일 서울경찰청 사이버범죄수사대 초고속신망 업체인 하나로 텔레콤(현 SK브로드밴드)이 2006년 1월부터 2008년 12월 말까지 가입자 600만 명의 개인정보 8500만 건을 제휴업체인 텔레마케팅 회사 1000여 곳에 제공해 이를 상품판매에 이용하도록 했다. 텔레마케팅 업체들은 제공된 고객의 개인정보를 주로 대출, 신용카드 모집, 인터넷·전화 등 통신상품 구입 권유, 바이러스 백신 프로그램 가입 권유 등에 하

80) 정보보호 제품 사용현황을 살펴보면, 침임차단시스템 45.9%, 침임탐지시스템 9.5%, 웹방화벽 18.3%이다. 2008년 국가정보보호백서 참조.
81) 정보보호진흥원(KISA)이 운영중인 1일 1회 모니터링을 4-6회로 확대하였다.

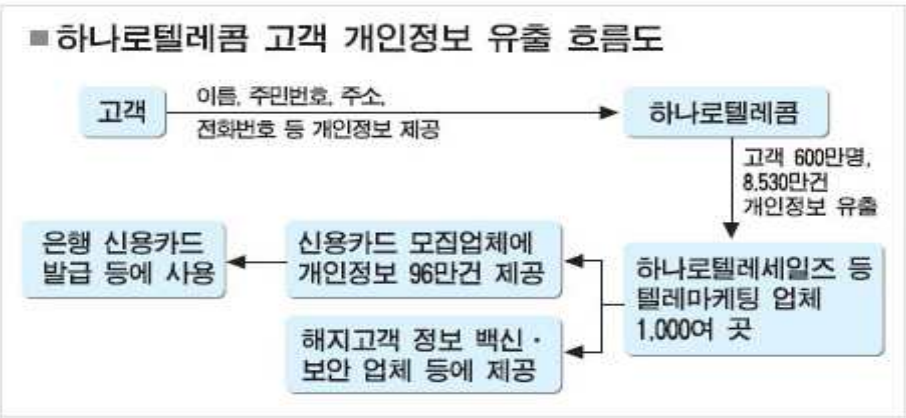
나로텔레콤 고객의 개인정보를 이용하였다. 특히 이 사건의 개인정보 무단 유출은 종전 관리 실수 등에 따른 개인정보 유출과는 달리 회사가 직접적으로 개입하였다는 특징이 있다.

경찰 수사 결과에 의하며, 가입자 본인의 동의도 없었고, 심지어 계약을 해지한 고객들의 개인정보도 계속 사용했으며, 고객정보를 이용하기 위한 마케팅 회사까지 만드는 등 본사 차원에서 조직적으로 하였다.[82]

그 결과 2008년 6월 방통위로부터 40일 간의 영업정지와 1억4800만 원의 과징금 및 30000만 원의 과태료 처분을 받았다.

이 사건은 대기업이 무단으로 가입자 정보를 유용했다는 점에서 충격을 주었으며, 아울러 피해자들 사이에서 보상을 위한 단체소송 분위기가 조성돼, 피해에 소극적이던 태도에서 적극적인 대응태도로 전환하는 계기도 마련되었다.[83]

<그림 8> 하나로 텔레콤 고객 개인정보 유출 흐름도



82) MBC, 20028. 4. 24일 방송
83) 보안뉴스, 2008. 12. 31 일자.

제4장 개인정보 침해 방지와 이에 대한 입법적 대응

제1절 개인정보 침해 대응 방향

앞에서 개인정보 침해 사례에서 보았듯이 현재 우리 정부 및 공공기관, 금융기관에서 유출된 개인정보가 범람하고 있지만, 이를 막으려는 국가적 · 사회적 대책과 노력이 너무 미흡한 것이 현실이다. 오히려 정부와 공공기관이 정보 흘리기에 앞장서는 듯한 인상마저 준다. 사생활(프라이버시)을 존중하고 지켜주려는 인식의 확산이 절실하다.

금융위원회의 국회제출 자료에 따르면, 금융기관들이 2007년 수사기관과 공공기관에 제공한 금융거래정보는 35만7751건에 이른다. 이 가운데 83%인 297,696건은 계좌 명의자의 동의 없이 몰래 넘겼다고 한다. 수사기관의 계좌추적과 내부자거래, 불공정행위 조사 등을 빼고는 사전에 서면동의를 받게 되어 있고 계좌추적에도 법원의 영장이 필요하다. 그럼에도 불구하고 본인 동의 없는 개인정보제공이 해마다 급증하는 추세이다. 즉, 개인정보를 내주는 쪽이나 받는 쪽 모두 금융실명거래 및 비밀보장법에 위반이라는 사실은 인식하지 않는다.

2008년 4월에 있었던 국민건강보험공단의 개인정보 72만 건 유출사건은 사생활 침해의 심각성을 잘 보여준 사례이다. 2002년 이후 전·현직 대통령 등 유명 정치인들과 인기 연예인 등의 개인정보 1만2000여 건이 불법 열람되고 1,800여 건이 유출된 것도 놀라운 일이다. 공단 직원들이 대상자들의 성병 치료 유무나 아파트 위층에 누가 사는지 등 개인적 호

기심을 채우는 데 악용했다고 한다.[84]

이처럼 유출된 개인정보는 명의도용, 스팸, 보이스 피싱 등 제2차 피해 가능성이 높아 국민의 불안감을 확산시키고 고객의 신뢰를 기반으로 하는 인터넷 비즈니스의 기반을 약화시키는 부정적 영향을 확산시키게 되므로 개인정보 침해방지 대책을 수립하여 추진하여야 할 것이다.

우선 이용자의 피해를 최소화하기 위해 인터넷상 유포된 개인정보에 대한 모니터링 강화와 유출된 개인정보를 이용한 인터넷상 명의 도용 방지, 비밀번호 변경 캠페인을 실시하고, 개인정보 침해 대응을 위한 핫라인(Hot-line)을 구축하여 피해구제 활성화 방안을 모색하여야 한다. 특히 통신, 인터넷 사업자의 개인정보보호 책임성 강화를 위해 주민번호 수집금지 방안, 주민번호 대체수단 확산 및 의무화, 주민번호 암호화 저장 및 비밀번호 생성 기준 적용 의무화를 들 수 있다.

또한 개인정보보호 인식제고로는 사업자 단체 윤리강령 제정 등 자율적 개인정보보호 활동을 강화하여 언론, 공익광고 등을 통한 예방요령 전파와 사업자 및 이용자 대상 개인정보보호 교육을 확대시키는 방안을 제시하야야 할 것이다. 이 외에도 개인정보 해킹에 대한 기술적 대책으로 보안서버 보급, 악성코드 탐지 등 네트워크 개인정보보호 강화와 개인정보 유출 종합대응 시스템 구축 등이 있으며, 국내·외 공조체제를 강화하기 위하여 한국정보보호진흥원과 경찰, 검찰 등의 수사기관 그리고 사업자간의 침해신고 대응 핫라인을 구축하고, 해외 개인정보 오·남용 대응을 위한 관계국과의 공조강화 등 지적으로 증가하고 있는 개인정보 유출 및 노출사건에 대한 적극적인 대응방안을 추진해야 한다.[85]

더불어 국민의 사생활을 마구 들여다보는 행태를 불식하기 위한 특단의 대책과 법제도적 시스템 구축이 시급하다.

---

84) 동아일보, 2008. 9. 22 일자.
85) 2009 국가정보보호백서, 전게서, 105면 참조.

제2절 개인정보 침해 방지 대책

1. 개인정보 침해 예방

가. 주민번호 대체수단으로 I-PIN 보급

인터넷 웹사이트에서 주민등록번호의 과도한 수집 · 사용으로 인하여 발생하는 도용 및 침해 문제를 해결하기 위하여 방송통신위원회는 주민번호 대체수단으로 아이핀(i-PIN, Internet Personal Identification Number)을 보급하였다.

행정안전부는 2008년 8월부터 공공 아이핀(i-PIN)을 보급하여, 2009년 11월 현재 약 2,350여개 공공기관 홈페이지에서 서비스를 제공하고 있으며, 2012년도에는 약 5,000여개의 공공기관에서 서비스를 제공할 예정이다.

아이핀이라 함은 인터넷 상에서 주민번호를 대신하여 ID와 패스워드를 이용하여 본인확인을 하는 수단으로써 아이핀 아이디와 패스워드를 이용하면 웹사이트에 더 이상 주민번호를 이용하지 않아도 회원가입 및 기타 서비스 이용이 가능하다.[86]

아이핀은 인터넷에서 주민등록번호를 대신해 신원확인을 할 수 있는 개인 식별번호로 주민등록번호의 유출과 불법적인 명의 도용을 방지하기 위하여 공공기관 웹사이트에는 행전안전부가 민간업체 웹사이트에는 방송통신위원회가 아이핀 콘텐츠를 보급하고 있다.[87]

웹 사이트는 아이핀(i-PIN) 도입을 통해 주민등록번호를 제공하지 않

86) 한국인터넷진흥원, http://www.kisa.or.kr
87) 보안뉴스, 2009. 11. 24일자.

