개인정보와 사생활의 비밀과 자유 보호를 위한 정책 연구

국가인권위원회 2004년도 연구용역사업의
최종보고서를 제출합니다

2004. 9

연구책임자

윤영민(한양대학교 정보사회학과 교수)

연구자

김현석(한양대학교 연구교수)
고동현(연세대 강사)
최　홍(한양대학교 대학원)
류자현(한양대학교 대학원)

한 양 대 학 교

목 차

1. 서 론: 네트워크사회와 프라이버시

1.1. 사회적 쟁점으로서의 프라이버시

우리나라에서 지난 10여 년 동안 개인정보 혹은 프라이버시 보호만큼 새로운 사회적 쟁점은 찾아보기 어렵다. 아직도 그것은 많은 사람들에게는 잘 이해가 되지 않는 낯선 쟁점이다. 대부분의 사람들은 프라이버시 침해가 왜 그렇게 심각한 문제가 되는지 왜 프라이버시를 다른 사회적 가치를 포기하면서까지 지켜야 하는지를 이해하지 못한다.

이는 놀라운 일이 아니다. 무엇보다 5-6년 전까지만 해도 개인정보 혹은 프라이버시 보호에 대해서는 '~하지 않는다면 앞으로 ~할 것이다' 라는 식의 미래가정법으로 문제가 제기될 수밖에 없었고, 최근에야 겨우 몇몇 구체적인 피해 사례들을 가지고 논쟁할 수 있게 되었다.

더구나 공공부문에서는 아직도 개인정보보호가 예방적 성격의 입법이나 정책이다. 민간부문과 달리 개인정보의 유출로 인한 심각한 피해를 발생하지 않았기 때문이다.

사람들은 사생활 혹은 이름도 낯선 프라이버시가 자유, 민주, 정의만큼 목숨을 걸고 지켜야 할 가치라는데 동의하기 어렵다. 무엇보다 우리사회는 개인의 사생활을 존중하고 강조하는 문화적 전통을 갖고 있는 것도 아니고 근대화를 통해 개인주의가 충분히 개화한 것도 아니기 때문이다.

게다가 프라이버시에 대한 주장들은 이념적으로 충분히 성숙되지 못했다. 아직 어떤 이론가도 그것이 목숨을 바칠 만큼 중요한 가치임을 입증하는데 성공하지 못하고 있다. 몇몇 학자들이나 운동가들이 그것의 중요성을 소리 높여 외치고 있을 뿐 큰 사회적 반향을 찾을 수 없다.

그리고 또 하나 빼 놓을 수 없는 이유는 프라이버시에 대한 제약이 늘 시민들이나 소비자들에게 상당히 매력적인 보상과 함께 제시된다는 점이다. 국가안보, 생명과 재산의 안전, 효율성, 국가경쟁력, 편의성 등 결코 무시될 수 없는 가치가 프라이버시의 제약에 대한 보상으로 거론된다. 때문에 사람들에게 프라이버시와 관련된 선택은 항상 혼란스럽다.

이 때문에 프라이버시에 관한 입법이나 정책 추진에 있어 강력한 사회적 지지나 정치적 동력을 끌어내기 쉽지 않다.

그러나 그럼에도 불구하고 개인정보 혹은 프라이버시 보호에 관해 시급히 국가적 입장을 세우지 않으면 안 된다. 당분간 프라이버시는 갈수록 뜨거운 사회적 쟁점이 될 것이기 때문이다.

이미 전자주민카드, 전자건강보험증, NEIS 등 정보화 국책사업을 둘러싸고 우리사회는 적지 않은 혼란을 경험하였으며, 그에 따른 거액의 사회적 비용을 지불하였다.

정부는 유비쿼터스 컴퓨팅을 우리 경제의 차세대 성장엔진 중 하나로 선택하여 적극적으로 관련 사업들을 추진하고자 한다. 그런데, 스마트카드, 무선 인터넷, LBS, RFID, IP v.6 등 유비쿼터스 컴퓨팅에 적용되는 정보기술 중 어느 하나 프라이버시 문제를 내포하지 않는 것이 없

다.

전자정부사업도 계속 프라이버시 문제를 불러일으킬 것이다. 현 단계에서 전자정부사업들은 거의 모두 부처간 정보공유를 전제로 하고 있기 때문이다.