고도 회원가입이 가능한 방법을 이용자에게 제시함으로써 이용자의 선택권을 보장할 수 있고, 또한 인터넷 사업자들은 아이핀(I-PIN)을 도입함으로써 개인정보관리에 대한 부담을 줄이고 본인임이 확인된 이용자의 확보를 통해 내실 있는 회원 데이터베이스를 구축할 수 있다는 장점이 있다. 방송통신위원회는 2006년 10월에 '인터넷상의 주민번호 대체수단 가이드라인'을 통해 아이핀(I-PIN) 서비스를 제공하는 본인 확인기관의 요건과 서비스 안정성 확보를 위한 정기점검 방안 등을 확정하여 발표하였다. 이러한 아이핀(I-PIN) 서비스 안전성을 바탕으로 2008년에는 총 190개 기관이 도입하였으며, 63만 여건의 I-PIN이 발급되었다. 특히, 2008년 6월 13일에는 이용자의 개인정보 자기통제권을 강화하기 위하여 인터넷 사이트 회원가입시 주민등록번호 대신 대체수단으로도 가입할 수 있는 방법을 제공하도록 하는 정보통신망 이용촉진 및 정보보호 등에관한 법률의 개정안[88]이 통과되었다.[89]

따라서 2009년부터는 I-PIN 등 주민등록번호 대체수단의 활성화되었으며, 그 대표적인 사례로 주민등록증이 없는 초·중·고 학생의 공공 아이핀(I-PIN) 회원가입이 쉬워졌는데, 행정안전부는 초·중·고 학생에 대한 공공 아이핀(I-PIN) 발급절차를 간소화하고 노약자 등을 위한 콘텐츠를 확대하는 등 공공 아이핀(I-PIN) 기능을 대폭 개선해 11월 23일부터 서비스하고 있다. 그동안 초·중·고 학생은 공인인증서나 주민등록증 등 신원확인 수단이 없어 공공 아이핀(I-PIN)을 사용하려면 보호자와 읍·면·동사무소(자치센터)를 방문해야 하는 불편이 있었다. 아울러 글자크기 확대/축소 기능, 음성안내 기능 등 노약자, 시각장애인 등을 위한 웹 접근성 콘텐츠도 대폭 개선하여 취약계층이 공공 아이핀 이용시 불편이 없도록 했으며, 영어 외에도 중국어, 일본어용 콘텐츠를 추

88) 정보통신망 이용촉진 및 정보보호등에 관한 법률 [법률 제9119호, 2008. 6. 13, 일부개정, 2008. 12. 14 시행].
89) 2009 국가정보보호백서, 전게서, 109면 참조.

가 제작하여 국내에 거주하는 중국, 일본인 등도 공공 아이핀(I-PIN)을 쉽게 이용할 수 있게 되었다.[90]

또한 주민등록번호를 요구하는 법 · 제도적, 사회적 인프라를 검토하여 민간분야에서 주민등록번호를 가급적 제한하고, 대체수단으로 사용하기 위해 법제도적 개선방안과 사회적 인식제고를 위해 노력해야 할 것이다.

나. 개인정보보호를 위한 보안서버 확대

보안서버는 인터넷 상에서 주민등록번호, ID, 비밀번호 등 개인정보를 암호화하여 안전하게 전송하는 서버로서 중간자 공격 등에 따른 개인정보 유출사고를 막을 수 있는 웹사이트에서는 기초적으로 갖추어야 할 개인정보보호 수단이다. 현행 정보통신망법에서도 개인정보를 수집하는 사업자의 보안서버의 구축이 의무화돼 있고, 미 이행 시에는 과징금이 부과가 규정돼 있다. 하지만 이러한 규제에도 불구하고, 보안서버 구축에 따른 비용과 더불어 보안서버 구축에 대한 기술적 지원 문제로 영세 중소기업은 보안서버를 외면해 온 것이 사실이다.[91]

보안서버는 별도의 하드웨어 장치가 아니라 기존에 운영중인 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하거나 별도의 암호화 기능을 추가하는 소프트웨어적인 방식으로 구축된다. 2006년 9월 국무회의에 '개인정보보호 강화를 위한 보안서버 보급확대 방안'을 보고하여 민간부문을 포함한 범부처적인 보안서버 확산기반을 조성하였다.

이후 보안서버 보급확대를 위하여 2006년 10월부터 3개월에 걸쳐 국가기관, 지자체 및 민간 주요 웹사이트 19,584개의 담당자를 대상으로 안

90) 디지털타임스, 2009. 11. 24 일자.
91) DATANET, 2009. 8. 5 일자.

내메일을 발송하고 전화 상담을 실시하였다. 12월에는 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의한 '개인정보의 기술적 · 관리적 보호조치 기준'에 개인정보 송 · 수신시 보안서버 구축 등을 명기한 개정안을 마련했다. 또한 2007년 10월에는 보안서버 구축에 대한 이해를 돕기 위하여 '보안서버 구축 가이드'를 발간하였다. 그래서 2007년에는 민간부분에 총 17,966개의 보안 서버를 구축했으며, 이를 위해 한국정보보호원에서는 상장사 및 일일 방문자수 1만명 이상 2,243개 주요 웹사이트를 중점 관리 대상으로 선정하였다. 선정된 사업자 중 보안서버 미구축 사이트에 대해서는 개선권고 및 전화계도를 실시했으며, 일일 방문자 수 기준으로 15,000개 웹사이트를 선정하여 보안서버 구축 실태를 점검하고 미구축 사이트를 대상으로 계도활동을 수행하였다.

2008년에는 민간부문 25,000여개 웹사이트를 대상으로 실태점검 및 계도활동을 수행하여 지속적으로 보안서버 구축을 독려하였으며, 웹사이트 개발단계에서 보안서버 구축을 유도할 수 있는 사전점검체계 구축방안을 만들어 웹사이트 개발사 및 개발자를 대상으로 한 교육 및 홍보활동을 수행하였다.[92]

다. CCTV 및 위치정보 등 개인정보보호 강화

현재 신규 IT 서비스가 지속적으로 도입됨에 따라 서비스 도입 전 · 후에 개인정보 침해 여부를 파악하여 개선하는 것이 중요해지고 있다. 2007년에 수행한 신규 IT 서비스 관련 프라이버시 보호대책은 RFID 프라이버시 보호, 바이오 정보보호, 개인영상 정보보호(CCTV, Closed Circuit Television),[93] 개인위치 정보보호에서 이루어졌다. 2007년 이 분야들

92) 2009 국가정보보호백서, 전게서, 110면 참조.
93) 특정한 수신자만 서비스하는 것을 목적으로 하는 텔레비전 전송시스템으로서, 일반적으로 원

과 관련된 활동의 자율규제를 지원하고 사업자의 보호 역량을 강화하는 방향을 진행되었는데, 우선 기존에 마련해 놓은 가이드라인을 개정(RFID, 바이오정보, 개인영상정보)하고, 해설서를 제작하였다. 또한 가이드라인 준수 여부를 사업자가 자율적으로 점검할 수 있는 체크리스트도 개발 및 보급하였다. 그리고 RFID, 바이오정보, 개인위치정보에 대한 이용기관 및 이용자를 대상으로 개인정보보호 의식 및 이용 실태 등을 실시하였다. 이에 대한 실태조사 결과는 향후 정책 방향 수립을 위한 참고자료로 활용할 것이며, 이 외에 개인 위치정보 분야에서는 위치정보사업자 대상 허가심사 및 위치정보심의 위원회를 운영하였다.

2008년 3월에 발생한 안양 어린이 유괴살인 사건을 계기로 아동, 부녀자 납치, 실종사건 등에의 신속한 긴급구조와 대응을 위한 위치정보를 이용해야 한다는 사회적 요구가 증가하여, 이에 경찰에 위치정보제공 요청권을 부여하고, 개인위치정보의 제3자 제공시 즉시 통보하는 방법을 합리화 하는 등 신속한 긴급구조 대응에 불필요한 규제를 완화하였다. 더불어 긴급구조를 위한 정확한 위치정보 제공을 위해 휴대전화에 GPS 장착을 의무화하는 방안 등 위치정확도 향상을 위한 제도 개선 방안을 마련하였다. 이와함께 이용자의 개인위치정보 보호를 위해 보호조치 수준이 마련된 사업자에 한해서 위치정보 사업을 영위토록 허가하였으며, 정기적으로 사업자에게 개인위치정보보호에 대한 교육을 실시하여 위치정보에 대한 관리 및 기술적 보호조치를 개선토록 하였다.[94]

어를 그대로 번역하여 폐쇄회로텔레비전이라는 용어로도 쓰인다. 교육, 의료 및 지역 정보서비스 등 산업분야 전반에 이용되고 있는 CCTV는 송신측에서 수신측까지 유선 또는 무선 전송로를 이용하므로 일반인은 마음대로 수신할 수 없으며, 산업용 텔레비전(ITV) 또는 전용 텔레비전이라고도 한다. 촬영자 없이 영상 포착에 의미를 두어 무인감시카메라로 통용되고 있으나, 화상통신용어로는 CCTV라 칭함이 적절하다. 정보통신부, CCTV 개인영상정보보호 가이드라인해설서, 한국정보보호진흥원(KISA)·정보통신부(MIC), 2006. 10, 6면 참조.

94) 2009 국가정보보호백서, 전게서, 110-111면 참조.