어떤 방식으로든 국민들 사이에 공감대가 형성될 수 있는 대안이 마련되지 않으면 우리나라의 정보화는 심각한 장벽에 부딪치게 될 것이다.

1.2. 프라이버시의 역사성

한 사회에 있어 프라이버시 개념은 대체로 정보통신기술의 발전과 그에 따른 사회적 변화를 반영한다.

19세기말 명사들의 스캔들 보도에 경쟁적이었던 황색저널리즘은 '홀로 있을 권리'라는 고전적 의미의 프라이버시 개념을 등장시켰다. 대중매체의 보도로부터 보호받아야 할 사적 영역이 존재한다는 인식이 탄생한 것이다.

근대적 우편제도가 시작된 19세기 중엽부터 통신의 비밀이 법적 권리로 등장했으며, 20세기에 들어와 전화가 널리 보급되고 도·감청이 증가하면서 프라이버시 개념은 통신의 비밀까지 포함하도록 확장되었다.

그러나, 대중매체나 전화까지만 해도 아직 프라이버시는 유명한 정치인, 연예인, 혹은 운동선수가 아닌 보통사람들에게 관심을 가질만한 권리로 인식되지 않았다.

컴퓨터가 통신에 널리 활용되고 대규모의 데이터베이스에 대한 원격접속이 가능해짐에 따라 개인정보의 보호가 프라이버시 개념에 추가되었으며, 비로소 프라이버시는 대중적 관심사로 발전하였다.

디지털 정보기술에 의존한 대규모 데이터베이스의 등장은 개인정보의 가치를 높여주었다. 사실 보통사람의 개인정보는 개별적으로 존재할 때 교환가치가 거의 없으며, 데이터베이스에 집적되었을 때 비로소 상업적 가치를 획득하게 된다. 두 가지 의미에서 그러하다. 첫째, 개인정보는 대량으로 처리되는 정보의 일부가 되었을 때 가치를 갖는다. 예컨대 정크메일을 발송하는데 사용되려면 많은 사람들의 주소가 담긴 데이터베이스가 필요하며, 개인주소는 그 데이터베이스의 일부가 되었을 때 상업적 가치를 갖게 된다.

둘째, 행정이나 금융 업무가 데이터베이스로 관리되는 구조이기 때문에 주민등록번호, 은행구좌번호, 신용카드번호 등과 같은 개인정보의 유출이 정보주체에 심각한 피해를 입힐 수 있는 가능성을 갖게 되었다. 만약 행정이나 금융 업무가 수작업으로 처리되고 민원서비스가 대면적(對面的)으로 수행된다면 주민등록번호나 은행구좌번호가 남에게 알려진다고 해도 정보주체에 피해가 돌아가 가능성은 아주 적을 것이다.

사실 보통사람들에게 있어 프라이버시는 정보사회에 진입하면서 비로소 관심사가 되었다. 정보화는 개인정보에 가치를 부여하면서 동시에 개인정보 혹은 프라이버시 침해를 사회적 쟁

점으로 끌어올렸다. 혹자는 정보화가 프라이버시 침해를 초래하고 있다고 주장하지만 그것은 반쪽의 진실이다. 프라이버시 침해를 논하기 이전에 프라이버시를 침해할 만한 가치로 격상시킨 것이 바로 정보화이기 때문이다.

정보화는 프라이버시를 사회의 보편적 가치로 끌어올렸을 뿐 아니라 그것의 의미를 확장시켰다. 최근에 프라이버시는 다음과 같이 여러 가지 의미로 사용되고 있다.

첫째, 프라이버시는 원하지 않은 접근으로부터 자유로울 권리를 말한다. 이는 '홀로 있을 권리'라는 고전적 의미의 연장으로 볼 수 있다. 그것은 개인의 신체나 공간에 대한 물리적 접근을 의미할 뿐 아니라 전자우편, 메시징, SMS 등과 같은 전자적 접근도 포함한다. 다시 말해 주민이나 소비자가 온라인이나 오프라인을 통한 타인의 접근을 거부할 수 있는 권한을 갖는 것을 가리킨다.