라. 개인정보보호 교육 및 홍보 강화

2008년 4월부터 12월까지 한국정보문화진흥원(KADO)의 지원을 받아 수도권의 231개의 초 · 중 · 고교, 125,833명의 학생, 학부모, 교직원 등을 대상으로 개인정보보호 기본교육을 실시하였는데, 교육은 개인정보에 대한 이해와 피해 예방을 목적으로 진행되었다.

올해 2009년도에는 개인정보영향평가 전문교육의 경우 총 3회에 걸쳐 개인정보보호 관련 법 · 제도, 보호조치, 영향평가 방법론 및 실습 등 관련 교육을 실시하였다. 또한 개인정보보호조치 미구축 사업자 200여명을 대상으로 하여 개인정보보호 조치 구축 지원을 위한 개인정보보호 교육과 사업자 홈페이지 관리자 페이지 노출업체, 홈페이지 제작업체를 대상으로 개인정보보호 교육을 실시하였다.

개인정보보호를 위한 10계명[95] 리플렛을 제작하여 수도권 외 5개지역 100여개 학교에 '2008년 건전정보문화 캠페인' 행사시에 배포를 하였으며, 지하철 신문에 개인정보보호 10계명을 게제하는 등 개인정보보호를 위하여 활발한 홍보를 실시하였다.

---

95) 개인정보 오남용 피해 예방 10계명. 제1계명: 회원가입을 하거나 개인정보를 제공할 때에는 개인정보취급방침 및 약관을 꼼꼼히 살핀다(개인정보취급방침이 없는 사이트는 가입하지 않는다). 제2계명: 회원가입 시 비밀번호를 타인이 유추하기 어렵도록 영문/숫자 및 특수문자를 조합하여 8자리 이상으로 설정한다. 제3계명: 가급적 안전성이 높은 주민번호 대체수단(아이핀: i-PIN)으로 회원가입을 하고, 꼭 필요하지 않은 개인정보는 입력하지 않는다. 제4계명: 자신이 가입한 사이트에 타인이 자신인 것처럼 로그인하기 어렵도록 비밀번호를 주기적으로 변경한다. 제5계명: 타인이 자신의 명의로 신규 회원가입 시 즉각 차단하고, 이를 통지받을 수 있도록 명의도용확인서비스를 이용한다. 제6계명:자신의 아이디와 비밀번호, 주민번호 등 개인정보가 공개되지 않도록 주의하여 관리하며 친구나 다른 사람에게 알려주지 않는다. 제7계명: 인터넷에 올리는 데이터에 개인정보가 포함되지 않도록 하며, P2P 로 제공하는 자신의 공유폴더에 개인정보 파일이 저장 되지 않도록 한다. 제8계명: 금융거래 시 신용카드 번호와 같은 금융정보 등은 암호화하여 저장하고, PC 방 등 개방환경을 이용하지 않는다. 제9계명: 인터넷에서 아무 자료나 함부로 다운로드 하지 않는다. 제10계명: 개인정보가 유출된 경우 해당 사이트 관리자에게 삭제를 요청하고, 처리되지 않는 경우 즉시 개인정보침해신고센터에 신고한다. 방송통신위원회, 전게논문, 14면 참조.

또한 개인정보취급자를 대상으로 개인정보보호전문교육을 사업자를 대상으로 하여 순회교육을 실시하고, 더불어 준용사업자 각 협회의 워크샵 및 각종 행사시에 개인정보보호 강사를 지원하였다.[96]

이처럼 개인정보보호의 예방을 위하여 지속적인 교육 및 홍보를 강화하는 것이 개인정보 침해 방지를 위한 또 다른 대책이라 할 것이다.

2. 개인정보 침해 대응 방안

가. 인터넷상 노출된 주민번호의 삭제

인터넷상에 주민등록번호가 노출되는 원인은 이용자가 고객 상담 게시판 등에 ID나 패스워드 분실 문의를 하면서 본인임을 입증하기 위하여 스스로 주민등록번호를 기재하는 경우 등 이용자의 개인정보보호 인식 부족에 의한 경우와 웹사이트 운영자 또는 해당 기관 종사자 등이 웹사이트에 파일 등의 자료를 올려놓거나 글을 게시하면서 공개하지 말아야 할 개인정보를 올려놓는 경우, 그리고 웹사이트 운영자가 기본적인 보안 사항을 적용하지 않거나 실패하여 검색엔진이 인증 없이도 관리자 페이지에 접근하여 개인정보를 가져가는 경우가 많은 것으로 조사되었다.

인터넷 웹페이지에 노출된 주민등록번호를 조기에 탐지 및 삭제하기 위하여 정보보호진흥원은 2007년 7월부터 ‘구글 검색 데이터베이스 주민등록번호 노출 상시 점검 체계’를 도입하여 매 근무일로 점검을 하고 있다. 2008년 상반기부터는 공공기관의 개인정보 노출이 사회적으로 문제가 됨에 따라 노출된 개인정보 삭제 요청을 이메일로 자동 발송할 수 있는 시스템을 개발하여 인력증원 요인을 해소하였다.[97]

---

96) 2009 국가정보보호백서, 전게서, 111-112면 참조.

2008년에 이어 2009년에도 인터넷상에서의 개인정보 누출은 지속적으로 나타났으며, 2010년에도 개인정보의 누출은 지속적으로 나타날 것이라 예상된다. 따라서 이를 방지하기 위한 다각적인 노출 원인 분석 및 대응 기술 개발, 사업자의 예방 교육, 관련 유관기관과의 지속적인 협력 구축체계가 필요하다. 이와 함께 개인정보보호에 대한 인식제고를 위한 지속적인 교육과 홍보도 병행해야 할 것이라 생각한다.

나. 개인정보 침해에 따른 대응체계 구축

현재의 국내 주민등록번호 노출 및 유출점검을 위해 기존의 노출 및 유출 점검 시스템은 구글에 노출된 주민등록번호만을 점검하여 사회적 요구에 부합하고, 국가차원의 대응 전략을 위해 개인정보 유출, 노출에 대한 종합적인 대응시스템 구축을 추진하기 시작하였다. 사전예방을 위한 개인정보 유출 공격 탐지, 공격 유형 종합 수집 · 분석, 위험성 평가 및 전파 기능을 구축하고 신속한 대응체제를 위해 웹사이트의 직접점검 시스템, 포털 데이터베이스 연계 검색 시스템, 유관기관과의 연락체계 구축, 현황 모리터링 및 통보 시스템을 구축 중에 있다.[98]

이러한 개인정보 침해에 따른 대응체제 시스템들이 조속한 시일안에 구축되어 지속적으로 증가하는 개인정보 침해 방지해야 할 것이다.

다. 개인정보 침해 실태 점검 및 법집행력 강화

2007년부터 2008년까지 최근 2년간 총 60건의 개인정보보호 현장 점

97) 2009 국가정보보호백서, 전게서, 112-113면 참조.
98) 2009 국가정보보호백서, 전게서, 113면 참조.

검을 실시했다.

주요 조사 내용은 초고속 인터넷, 게임, 포털, 대입원서 접수대행 실태점검, 백화점 등 유통업체의 무선랜 암호화 조치 현황 조사, 초고속통신사업자 해지고객 정보 남용 현장점검, 대형할인점 개인정보실태 현장점검 등 총 25개 정보통신서비스 제공자 25개회사와 준용사업자 35개 회사에 대하여 개인정보 침해 실태를 점검하였다. 또한 2008년도는 26,000개 웹사이트를 대상으로 개인정보 수집 여부 및 법규 준수율을 조사했는데, 조사 결과 전체의 약 85%인 22,216개의 웹사이트가 개인정보를 수집하고 있는 것으로 나타났다.

최근 4년간 개인정보 수집현황을 비교했을 때, 2008년도 조사 결과가 가장 높은 통계를 나타내고 있으며, 개인정보를 수집하고 있는 웹사이트 중 정보통신망법 제22조 제2항의 규정에 의한 고지의무를 준수하고 있는 사업자 비율은 2%로 약 431개 였다.

개인정보보호 법집행력 강화를 위해 정보통신망법 개정안이 국회에 제출되어진 이후 2008년 12월 개정된 정보통신망법이 시행되면서 개인정보보호가 강화되고 있다. 개인정보보호의 위반 행위자에 대한 과징금 부과 및 과태료의 형사처벌화, 사경권 도입 등 제재수단을 강화하여 법규의 실효성을 확보하고 있다. 또한 동의를 받지 않은 개인정보 수집, 영업양도 등에 따른 통지 없는 개인정보 이전 행위 등 위법성이 큰 행위에 대해 현행 과태료에서 형사처벌 대상으로 상향 조정함으로써 이용자의 권익 침해에 대한 제재를 강화하였다.[99] 이는 법 집행력 강화를 통하여 개인정보 침해에 대한 적극적인 대응 방안을 구체화 하였다고 볼 수 있다.

99) 2009 국가정보보호백서, 전게서, 113-114면 참조.

제3절 개인정보보호에 관한 입법적 대응

1. 개인정보보호법 추진 배경 및 과정

우리 정부는 개인정보의 유출 및 오·남용 근절을 통해 안전하고 신뢰받는 정보사회를 구현하기 위하여 공공· 민간을 포괄하는「개인정보보호법」제정(안)을 마련하고, 2008년 8월 12일에 입법예고 하였다.