둘째, 프라이버시는 자신에 관한 정보가 자신이 원하지 않는 방식으로 이용되지 않을 권리를 의미하기도 한다. 이는 본인의 동의 없이 혹은 법적 근거 없이 개인정보가 수집, 보유, 매매, 이전, 노출, 매칭 등이 되지 않을 권리를 말한다.

셋째, 프라이버시는 자신이 정확하고 올바르게 표현될 권리를 의미하기도 한다. 데이터베이스의 소유자나 관리자는 그곳에 담긴 개인정보의 무결성(integrity)을 유지해야할 의무가 있으며, 정보주체는 데이터베이스에 들어있는 자신의 정보를 열람하고 정정하거나 정정을 요구할 수 있어야 한다는 말이다.

넷째, 프라이버시는 자신의 정보가 지닌 가치에 대해 보상받을 권리를 의미하기도 한다. 상업적 목적으로 개인정보를 수집하고 이용할 때는 각 정보주체에게 어떤 형태로든 적절히 보상해야 함을 가리킨다.

다섯째, 보다 포괄적 관점에서 프라이버시는 정보주체의 자기정보 통제권이라는 의미로 사용되고 있다. 프라이버시는 개인정보의 수집에서부터 보관, 관리, 이용, 이전, 그리고 폐기에 이르기까지 개인에 관한 정보가 사회적으로 활용되는 모든 과정과 방식에 관해 개인정보에 관한 정보주체의 권리가 어떻게 보장될 수 있는가라는 의미로 확대되었다는 말이다. 다시 말해 프라이버시가 개인이 자신의 어떤 정보가, 누구에 의해, 어떻게 수집되고, 어떻게 보관되며, 어떻게 이용되는가에 대해 스스로 결정할 수 있는 권리로 인식되고 있다.

이러한 개념적 변화에서 가장 주목할만한 경향은 프라이버시 보호에 관한 담론에서 정보주체라는 존재가 확실히 자리 잡기 시작했다는 사실이다. 다시 말해 정보주체가 정보소유자로부터 구분되고 정보주체의 권리가 새롭게 인식되고 있다는 것이다.

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

그러나, 정보기술의 발달이 가져오는 프라이버시의 개념적 변화가 여기서 끝날 것으로 보이지 않는다. 그것은 정보화가 궁극적으로 프라이버시가 전제하는 개인(individual)에 대한 관념 자체를 바꿀 것으로 예상되기 때문이다.

서양문명에서 개인에 대한 관념 혹은 개인주의는 고대 그리스 소피스트 시대에 최초로 등장한다. 그러나 그것이 근대성(modernity)의 핵심적 요소로 자리 잡기 시작한 것은 르네상스 이후이다. 자신을 중심으로 우주를 바라보고, 자신이 자신의 행동과 삶, 나아가 운명에 대해 성찰하고 책임져야하는 존재라는 인식, 사회 속에서 살아가지만 인간은 궁극적으로 혼자이며 고독한 존재라는 인식, 인간은 사물과 현상을 객관적 가치에 따라 합리적으로 판단하고 결정하는 존재라는 인식, 그리고 나(Self)와 타자(Others) 사이의 분명한 구분은 근대성을 이전의 문명과 구분 짓는 요소 중의 하나이다.

이런 의미에서 개인은 근대의 산물이다. 현대사회에서 더 이상 개인은 가족, 부족, 혹은 지역사회와 같은 전통적 공동체의 일부로서만 존재할 필요가 없게 되었다. 개인은 자신의 행복을 최우선적으로 추구하며, 개인에 대한 평가와 판단은 개인이 속한 공동체가 아니라 그 개인의 재능, 성격, 행동, 그리고 업적에 근거를 두어야 한다는 사고가 지배적이 된 것이다.

정보화로 인한 개인정보의 가치 증식은 이러한 근대적 개인의 문화와 만남으로서 프라이버시 문제로 부상된다. 만약 정보화로 인해 근대적 개인이 어떤 다른 존재나 존재인식에 의해 대체된다면 프라이버시는 개념적으로 어떻게 변화될까?

이러한 인식변화를 요구하는 기술적 발전이나 조직적 변화가 이미 빠르게 진행되고 있다는데 프라이버시에 대한 논의, 나아가 프라이버시에 대한 입법과 정책 수립의 진정한 어려움이 있다.