최근 대규모 개인정보 유출이나 크고 작은 개인정보 오· 남용 사례가 빈번하게 발생하여 국민적 불안이 가중되고 있으나, 공공기관과 정보통신사업자 등 일부만을 규율하는 현행법 체계 하에서는 국가사회 전반의 개인정보보호 수준을 대폭 강화하는 근본적 문제 해결이 어렵다는 지적이 많았었다. 이에, 정부는 그간 국회, 시민단체 등에서 지속적으로 요구해 온 바 있는「개인정보보호법」을 제정하여, 공공·민간의 모든 영역에 적용되는 개인정보 수집에서 파기까지의 단계별 처리원칙을 제시하는 한편, 주민등록번호 등 개인식별번호의 수집·이용 제한, CCTV 개인영상정보보호, 개인정보 유출사실의 통지제도, 개인정보분쟁조정위원회 등 개인정보의 실질적 보호와 국민의 사후 권리 구제 강화를 위한 제도적 장치를 도입키로 하였다.

개인정보보호법 입법 추진과정을 살펴보면, 2008년 3월 행정안전부·학계· 전문기관을 중심으로 “개인정보보호법제정TF” 팀을 구성하여, 11차례 TF 논의를 통하여 전문가의 의견을 수렴하고 쟁점을 정리하였다. 그 후 동년 6월 27일과 8월28일 2회에 걸쳐 개인정보보호법 제정을 위한 공청회를 개최하여 개인정보 추진체계, 개인정보보호와 이용의 조화방안, 주민등록번호 수집제한 등 주요 이슈에 대하여 활발한 토론과 의견교환한 후 2008년 7.24 ~ 9.21 관계부처간에 의견조회· 협의를 거쳐, 입법예고를 하였다. 9월 이후에는 규제개혁위회회의 심사를 완료하고,

법제처 심사를 거쳐 국회에 제출하였다.

2009년 2월 20일 행정안전위원회에 상정 및 법안심사소위원회에 상정하였다. 그 후 2009년 4월 23일 개인정보보호법 공청회를 실시하였다.

이미 17대 국회에서 여야 의원들에 의하여 무려 5개의 개인정보보호법안이 발의되었을 만큼 개인정보감독기구의 설치와 개인정보보호법의 제정은 국민적 공감대를 형성하고 있다.

그러나 현재까지 개인정보보호법은 그 중요성에 걸맞지 않게 아직도 국회 처리가 너무 지연된 측면이 있다. 이 법안의 중요성을 인식한다면, 조속한 시일안에 처리되어야 할 것이다.

2. 개인정보보호법 제정 이유

현재 정보사회의 고도화, 정보통신기기의 보급 확대, 전자정부의 추진 등과 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용, 처리가 보편화되고 있으나, 현행 개인정보보호 관련 법률은 공공행정, 정보통신, 신용 등 특정 분야에 한정되어 있어 사회 전반에 걸쳐 광범위하게 수집·처리되고 있는 다양한 형태의 개인정보를 적절히 보호하지 못하고 있는 것이 현실이다. 이처럼 국가사회 전반을 규율하는 개인정보 보호원칙과[100] 개인정보 처리기준이 마련되지 못해 개인정보 보호의 사각지대가 발생할 뿐만 아니라, 최근 개인정보의 유출·오

100) OECD 개인정보보호 8원칙

○ 수집제한의 원칙(제1원칙)	○ 정보의 질 확보의 원칙(제2원칙)
○ 목적 명시의 원칙(제3원칙)	○ 이용제한의 원칙(제4원칙)
○ 안전성 확보의 원칙(제5원칙)	○ 공개의 원칙(제6원칙)
○ 개인참여의 원칙(제7원칙)	○ 책임의 원칙(제8원칙)

용·남용 등 개인정보 침해 사례가 지속적으로 발생함에 따라 국민의 프라이버시 침해는 물론 명의도용, 전화사기 등 정신적·금전적 피해를 초래하고 있다.[101]

<표 5> 2008년도 국가간 정보보호 수준 비교

순위	국가명	순위	국가명
1	아이슬란드	11	Malta
2	미국	12	스웨덴
3	캐나다	13	네델란드
4	오스트레일리아	14	노르웨이
5	뉴질랜드	15	핀란드
6	룩셈부르크	16	독일
7	스위스	17	싱가포르
8	영국	18	일본
9	덴마크	19	오스트리아
10	아일랜드	**51**	**한국**

*** 출처 : 행정안전부**

특히, 최근에는 이 같은 제도적 결함을 악용하여 국내·외 범죄 집단들이 해킹, 피싱 등 갖가지 불법적인 방법으로 개인정보를 수집하여 암시장을 통해 국내 기업이나 개인들에게 되파는 먹이사슬까지 생겨나고 있어 국민들의 사생활 안전이 위협받고 있으며 막대한 경제적 피해까지 우려되고 있는 상황이다. 따라서 사회 각 분야의 개인정보처리에 대하여 공통적으로 적용될 수 있는 원칙과 기준의 제시가 시급하다.

오늘날 개인정보보호는 국제사회의 공통적 가치와 관심사가 되고 있다. 이미 국제연합(UN), 경제협력개발기구(OECD), 아시아·태평양경제협의체(APEC), 국제노동기구(ILO) 등이 개인정보의 적절한 보호와 합리적 이용을 보장하기 위한 원칙들을 제시한 바 있다. 이들 국제규범은 강제력은 없지만, 개인정보의 보호 및 이용에 관한 현대사회의 보편적 기준

101) 2008년도 국가간 정보보호 수준 비교(행정안전부)

이 되고 있다. 특히 이들 국제규범은 개인정보의 보호뿐만 아니라 합리적 이용권도 보장되어야 함을 강조하고 있어 이에 따라 국제적인 흐름에 맞추어 개인정보의 보호와 활용을 조화롭게 이끌어갈 수 있는 종합적인 개인정보보호법을 제정해야 한다는 사회적 요구가 증대되고 있어 사회 각계각층의 의견을 수렴하여 이에 부합하는 「개인정보보호법」을 제정하고자 하며, 특히 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화하여 국민의 사생활의 비밀을 보호하며, 개인정보에 대한 권리와 이익을 보장하고 동시에 개인정보의 적정한 활용을 보장함으로써 정보사회의 균형적인 발전에 이바지하고자 하는 것이 개인정보보호법 제정의 주된 이유이다.

물론 공공부문과 민간부문을 포괄하는 개인정보보호시스템의 원리가 다르다는 점은 유의해야 할 것이다.[102]

3. 개인정보보호법의 주요내용

최근 행정안전부에서 입법예고한 「개인정보보호법」 제정(안)의 주요 골자는 다음과 같다.[103]

첫째, 법 적용 대상을 공공·민간의 모든 개인정보처리자로 확대하여 개인정보보호 사각지대를 해소하고자 하였다. 특히 국회·법원 등 헌법기관, 동창회·친목회 등 비영리단체를 포함, 업무상 개인정보파일을 운용하기 위하여 개인정보를 처리하는 모든 자에 대하여 법률을 적용하고, 전자적으로 처리되는 문서 이외에 행정서식, 가입신청서 등 수기문서까

102) 趙泰濟, 「公共情報의 作成및 取得段階에서의 制度改善方案」, 인터넷법률 통권 제16호, 2003. 3, 46면.
103) 2009년 행정안전부에서 입법예고한 「개인정보보호법」 제정(안)을 참고하였다.

지 보호범위에 포함하였다.

둘째, 개인정보의 수집·이용·제공 등 단계별 보호기준을 강화하였다. 정보주체의 동의, 법률의 규정이 있는 경우 등 일정 기준에 해당하는 경우 수집·이용·제공을 허용하고, 동의를 얻는 경우 정보주체에게 수집·이용 목적, 이용기간 등을 반드시 알리도록 하였다. 또한, 수집·이용 목적 달성 등으로 불필요하게 된 때에는 지체 없이 개인정보를 파기하도록 규정하였다. 특히, 정보주체의 개인정보 제공 여부에 대한 선택권을 실질적으로 보장하기 위하여 필수 동의 사항과 선택 동의 사항을 반드시 구분하여 동의를 얻도록 하는 한편, 이용자가 원치 않는 마케팅 목적의 활용을 금지하기 위하여 마케팅 목적으로 개인정보를 수집·이용하고자 하는 경우 정보주체에게 이를 명확히 알리고 동의를 얻도록 하였다.

셋째, 주민등록번호 등 고유식별정보에 대한 보호를 강화했다. 주민등록번호 등 고유식별번호의 오·남용, 도용 근절을 위해 고유식별번호 처리를 원칙적으로 금지하고, 정보주체의 별도의 동의나 법령 규정이 있는 경우 예외적으로 사용할 수 있도록 하였다. 또한, 공공기관 등 일정 기준 이상의 개인정보처리자에게는 인터넷 웹사이트 회원가입 등 본인확인이 필요한 경우 주민등록번호 이외의 방법(I-PIN, 공인인증서 등)을 반드시 제공하도록 의무화하였다.

넷째, 개인정보파일등록제, 개인정보영향평가제 도입 등 공공부문의 개인정보관리를 강화하였다. 공공기관에서 처리하는 개인정보파일 현황을 투명하게 관리하고 공개하기 위하여 '개인정보파일 등록 및 공개제도'를 도입하고, 대규모 개인정보파일을 구축하거나 연계·연동하는 경우 개인정보 침해 위험성과 보호대책을 미리 평가하여 취약점을 개선하는 개인정보영향평가를 실시하도록 의무화하였다.