여러 연구가 지적했듯이 최근까지 인터넷 확산은 개인화(individualization) 혹은 개인주의를 촉진하는 경향을 나타냈다. 인터넷으로 인해 개인 자체와 개인이 지닌 가치에 대한 인식이 제고되었을 뿐 아니라 개인적으로 행동할 수 있는 역량이 크게 강화되었다. 인터넷은 개인이 더 이상 전통적인 사회적 굴레에 억매일 필요가 없게 만들었다. 사이버공간에서 개인은 자신의 선호와 기호에 따라 수없이 많은 가상공동체에 가입해서 자유롭게 활동할 수 있다. 사이버공간은 극도로 세분화되어 사람들은 아주 미세한 관심사, 취미, 기호 등으로 형성된 가상공동체에서 기능적 욕구를 충족한다. 이렇게 해서 개인의 정체성을 규정했던 기존의 사회적 범주들(예: 성별, 인종, 계층)이 힘을 잃게 된다.

이러한 의미에서 어떤 학자들은 정보화가 개인의 승리 그리고 근대의 완성을 가져올 것으로 기대하고 있다. 그러나 역사는 반전을 좋아하는지 모른다. 최근에는 컴퓨터 네트워크의 발달이 그와는 매우 다른 방향으로 역사를 구동시킬 지도 모른다는 예측이 등장하고 있다.

Douglas Rushkoff(2004)는 인터넷이나 이동전화를 통해 항상 네트워크에 접속되어 있게 되면 더 이상 개인은 자신의 축적된 능력과 업적의 총합이 아닐 것이라고 예상한다. 또한 그는 물건이든 돈이든 데이터든 무엇을 얼마나 소유하고 있는가가 큰 의미를 지닐 수 없게 될 것이라고 예상한다. 더 이상 희소성이 지배하는 사회가 아닐 것이기 때문이다. 그는 그러한 네트워

크사회에서는 다른 사람과 함께 네트워킹하고 정보와 지식을 공유하는 행위가 사회적으로 높이 평가될 것이라고 예측한다. 그는 네트워크사회에서 궁극적으로 개인성(individuality)이라는 생각 자체가 사라지게 될 지도 모른다고 예상한다.

정보기술의 발전이 한걸음 더 나아가 인간의 신경계와 컴퓨터네트워크가 직접 연결되는 사이보그(cyborg) 사회가 출현하면 어떻게 될 것인가? 인공두뇌학자 Kevin Warwick(워릭, 2004)은 2050년경이면 모든 의사소통이 인간의 신경계가 직접 네트워크에 연결된 상태에서 이루어지게 될 것이고 따라서 말과 언어-따라서 전화도-가 불필요하게 될 것으로 예측한다. 그는 하나의 물리적 개체로서의 개인은 희미한 존재가 되고 대신에 네트워크 상에서 집단적 개인이나 새로운 인격체가 출현할 것으로 예상한다.

이러한 상상을 먼 미래의 일이라고 치부할 것인가?

실제로 최근의 기술적 혹은 사회적 변화를 보면 이미 우리는 그러한 네트워크사회에 깊숙이 진입해 있으며 개인과 프라이버시에 대한 새로운 인식이 필요한 시점에 도달해 있다는 생각이 든다. 이동전화의 발달, 무선통신기술과 네트워크 기술의 발달 그리고 그러한 기술발달에 힘입은 사회조직의 변형이 급속히 진행되고 있다. 전자정부는 전통적인 의미의 부서(혹은 부처)간의 경계를 넘어선 '정보의 공유'를 요구하고 있으며, 통상적 의미의 기업간 경계를 넘어선 네트워크기업(혹은 가상기업)이 출현하여 민간영역에서도 '정보의 공유'가 '정보의 소유' 문화를 빠르게 대체하고 있다.

어쩌면 지금 우리 사회는 프라이버시 영역에서 문화지체(cultural lag) 현상을 겪고 있는지도 모른다. 프라이버시에 관한 한 유엔인권헌장 정도로 간주되는 프라이버시에 관한 OECD 가이드라인은 25년 전 정보사회의 초입에 제시된 구상이다. 1980년 이후에 일어난 엄청난 기술적 그리고 사회적 변화를 고려한다면 우리는 그것이 지닌 현실적합성에 대해 진지하게 검토해 보아야 할 것이다(Waters, 2000).