특히, 민간부문에 비해 상대적으로 낮았던 공공부문의 개인정보 유출, 무단열람 등 불법 행위에 대한 처벌 수위를 대폭 높이고(현행 3년이하

징역 → 5년이하 징역), 명백한 위법사항에 대해서는 징계권고, 시정명령, 형사 고발, 위반사실 공표 등을 통하여 실효성 있는 제재가 가능하도록 근거를 마련하였다.

다섯째, CCTV 개인영상정보보호를 위한 법적 근거를 마련하였다. CCTV, 네트워크 카메라 등 영상정보처리기기는 범죄예방, 화재예방, 시설안전, 교통단속 등 법령에서 정하는 목적으로만 설치·운영토록 하고, 안내판을 설치하여 정보주체에게 운영 사실을 알리고, 수집한 개인영상정보 유출 방지를 위한 보호조치를 의무화하였다.

여섯째, 개인정보 침해에 따른 국민의 신속한 권리 구제를 위하여 개인정보 유출사실 통지제도를 도입하였다. 개인정보 유출이 발생한 경우 개인정보처리자가 유출된 개인정보의 항목, 유출 발생 경위 및 시점, 피해 최소화를 위한 방법 등을 지체 없이 통지토록 의무화하여, 정보주체가 신속히 대처하고 피해확산을 방지할 수 있도록 하였다.

일곱째, 개인정보보호정책의 객관성과 전문성을 확보하고, 피해 구제의 독립성을 확보하기 위한 추진체계를 마련하였다.

국무총리실 산하에 개인정보보호위원회(민간인 위원장)을 구성하여 개인정보보호 기본계획, 개인정보보호 관련 정책·제도 개선에 관한 의견제시, 공공기관의 개인정보 이용·제공에 관한 사항 등에 관한 사항을 심의하도록 하고, 현재 민간영역에서 이용자·사업자 간 분쟁조정을 위해서 운영되어 오던 '개인정보분쟁조정위회(민간인 위원장)'를 공공·민간의 모든 개인정보 분쟁을 조정할 수 있도록 대상을 확대하는 한편, 금전적 손해 배상에 대한 합의뿐만 아니라, 침해행위의 중지, 재발방지를 위한 조치 등을 권고할 수 있도록 하였다.

앞으로 정부는 입법예고 기간 중 전문가, 일반국민, 산업계 등의 의견을 적극 검토·반영하여 개인정보의 엄격한 보호와 안전한 이용을 담보

하는 법안을 마련하여 조속한 시일안에 제정코자 하였다.

4. 개인정보보호법의 법안 체계 및 주요 조항

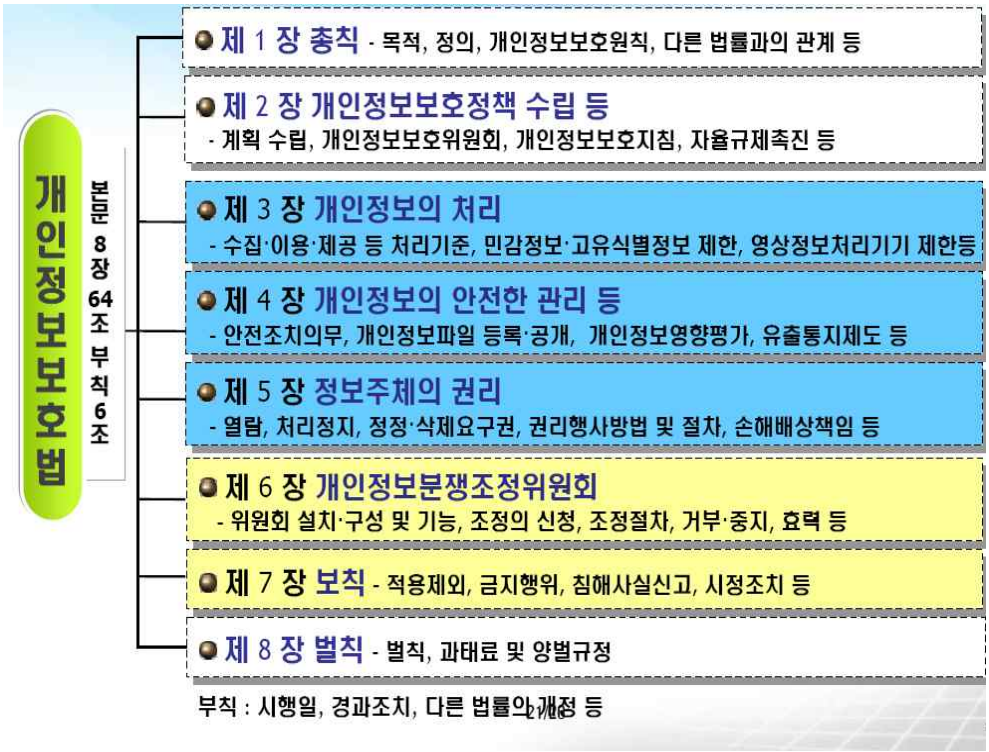
개인정보보호법안 체계는 본문 8장 64조 부칙 6조로 구성되어 있다. 제1장은 총칙으로서 목적, 정의, 개인정보보호원칙, 다른 법률과의 관계 등을 정의하고 있다. 제2장은 개인정보보호정책의 수립으로서 계획을 수립, 개인정보보호위원회, 개인정보보호지침, 자율규제촉진 등을 규정하고,[104] 제3장에서는 개인정보의 처리 부문으로 수집 · 이용 · 제공 등 처리기준, 민감정보, 고유식별정보의 제한, 영상정보처리기기 제한 등을 규정하고 있다. 제4장에서는 개인정보의 안전한 관리 등으로 안전조치 의무, 개인정보파일 등록 및 공개, 개인정보영향평가, 유출통제 제도를 규정하고, 제5장에서는 정보주체의 권리부문으로 개인정보 열람, 처리정지, 정정 및 삭제요구권, 권리행사방법 및 절차 그리고 손해배상책임 등을 규정하였다. 제6장에서는 개인정보분쟁조정위원회에 관한 부문으로 위원회의 설치, 구성 및 기능과 조정의 신청, 조정절차, 거부 · 중지, 효력을 규정하고 제7장에서는 적용제외, 금지행위, 침해사실신고, 시정조치 등의 보칙을 규정하고 있다. 마지막으로 제8장에서는 벌칙에 규정으로 벌칙과 과태료 및 양벌규정을 규정하였다.

이러한 개인정보보호법의 체계는 다음 표와 같고, 이하에서는 개인정보보호법안의 주요 조항에 대하여 살펴보고자 한다.

---

104) 주요 외국의 경우 대부분 개인정보보호에 대한 자율규제시스템이 정착되어 있어 개인정보보호의 규율방식이 Opt-out 방식(정보 수집은 자유롭게 하되, 정보주체에게 고지한 후 정보주체가 사후에 거부할 수 있도록 하는 방식)으로 되어 있으나, 우리의 경우 개인정보보호에 대한 사회적 인식 수준 및 일천한 역사 등을 감안하여 Opt-in 방식(정보주체가 사전에 동의한 경우 정보수집이 가능하도록 하는 방식)을 취하고 있다. 국회행정안전위원회,「개인정보보호법안 」에 대한 공청회 자료집, 행정안전부, 2009. 4. 23, 234면.

<그림 9> 개인정보보호법(안) 체계



* 출처: 행정안전부

개인정보보호법안의 주요 조항을 살펴보면 다음과 같다.

① 개인정보 보호법안의 적용대상을 공공·민간부문의 모든 개인정보처리자로 하였다(안 제2조). 공공기관 뿐만 아니라 비영리단체 등 업무상 개인정보파일을 운용하기 위하여 개인정보를 처리하는 자는 모두 이 법에 따른 개인정보 보호규정을 준수하도록 하고, 전자적으로 처리되는 개인정보 외에 수기(手記) 문서까지 개인정보의 보호범위에 포함하였다.

그 동안 개인정보 보호 관련 법률 적용을 받지 않았던 사각지대를 해

소함으로써 국가사회 전반의 개인정보 보호수준이 제고될 것으로 기대된다.

② 개인정보 보호위원회 설치(안 제9조 및 제10조)조항으로 개인정보 보호 기본계획, 법령 및 제도 개선 등 개인정보에 관한 주요 사항을 심의하기 위하여 국무총리 소속으로 개인정보 보호위원회를 두었다.

이는 개인정보 보호와 관련한 중요 사항에 대하여 의사결정의 신중성・전문성・객관성을 확보할 것이다.

③ 개인정보의 수집, 이용, 제공 등 단계별 보호기준 마련(안 제15조부터 제20조까지)하였다.

개인정보를 수집, 이용하거나 제3자에게 제공할 경우에는 정보주체의 동의 등을 얻도록 하고, 개인정보의 수집・이용 목적의 달성 등으로 불필요하게 된 때에는 지체 없이 개인정보를 파기하도록 하였다. 다시말해, 개인정보의 수집, 이용, 제공, 파기에 이르는 각 단계별로 개인정보 처리자가 준수하여야 할 처리기준을 구체적으로 규정함으로써 법규의 실효성이 높아지고 개인정보의 안전한 처리가 가능해질 것이다.