그런데, 현실은 그 가이드라인을 금과옥조처럼 받들고 있으며, 그것의 사회적 적합성을 따지는 논의는 거의 전무하다. 그것이 의사-이념적(擬似-理念的) 갈등 형태를 띠면서 논점이 수면위로 떠오르지 못하고 있다고 판단된다. 그 낡은 가이드라인마저도 이제야 우리나라의 입법과 정책에 제대로 반영되기 시작했다는 사실이 안타깝지만, 적어도 거기에 포함된 개념들이 시대착오적일 수 있다는 가능성을 배제해서는 안 될 것이다.

1.3. 프라이버시의 사회적 특성

대부분의 다른 권리도 그렇지만 프라이버시는 특히 다른 권리나 가치와 충돌하는 경우가 많다. 프라이버시가 포괄적인 가치이면서 도구적 가치이기 때문일 것이다.

애초부터 프라이버시는 언론의 자유 혹은 독자들의 알권리와 충돌하였다. 명사들의 사생활 보호를 강조하면 기자와 언론에 주어지는 보도의 자유가 위축된다. 그래서 언론에 있어 프라이

버시 보호는 보도의 자유와 프라이버시 사이의 끝없는 줄다리기였다.

프라이버시 보호는 국가안보와 국민의 안전을 책임지는 수사기관의 법집행을 위한 요구와 충돌하기도 한다. 9.11 사건이후 미국의 공항에서는 지문과 같은 생체인식시스템을 이용해 외국인의 출입국을 관리하고 탑승자 모두에게 대단히 엄격한 검색-다른 때 같았으면 프라이버시 침해라고 고소를 당했을 정도로 엄격한 조사-를 받도록 요구하고 있다.

그리고 최근 유럽위원회와 유럽의회는 회원국들이 이동전화, SMS, 전화, 팩스, 전자우편, 채팅, 인터넷 등을 통해 발생하는 모든 통신자료의 보관을 의무화하는 법률을 제정할 수 있도록 하는 결의안을 채택했다. 테러리즘과 효과적으로 싸우기 위한 조치라고 하지만 그것은 프라이버시를 위축시킬 수 있는 선택이었다(Laurant and PI, 2003).

또한 미국, 영국 등 여러 나라에서는 암호키의 위탁관리 문제를 두고 치열한 논쟁이 벌어졌다. 수사기관들은 마약, 테러, 납치 등의 범죄를 효과적으로 예방하고 수사하기 위해서 암호키의 위탁을 의무화해야 한다고 주장한 반면 프라이버시 보호를 우선시하는 학자와 전문가들은 프라이버시 보호를 위해서는 국민들이 암호키를 자유롭게 사용할 수 있어야 하며 강제적인 키 위탁은 어떤 경우에도 수용될 수 없다고 주장하였다(Waters, 2001).

지난 8월 지리산의 조난객이 신속하게 구조되지 못하여 생명을 잃은 사건이 발생하면서 통신비밀보호법의 엄격한 운용이 논쟁의 대상이 되었다. 당시에 119(소방방재청)가 통신 사업자에게 이동전화 위치정보을 요청하였지만 통신비밀보호법을 근거로 협조를 거절하였기 때문이다. 그 후 정보통신부는 사전에 서비스 가입자의 동의가 있는 경우 119와 같은 긴급구조기관에게는 이동전화 위치정보를 제공할 수 있도록 했다(디지털타임스, 04/09/24).

이상에서 보듯이 프라이버시와 다른 가치와의 관계는 복합적이다. 한편으로 테러리스트로부터 국가안보는 물론 개인의 생명과 재산을 보호하기 위해서 어느 정도 프라이버시를 제한받지 않을 수 없다. 다른 한편으로 프라이버시가 철저히 보호되어야 개인의 생명과 재산이 보호될 수 있다. 신용카드번호, 위치정보, 유전자정보 등은 물론이고 주민등록번호나 이동전화번호도 개인의 생명이나 재산을 위협하는데 사용될 수 있다.

이 때문에 프라이버시는 어느 경우에도 보호되어야할 절대적인 가치로 간주되지 않는다. 실제로 프라이버시는 다른 가치와 충돌할 경우 양보되는 경우가 대부분이다.