④ 고유식별정보의 처리제한 강화(안 제23조)하였다. 주민등록번호 등 법령에 의하여 개인을 고유하게 구별하기 위해 부여된 고유식별정보는 원칙적으로 처리를 금지하고, 별도의 동의를 얻거나 법령에 의한 경우 등에 한하여 제한적으로 예외를 인정하는 한편, 대통령령으로 정하는 개인정보 처리자는 홈페이지 회원가입 등 일정한 경우 주민등록번호 외의 방법을 반드시 제공하도록 의무화하였다. 주민등록번호의 광범위한 사용 관행을 제한함으로써 주민등록번호 오・남용을 방지하고, 고유식별정보에 대한 보호가 한층 강화될 것이다.

⑤ 영상정보처리기기의 설치제한 근거마련(안 제24조)하였는데, 앞으로 영상정보처리기기 운영자는 일반적으로 공개된 장소에 범죄예방 등

특정 목적으로만 영상정보처리기기를 설치할 수 있도록 하였다.

영상정보처리기기의 설치·운영 근거를 구체화함으로써, 폐쇄회로 텔레비전(CCTV) 등 영상정보처리기기의 무분별한 설치를 방지하여 개인영상정보 보호를 강화할 수 있을 것이다.

⑥ 개인정보 영향평가제도 도입(안 제31조)하였다. 개인정보처리자는 개인정보 파일의 구축·확대 등이 개인정보 보호에 영향을 미칠 우려가 크다고 판단될 경우 자율적으로 영향평가를 수행할 수 있도록 하되, 공공기관은 정보주체의 권리침해 우려가 큰 일정한 사유에 해당될 때에는 영향평가 수행을 의무화하도록 하였다.

개인정보 침해로 인한 피해는 원상회복 등 사후 권리구제가 어려우므로 영향평가의 실시로 미리 위험요인을 분석하고 이를 조기에 제거하여 개인정보 유출 및 오·남용 등의 피해를 효과적으로 예방할 수 있을 것으로 기대된다.

⑦ 개인정보 유출사실의 통지제도 도입(안 제32조)하였다. 개인정보처리자는 개인정보 유출 사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지하도록 하고 피해의 최소화를 위해 필요한 조치를 하도록 하였다. 이는 개인정보 유출로 인한 피해의 확산 방지를 위한 신속한 조치 및 정보주체의 효과적 권리 구제 등에 기여할 수 있을 것이다.

⑧ 정보주체의 권리를 보장(안 제33조부터 제37조까지)하였다. 정보주체에게 개인정보의 열람청구권, 정정·삭제 청구권, 처리정지 요구권 등을 부여하고, 그 권리행사 방법 등을 규정였다. 이처럼 정보주체의 권리를 명확히 규정함으로써 정보주체가 훨씬 용이하게 개인정보에 대한 자기통제권을 실현할 수 있을 것이다.

⑨ 개인정보 침해사실의 신고(안 제52조)는 개인정보처리자로부터 권

리 또는 이익을 침해받은 자는 행정안전부장관에게 그 침해사실을 신고할 수 있으며, 행정안전부장관은 신고 접수 및 업무처리 지원을 위해 개인정보 침해신고센터를 설치·운영해야 한다. 개인정보 침해사실을 신고하고 상담할 수 있는 창구를 마련하여 정보주체의 신속한 권리구제와 고충처리에 기여할 것이다.

이상으로 개인정보보호법의 주요 조항을 간단히 살펴보았다. 현재 정부와 여, 야당은 모두 개인정보보호법 제정의욕에는 적극적이다.

그러나 개인정보보호법의 계류 중인 이유 중에 하나는 감독기구의 기능과 역할 등에 대한 첨예한 의견 대립으로 인하여 지연이 되고 있는데, '개인정보보호위원회'를 별도의 독립감독기구로 두자는 주장과 국무총리 소속의 정책심의기구로 설치하자는 주장이 대립이 되고 있다.

그 주된 내용으로 다음과 같은데, 개인정보보호의 실질적인 강화 및 정보주체의 자기정보통제권을 효과적으로 보장하기 위해서는, 시장 및 행정권한 남용의 위험으로부터 독립된 중립적인 위원회 형태의 추진체계가 반드시 필요하다는 견해가 있다.[105]

그러나 정부는 책임성 · 신속성 · 강력한 집행력에 있어 다소 미흡한 위원회 형태의 조직보다는 개인정보의 유출, 오·남용 방지와 침해 시 즉각적인 대응을 위해서는 강력한 집행력 담보가 필수적이라는 점에서, 국가정보화를 총괄하고 있는 행정안전부에서 담당하는 것이 보다 효율적이라는 입장이다.[106]

---

105) 제17대 국회에서 제안된 3건의 개인정보보호법안에서도 추진체계는 모두 독립된 상설위원회 형태를 설치하도록 규정하고 있다. 국회행정안전위원회,「개인정보보호법안 」에 대한 공청회 자료집, 행정안전부, 2009. 4. 23, 239면.

106) 이 점과 관련하여, 각국(各國)의 개인정보 보호기구들로 구성된 「세계 개인정보 보호기구 협의회」에서 말하는 개인정보 보호기구의 독립성이란 기능상의 독립성과 그것을 유지할 수 있는 조직·인사·예산체계를 말하는 것일 뿐 반드시 조직 자체가 별도로 독립되어 있는 것을 요구하는 것은 아니라는 의견도 있다. 국회행정안전위원회,「개인정보보호법안 」에 대한 공청회 자료집, 행정안전부, 2009. 4. 23, 239면.

이와 같은 정부의 입장에 대해서는, 주민등록제도 운영 및 행정정보공동이용 등을 통해 개인정보의 침해위험성이 가장 큰 업무를 담당하고 있는 행정안전부가 개인정보보호 업무까지 관장한다는 것은 문제가 있다는 지적이 있다.[107] 개인정보 보호기구가 다양한 형태로 존재하고 있는 주요 외국의 사례에서 보는 바와 같이, 집행부로부터 독립적인 감독기구의 설치가 개인정보 침해를 예방하기 위한 필요 충분한 요소는 아니다.

<표 6> 주요 외국의 개인정보보호 추진체계 비교

구분		근거법률	형 태	비고
일본		개인정보보호법 행정기관개인정보보호법	내각부 소속 「정보공개·개인정보보호 심사회」설치 (공공) 총무성 장관 (민간) 각 부처	전담기구 없음
미국		(공공) 프라이버시법 (민간) 전자통신 프라이버시법 등 분야별 다수	(공공) 예산관리국(OMB) (민간)연방거래위원회(FTC), 통신위원회(FCC) 등 ※ 자율규제 원칙	
유럽	영국	정보보호법	정보커미셔너 (국왕 임명, 별도 통합기금)	행정부로부터 독립, 별도 기구
	프랑스	정보처리축적및자유에관한법률	정보자유위원회 (17인 구성, 법무부 예산)	
	독일	연방정보보호법	연방정보보호청	

107) 행정안전부는 업무 특성상 개인정보 침해의 가능성이 크고, 이런 점에서 행정안전부 역시 개인정보보호업무의 감독대상기관이라는 점에서 감독대상기관이 감독기관을 겸한다는 것은 객관성, 공정성, 투명성 측면에서 문제가 있다는 지적이다. 국회행정안전위원회,「개인정보보호법안 」에 대한 공청회 자료집, 행정안전부, 2009. 4. 23, 240면.

			(대통령 임명, 연방내무부소속) 정보감독청(민간부문,州별)	행정부 소속형
	스웨덴	정보보호법	정보조사원 (재정부장관 임명, 인력·예산 지원)	
	덴마크	개인정보처리에관한법률	개인정보보호원 (법무부장관 임명, 예산 지원)	
	그리스	개인정보의처리및보호에 관한법률	정보보호원 (대통령 임명, 행정부소속)	
아시아	**싱가포르**	없음(입법 논의 중)	보호기구 없으나, 재정부에서 일부 기능 수행	전담기구 없음
	대만	컴퓨터에 의해 처리되는 개인정보보호에 관한 법률	(공공) 법무부 (민간) 각 부처	
	인도	없음	통신규제국, 금융감독기구 등에서 일부 기능 수행	
기타	**캐나다**	(공공)프라이버시법 (민간)개인정보보호및전자문서에관한법	연방프라이버시커미셔너 (추밀원장 임명, 예산·인사 독립)	행정부로부터 독립, 별도 기구
	멕시코	없음(소비자보호법 등)	각 부처	
	칠레	개인정보보호법	각 부처	전담기구 없음

*** 출처: 행정안전부**

그러나 현재 공공기관에서의 개인정보 침해사례가 증가하고 있는 현실과, 정보보호의 역사 역시 일천한 우리나라의 특성을 감안해 볼 때, 개인정보보호 업무의 전문성 · 객관성 · 투명성을 강화하기 위한 독립적인 위원회 형태의 조직설치는 일정부분 필요한 측면도 있다.

결국, 개인정보보호 추진체계 형태의 적합성 여부는 우리나라의 사회 · 경제적 환경과 법적 전통, 개인정보보호 수준 및 주요 외국의 사례 등을 종합적으로 고려하여 입법정책적으로 결정되어야 할 것으로 본다.