PLPR(Privacy Law and Policy Reporter)의 부편집자인 Nigel Waters(2000)는 개인적 수준에서 대부분의 사람들은 프라이버시에 대해 다소 정신분열증적 태도를 갖고 있다고 지적한다. 우리 대부분은 평소에 프라이버시의 중요성을 인정하면서도 공중보건, 포르노그래피, 어린이 성추행, 납세사기 등과 같은 쟁점에 관해서는 프라이버시에 관한 평소의 입장을 쉽게 유보한다. 그래서 예컨대 청소년 성범죄자들에 대해서는 신상을 공개하는 사회적 처벌이 허용된다.

이렇듯이 프라이버시는 대단히 상황 의존적이기 때문에 프라이버시 보호는 정보주체의 개인적 선택과 결정에 크게 의존하지 않을 수 없다.

그런데, 이론적으로 개인적 선택은 프라이버시 문제에 대한 손쉬운 해답이 되겠지만, 현실

적으로 ‘선택’은 실현되지 않고, 실현되더라도 형식적이 되는 경우가 많다. 적지 않은 사람들에게 자신의 개인정보는 관리할만한 가치가 있다고 생각되지 않고 또 다수의 사람들은 몇 가지 조건만 충족된다면 개인정보관리에 신경을 쓰고 싶지 않기 때문이다.

최근 불법적으로 수집한 신용카드번호를 가지고 온라인 쇼핑을 하여 카드가입자에게 손해를 입힌 사건, 노숙자들의 개인정보를 도용해서 휴대폰 가입을 하고 그들에게 막대한 빚을 지게 만든 사건 등이 보여주듯이 프라이버시 침해는 누구에게나 심각한 피해를 초래할 수 있다. 하지만 아직도 다수의 사람들은 개인정보를 관리해야할 필요성을 느끼지 않는다.

이상에서 논의한 프라이버시의 사회적 성격으로 볼 때 결국 프라이버시 보호란 프라이버시와 서로 충돌하는 다른 공익(혹은 사익) 사이의 균형을 찾는 일이 될 것이다.

1.4. 바람직한 입법 및 정책 수립 방향

우리는 프라이버시에 대한 이상의 검토로부터 다음과 같은 입법 및 정책수립 방향을 제시하고자 한다. 법안과 정책에는,

○ 무엇보다도 개인정보가 정보주체로서 개인의 소중한 자산임과 동시에 사회적으로 공유되어야할 가치라는 점이 반영되어야 한다.

○ 개인정보에 대한 궁극적인 권리가 정보주체에게 귀속됨이 반영되어야 한다.

○ 정보주체에게 풍부한 혜택이 돌아가는 한 정보공유를 적극 허용하되, 개인정보 데이터베이스의 소유자인 기업이나 기관의 데이터베이스 관리가 정보주체의 권익에 반하지 않도록 적절한 규제가 포함되어야 한다.

프라이버시는 공공부문에서는 하나의 시민적 권리로서 이해될 수 있으나, 민간부문에서는 소비자의 권익(rights and interests)으로 이해되는 것이 바람직하다. 따라서 국가는,

○ 공공부문의 경우 개인정보가 시민에 대한 국가기관의 감시(surveillance)와 억압에 이용되지 않도록 각 기관의 개인정보관리에 대한 감시(monitoring)와 규제를 철저히 시행한다. 그것은 정보주체, 곧 시민의 대표가 참여하는 민주적 절차여야 한다.

○ 민간부문의 경우 개인정보가 정보소유자에 의해 정보주체(대부분 소비자를 가리킨다)의 권익에 반하여 이용되지 않도록 기업이나 기관의 개인정보관리를 적절히 규제한다. 이에는 정부기관에 의한 규제 뿐 아니라 정보주체, 소비자단체, 사업자단체 등이 참여하는 자율규제도 포함된다.

○ 정보주체의 자기정보관리 능력을 높여주어야 한다. 즉, 정보주체의 자기정보결정권이 이념적 구호에 끝나지 않고 실제로 구현될 수 있는 PMS(Privacy Management System)와 같은 개념의 기술 개발을 적극 촉진해야 한다.

2. 개인정보보호를 위한 법률 및 제도

2.1. 개인정보 수집 및 이용의 제한 원칙의 강화

2.1.1. 개인정보관리의 필요성

정보사회에서 디지털화된 개인정보는 정보주체도 인식하지 못한 상태에서 정부나 기업의 수중에서 수집, 처리, 이용, 제공될 수 있게 되었다. 개인정보를 축적 처리하는 기관은 개인에 대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이다. 그리하여 이들 개인정보를 토대로 개인의 성향과 동태를 파악할 수 있다. 이것은 때로 특정 부류의 사람들에 대해 사회적 낙인을 가능하게 만들고, 이를 통해 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수 있다.

그러나 개인정보처리의 위험성만을 지나치게 강조해서 개인정보의 수집과 유통을 전면 금지시킨다면 그것은 곧 정부와 시장의 기능을 마비시킬 것이고, 심지어 시민사회도 제대로 기능할 수 없게 될 것이다. 정부의 역할이 커지면 커질수록 개인정보 수집 및 이용의 필요성은 늘어나게 된다. 예컨대, 효과적인 법집행, 복지체계의 효율적 이용, 조세포탈자의 추적, 국민보건의 증진 등 개인정보의 수집 및 이용을 통해 보다 효율적인 관리가 가능하다. 민간의 시장 또한 소비자의 개인정보를 수집·처리함으로써 자원배분의 효율성을 극대화하고 소비자에 대한 맞춤서비스를 제공할 수 있다.

여기서 개인정보처리의 위험성과 필요성 사이의 균형을 맞추는 일은 매우 중요한 과제라 하겠다. 그 균형추로서 기능하는 것이 '개인정보의 자기결정권'이라는 정보인권이다. 이를 통해 정보주체는 자신에 관한 정보가 누구에 의해 어떤 목적으로 어떻게 수집·이용·제공되는지를 명확하게 인식하고, 그러한 정보처리의 과정에 함께 참여할 수 있어야 한다. 이러한 점에서 개인정보관리의 원칙을 분명히 정립하는 것은 정보사회에서 인권 보장을 위한 첫걸음인 동시에 가장 핵심적인 요소라고 말할 수 있다.

특히 정보통신기술의 발달과 함께 심각한 사회문제로 대두되고 있는 개인정보 유출 문제의 시발점은 서비스 제공자의 무분별하고 과도한 개인정보 수집에 기인한다. 이용목적에 부합하는 최소한의 정보를 공정한 절차에 의해 수집한다면 개인정보 유출의 위험은 현저하게 감소될 것이다. 최소한의 정보를 수집하고 보유한다면 정보 유출의 범위 또한 최소화될 것이기 때문이다.

또한 개인정보 관리는 수집된 정보가 어떻게 이용되느냐의 문제를 핵심 사안으로 삼고 있다. 수집된 정보가 누구에 의해 어떤 목적과 용도로 어떻게 이용되는가에 의해 개인정보 관리에 관한 총체적인 평가가 좌지우지될 수 있기 때문이다. 개인정보의 제3자 공유 및 제공 문제나 보안 문제, 스팸(spam)이나 도·감청에 관한 문제 등도 궁극적으로는 개인정보의 이용 문제에 포함된다.

따라서 개인정보 수집 및 이용 단계에 해당되는 기본적인 원칙을 명확히 제시하여 개인정보 보호의 기반을 확고히 할 필요가 있다.

2.1.2. 사회적 쟁점 및 현안의 사례

정보의 수집 및 이용에서 개인정보 보호의 기본 원칙이 지켜지지 않아 발생하는 개인정보 피해가 사회적 문제로 비화되는 사례들이 점차 늘어나고 있다.

구분	2000년	2001년	2002년	2003년	계
신고	329	388	1,237	5,183	7,137
상담	1,706	10,776	16,719	12,594	41,795
신고대회				3,808	3,808
계	2,035	11,164	17,956	21,858	52,740

<표 1> 개인정보침해 현황
출처: 한국정보보호진흥원, 2004

한국정보보호진흥원에서 발간한 '2003년 개인 인터넷 이용자의 정보화 역기능 실태조사 보고서'에 의하면, 웹사이트를 이용하면서 자신이 제공한 개인정보를 통해 프라이버시를 침해당할 가능성에 대해서는 '약간 우려한다(49.3%)', '매우 우려한다(35.1%)'로 나타나 개인의 프라이버시 침해에 대한 우려의 수준이 매우 높은 것으로 조사되었다.