다만 정부안의 추진체계가 우리의 실정에 부합한다는 입장을 견지하더라도, 행정안전부 역시 개인정보보호 업무의 감독대상기관이라는 점에서 개인정보보호 업무의 소홀 우려 및 정책의 객관성 · 투명성 미흡 가능성에 대한 지적을 감안하여, 심의기구에 불과한 「개인정보보호위원회」의 소속 및 권한을 보다 강화하고, 위원 구성의 독립성을 제고하는 등 실질적인 기능상의 독립성을 강화하는 방안을 검토할 필요가 있다.[108]

하지만 지금 현재에도 개인정보가 유출, 도용은 지속적으로 발생하고 대규모 개인정보가 유출 및 오· 남용 되는 등 침해 사례가 증가 있다.

따라서 정부와 여·야당은 국민의 기본권 보호와 더불어 불안감을 해소시키고, 공공기관, 민간기관의 적극적인 보호차원에서라도 현재의 논쟁을 효율적으로 해결하여 계류중인 이 개인정보보호법이 조속히 통과되어 시행되어야 할 것이다.

108) 국회행정안전위원회,「개인정보보호법안 」에 대한 공청회 자료집, 행정안전부, 2009. 4. 23, 239-242면 참조.

제5장 결 론

오늘날 개인정보는 인간의 존엄과 자유를 실현하기 위해 보호되어야 할 필수 불가결한 조건인 동시에 기업활동을 위해서는 없어서는 안될 중요한 영업자산으로 인식되고 있다. 그러나 정보통신기술의 발달에 따른 가상공간에서의 개인정보의 침해 및 오·남용 문제는 그 심각성이 더해가고 있으며, 여기에 더불어 인간으로서의 존엄과 자율성의 상실을 가져오고 있다. 더 나아가 사회·경제적으로도 개인정보를 적절히 보호하지 않고서는 정보사회를 통한 국가의 발전을 기대하기는 어렵다.

한 예로 미국은 2005년에만 3억3000만건의 개인정보침해 사건이 벌어지는 등 문제가 심각하였다.

그러나 2009년 11월 8일 현재 연 수억건에 이르는 개인정보 침해 사고를 막기 위해 관련 법안이 속속들이 통과되었다. 미국 상원 법사위는 '데이터침해 통지법'(Data Breach Notification Act)[109]과 '개인정보보호와 보안법'(PERSONAL Data Privacy and SECURITY Act)[110]을 압도적인 찬성 아래 통과시켰다고 한다. 이 법안은 이후 상원 전체의 의결을 거쳐 공표가 된다. 미국은 그동안 많은 기업들은 의회에 데이터 침해에 관한 연방법을 통과시켜달라고 요구해왔다. 지난 2005년 이래 45개 주가 모두

109) 민주당 다이앤 파인스타인 상원의원이 발의한 데이터침해 통지법의 골자는 정부기관과 기업이 개인정보가 이미 공개됐거나 공개됐을 것으로 추정될 때 당사자에게 그 사실을 고지해야 한다는 것이다. 또 개인정보에 누군가 접근했거나 유출됐을 경우에도 마찬가지다. 대규모 데이터 침해가 벌어졌을 경우 정부기관과 기업은 미국 첩보부에도 보고해야 한다. 디지털 타임스, 2009. 11. 9일자.

110) 개인정보보호와 보안법은 민감한 정보에 대한 침해 위험 평가와 취약성 테스트, 통제 등에 관한 가이드라인을 제시한다. 이 법에도 역시 개인정보를 보관하고 있는 기관이 침해사고가 일어났을 때 잠재적 희생자와 사법 기관에 그 사실을 통보해야 한다고 규정돼 있다. 또 개인정보 도용에 관한 형벌을 확대했다. 디지털 타임스, 2009. 11. 9일자.

개인정보 보호 관련 법안을 통과시켰다.[111]

이러한 미국과 달리 우리의 현실은 어떠한가?

2008년 3월 행정안전부와 학계, 전문기관을 중심으로 개인정보보호법 제정을 위하여 법제정 TF 팀이 구성된 이후 아직까지도 국회에 계류 중에 있다. 지금 이 순간에도 개인정보 유출, 노출, 침해는 계속해서 발생하고 있는데, 이를 해결할 수 있는 관련 법률은 국회에서 잠을 자고 있는 것이 지금 우리의 현실이다.

개인정보보호법의 통과 뿐만 아니라 개인정보보호를 위해서는 앞으로도 추진해야 할 과제들이 많이 있다. 구체적으로 예를 들면, 개인정보보호법 뿐만 아니라 관련 하위법률의 정비, 법 시행에 따른 개인정보보호위원회 구성과 같은 제도 마련도 해야 할 것이다. 그리고 개인정보보호 피해구제 활성화를 위해서 침해신고센터의 운영, 침해민원 포털시스템 구축, 개인정보분쟁조정위원회를 통한 신속한 권리구제 및 손해배상 기준을 마련해야 한다.

더불어 개인정보보호의 관리적 · 기술적인 보호조치도 강화를 해야한다. 여기에는 개인정보보호 수준진단을 확대해야 하며, 홈페이지 모니터링의 강화, 개인정보파일 관리 및 실태 점검의 강화, 개인영상정보 보호의 강화, 공공 I-Pin 서비스 확대, 개인정보 영향평가제 시행, 종합관리시스템 구축 기반 마련, 개인정보보호를 위한 인식제고 및 역량을 강화를 위해 공공기관과 민간기관의 교육을 강화 등 추진해야 할 것이 많이 있다.

이러한 후속적인 과제를 추진하기 위해서는 전제조건으로 현재 국회에 계류 중인 개인정보보호법이 통과되어 시행되어야 할 것이다. 조속한 시일안에 개인정보보호법이 통과되길 바라면서 이글을 맺고자 한다.

---

111) 디지털 타임스, 2009. 11. 9일자.

【참고자료】

<표 6> 개인정보보호법 제정으로 현재와 달라지는 점

구분	현 행	제정(안)
규율대상	o 공공기관, 정보통신분야 사업자, 신용정보 제공·이용자 등 분야별 규율대상 한정	o 공공·민간 통합 규율로 법적용대상 확대 - 현행법 적용을 받지 않던 오프라인 사업자, 의료기관, 협회·동창회 등 비영리단체, 국회·법원·헌법재판소·중앙선거관리위원회 등으로 확대
보호범위	o 공공기관은 컴퓨터등에 의해 처리되는 개인정보파일만을 보호대상으로 함	o 동사무소 민원신청서류 등 종이문서에 기록된 개인정보도 보호대상에 포함
수집·이용 제공기준	o 공공, 정보통신 등 분야별 개별법에 근거한 상이한 기준 적용	o 공공·민간 통일된 처리원칙과 기준 적용
고유식별정보 처리 제한	o 주민등록번호 등 고유식별정보의 민간사용을 사전적으로 제한하는 규정 없음	o 원칙적 처리금지 - 법령이 있거나 별도 동의가 있는 경우만 예외적으로 허용
	o 인터넷상에서 주민등록번호 외의 회원가입방법 제공 의무화 (정보통신서비스제공자 한	o 인터넷상 주민등록번호 외의 회원가입방법 제공 의무화 대상 확대 (정보통신서비스제공자 → 공공기관,

구분	현 행	제정(안)
	정)	일부 민간분야 개인정보처리자)
		o 주민등록번호 등 고유식별정보 처리시 암호화 등 안전조치 확보의무 명시
영상정보처리기기 규제	o 공공기관이 설치·운영하는 폐쇄회로텔레비전에 한하여 규율	o 공개된 장소에 설치·운영하는 영상정보처리기기 규제를 민간까지 확대 - 공개된 장소인 백화점·아파트 등 건물주차장, 상점 내·외부 등에 영상정보처리기기를 설치할 때에는 법령, 범죄예방·수사, 시설안전 및 화재예방, 출입통제, 교통단속, 기타 공익적 목적을 위해서만 가능함 o 규율대상을 기존 '폐쇄회로텔레비전(CCTV)'에서 네트워크카메라도 포함
		o 공중 화장실·목욕탕·탈의실 등 사생활 침해우려가 큰 장소는 설치 금지
텔레마케팅 등 규제	o 「정보통신망법」에 따라 정보통신서비스제공자에 한하여 규제 - 마케팅 목적으로 개인정보	o 마케팅을 위해 개인정보처리에 대한 동의를 받을 때에는 다른 개인정보 처리에 대한 동의와 묶어서 동의를 받지 않도록 명

구분	현 행	제정(안)
	취급을 위탁하는 경우 정보주체 동의를 받아야 함	시적으로 규정 - 정보주체가 알기 쉽도록 고지하고 동의를 받아야 함 o 모든 개인정보처리자는 마케팅 업무를 위탁시, 정보주체에게 위탁업무 내용 및 수탁자를 고지해야 함 (정보통신서비스제공자 → 모든 개인정보처리자로 규제대상 확대)
개인정보 파일 등록·공개 및 영향평가	o 공공기관이 개인정보파일 보유시 행정안전부장관과 사전협의	o 공공기관이 개인정보파일 보유시 행정안전부장관에게 등록
	o 행안부장관은 사전협의파일 관보 공고	o 행안부장관은 등록사항 공개
		o 대규모 개인정보파일 구축 등 침해위험이 높은 경우에는 사전영향평가 실시 의무화(민간은 자율시행)
유출 통지	o 관련 제도 없음	o 개인정보 유출사실 통지 의무화

*** 출처 : 행정안전부**

【參考文獻】

Ⅰ. 國內文獻

1. 單行本

桂禧悅, 憲法學(中), 博英社, 2007.

權寧星,「憲法學原論」, 法文社, 2007. 2.

金哲洙,「憲法學新論」, 博英社, 2007. 4.

南孝淳·丁相朝,「인터넷과 法律Ⅱ」, 法文社, 2005. 12.

文鴻柱,「美國憲法과 基本的 人權」, 裕豊出版社, 2002.

裵鍾大·李相暾,「刑事訴訟法(第6版)」, 弘文社, 2006.

成樂寅,「憲法學」, 法文社, 2007.

申東雲, 형사소송법[제4판]」, 法文社, 2007.

尹明善,「美國憲法과 統治構造」, 유스북, 2006. 2.

李在祥,「刑事訴訟法(第6版)」, 博英社, 2007.

조 국,「위법수집증거배제법칙」, 博英社, 2005.

2. 論 文

권건보, 「개인정보보호와 자기정보통제권」, 경인문화사, 2005.

고영석, 「전자감시사회와 프라이버시」, 커퓨티케이션북스, 1998.

권태웅, 「미국의 전자정부법제와 추진전략」, 법제, 법제처, 2004.

국회행정안전위원회,「개인정보보호법안 」에 대한 공청회 자료집, 행정안전부, 2009. 4.

김재광, 「영미법계 국가의 개인정보보호법제 동향 및 함의」, 공법학연구 제6권 제2호, 2005.

金正熙, 인터넷상 個人信用情報保護에 관한 法的 考察, 慶熙大學校 碩士學位論文, 2003. 3.

김행미,「전자상거래에서의 개인정보보호방안에 관한 연구」, 경희대학교석사학위논문, 2002.

金哲洙,「美國憲法이 韓國憲法에 미친 影響序說(美國憲法과 韓國憲法)」, 韓國公法學會, 大學出版社, 1989.

길준규, 「개인정보의 개념과 특징」, 토지공법연구 제18집, 2003.

박창욱, 「인터넷상 개인정보보호법제의 문제점과 개선방안에 관한 연구」, 울산대학교 대학원 석사학위논문, 2008.

백윤철, 「헌법상 개인정보자기결정권에 관한 연구」, 법조, 2002.

백윤철 외, 「개인정보보호법」, 한국학술정보(주), 2008.

방송통신위원회, 인터넷상 개인정보 침해방지 대책, 방송통신위원회, 2008. 4. 24.

사이버경제사회연구소, 「인터넷 개인정보 노출방지 및 프라이버시 보호 방안 연구」, 한국정보보호진흥원, 2007. 12.

쉔케/ 박종수 번역,「通信의 基本權的 問題」, 公法硏究 제30집 제2호, 2001.

成樂寅,「개인정보보호법제의 현황과 재정립 방향」, 인터넷과 法律Ⅱ, 法文社, 2005.

尹明善,「性的 프라이버시 權利」, 美國憲法硏究 제6호, 1995.

안경옥,「정보화사회의 새로운 수사기법과 개인의 정보보호」, 비교형사법연구 Vol.5 No. 1, 한국비교형사법학회, 2003.

이인호,「개인정보보호에 대한 국제적 논의방향과 국내 법제의 개선방향」, 한국정보보호진흥원 2002년 제2회 개인정보보호 워크샵 자료집, 2002. 7. 26.

이자성,「일본 개인정보보호제도에 있어서 운영현황 및 법적구성에 관한 고찰 -개인정보보호법 및 행정기관의 개인정보보호법을 중심으로-」,자치정보화조함 지역정보연구단, 국제지역학회, 2007.

임지봉, 「미국의 전장정부법제」, 한국법제연구원, 2001.

정보통신부, CCTV 개인영상정보보호 가이드라인해설서, 한국정보보호진흥원(KISA) · 정보통신부(MIC), 2006. 10.

정찬모,「개인정보 오·남용 실태와 법제도적 대응방향」, 정보역기능 방지대회 공청회 자료, 1999. 9. 8.

조연상 외 2인, 「기업경영자원으로서의 개인정보이용 및 보호방안 연구」, 한국정보보호진흥원, 2001.

趙泰濟, 「公共情報의 作成및 取得段階에서의 制度改善方案」, 인터넷 법률 통권 제16호, 2003. 3.

정준현,「유비쿼터스 컴퓨팅과 프라이버시보호」, 成均館法學 第16券 第1號, 成均館大學校 比較法硏究所, 2004.

丁泰鎬,「個人情報自決權의 憲法的 根據 및 構造에 대한 考察」, 憲法論叢, 제14집, 2005.

황종성,「국외 개인정보보호법제 분석 및 시사점」, 한국전산원, 2004.

황상철, 「일본의 개인정보보호를 위한 입법동향」, 법제, 2003.

행정안전부 공고 「개인정보보호법」제정안, 2008. 8. 11.

행정안전부, 2009년도 개인정보보호 정책 방향, 행정안전부 정보화전략실 개인정보보호과, 2009, 4. 24.

행정안전부,「공공기관 개인정보보호 이해와 해설」, 행정안전부 개인정보보호과, 2008.

행정안전부,「개인정보보호법안 」에 대한 공청회 자료집, 국회행정안전위원회, 2009. 4. 23.

행정안전부, 2008년도 국가간 정보보호 수준 비교, 행정안전부, 2008.

한국정보보호진흥원, 「2002 개인정보보호 백서」, 2002.

한국형사정책연구원,「개인정보침해에 관한 조사 연구」,연구보고서, 2001.

2009 국가정보보호백서, 국가정보원·방송통신위원회·행정안전부·지식경제부, 2009. 4.

II. 外國文獻

Bruckman, Amy, Finding One's Own Space in Cyberspace. Technology Review, January 1999.

Colin J. Bennett & Rebecca Grant, “Introduction”, in Visions of Privacy: Policy Choices for the Digital Age, Colin J. Bennett & Rebecca Grant eds., 1999.

EPIC & Privacy International, Privacy & Human Rights: An International Survey of Privacy Laws and Developments, Electronic Privacy Information Center Washington, DC, 2001.

Fernback J, There is a There There: Notes Toward a Definition of Cybercommunity. In S. Jones (Ed.). Doing Internet Research, pp. 203-220, Thousand Oaks: Sage, 1999.

Glasser, B., & Miller, J, The 'Inside' and the 'Outside' Finding Realities in interviews. In D. Silverman (Ed.). Qualitative Research: Theory, Method and Practice, pp. 99-129, 1997.

Healy, D, Cyberspace and place: The Internet as middle landscape on the electronic frontier. In D. porter (Ed.). Internet Culture, pp. 55-71, New York: Routledge, 1997.

Pavesich v. NEW England life Insurance Co., 122 Ga. 190. 50. S.E. 68(1904).

岡村久道・新保史生, 「電子ットフ-クと 個人情報保護- オンラインプライバシ-法入門」, 經濟産業調査會, 2002.

松井茂記, 「アメリカ-プライヴァシ-保護法制の展開」, 法律時報, 72卷10號, 200. 9.

III. 인터넷 웹사이트(Internet Web Site)

구 글, www.google.co.kr

네이버, www.naver.com

한국정보보호진흥원,www.kisa.or.kr

한국인터넷진흥원, http://www.kisa.or.kr

국제 법률·정책포럼, www.ilpf.org

국제연합(UN), www.uncjin.org

www.europa. eu. int

Ⅳ. 언 론

동아일보, 2008. 4. 17 일자.

동아일보, 2008. 9. 22 일자.

동아일보, 2008. 10. 30 일자.

DATANET, 2009. 8. 5 일자.

디지털 타임스, 2009. 11. 9일자.

디지털타임스, 2009. 11. 24 일자.

매일경제신문, 2009. 10. 8 일자.

보안뉴스, 2008. 11. 10 일자.

보안뉴스, 2009. 11. 24일자.

보안뉴스, 2008. 12. 12 일자.

보안뉴스, 2008. 12. 31일자.

서울경제신문, 2008. 9. 7 일자.

소비자가 만드는 신문, 2008. 8. 5일자.

시사1번지 폴리뉴스, 2008. 7. 20 일자.

월간 정보보호21c 통권 제100호.

MBC, 2008. 4. 24일 방송.

연합뉴스, 2008. 11. 10 일자.

유코피아뉴스, 2008. 8. 7일자.

조선일보, 2008. 4. 17 일자.

중앙일보, 2008. 4. 17 일자.

중앙일보, 2008. 10. 20 일자.

프라임 경제, 2008. 9 6 일자.

코리아 포스트, 2009. 6. 23일자.

한겨레 신문, 2008. 4. 17 일자.

한겨레 신문, 2008. 8. 20 일자.

한겨레 신문, 2008. 7. 19 일자.

한겨레 신문, 2008. 11. 11 일자.

한국경제신문, 2008. 4. 17 일자.

책임연구보고서 2009-20

개인정보 침해 분석과 이에 대한 입법적 대응에 관한 연구

발행일 : 2009년 12월 24일
발행인 : 김 길 배
발행처 : **치 안 정 책 연 구 소**
경기도 용인시 기흥구 언동1길 29
홈페이지 : www.psi.go.kr

POLICE SCIENCE INSTITUTE