첫째, 정보의 수집 단계에서 정보주체의 의사에 반한 수집행위로서 동의 없는 개인정보수집, 동의 하에서의 과다한 정보수집, 동의철회에 대한 거부 및 아동으로부터의 개인정보수집 등을 들 수 있다.

2000년 '국내 27개 대표 인터넷 사이트의 개인정보 보호실태 조사결과'(함께하는 시민행동)를 보면, 정보의 수집목적 및 이용목적을 구체적으로 명시한 곳은 거의 없었다. 또한 사이트의 서비스 목적에 부합하지 않는 과다한 정보 수집이 이루어지는 것이 대부분이었다. 또한 2003년 1/4분기 '개인정보분쟁위원회'에 접수된 개인정보 피해구제 신청 845건 중 법정대리인의 동의 없는 아동의 개인정보수집 유형이 561건(66.4%)를 차지하여 가장 높은 비율을 보이고 있다.

더욱이 최근 특정 프로그램을 이용하여 무작위로 개인정보를 모으거나 크래킹(cracking) 등의 기술을 이용해 타인의 정보를 절도하는 등 정보주체의 동의 없는 정보 수집 사건이 빈번하게 발생하고 있다. 또한 국정감사 때마다 핵심 사안으로 부각되는 권력의 무분별한 도·감청 실태 또한 정보주체의 통제권을 무시한 수집이라고 볼 수 있다.

둘째, 정보의 관리나 저장 및 이용 단계에서 개인정보의 프로파일링(profiling), 목적달성 후에 개인정보의 파기거부나 계약불이행의 문제를 들 수 있다.

개인정보침해신고센터의 ‘2001년 6월 한 달간 개인정보보호 신고접수 및 처리현황’을 보면, 해당 월에 신고접수 사건은 총 1,573건이었으며 이 가운데 절반 이상인 ‘857건’이 타인 개인정보의 훼손·침해·도용에 관한 내용이었다. 그리고 개인정보침해신고센터에서 국내 인터넷사이트 300개를 대상으로 실시한 ‘제4차 인터넷 사이트 의무 고지사항 모니터링’ 결과 개인정보 수집 시 고지의무 가운데 ‘개인정보의 이용·보유기간’에 관한 고지율이 60%에 불과해 다른 항목 평균 고지율에 비해 상당히 낮았다.

셋째, 개인정보의 이전 단계에서 부정한 방법에 의한 위법한 거래로서 정보주체의 동의나 통지 없이 제3자에게 임의제공 또는 판매, 또는 개인정보의 불법적인 유출이나 공개행위를 들 수 있다. 이와 같이 상업적 목적으로 기존의 오프라인의 기업에서 보유하는 개인정보를 불법적으로 거래하고 있다.

2001년 11월, 회원의 동의 없이 7개월 동안 4만~1백50만 명의 이름, 주소, 주민등록번호, 전자우편 주소 등의 개인정보를 신용카드업체 및 보험회사에 팔아넘긴 혐의로 기소된 8개의 국내 유명전자회사 및 인터넷 회사의 직원들에게 법정 최고액의 벌금형이 내려졌다. 또한 개인정보침해센터의 ‘2001년 5월 한 달간 개인정보보호 신고접수 및 처리현황’을 보면, 해당 월에 신고 접수된 총 915건 가운데 동의 없는 제3자 제공 및 목적에 사용이 51건이었다. 이는 개인정보 침해사고의 20% 이상이 제 3자 정보 공유로 인해 발생하고 있음을 시사하고 있다.

2.1.3. 현행 법률 및 제도의 현황

2.1.3.1. 개인정보보호 관련 법·제도의 현황

국내에서 개인정보의 보호와 관련한 법률로는 공공부문에서는 ‘공공기관의 개인정보보호에 관한 법률’(이하 ‘공공기관개인정보법’이라 한다)이 있으며, 민간부문에서는 ‘정보통신망 이용촉진 및 정보호호 등에 관한 법률’(이하 ‘정보통신망법’이라 한다)이 일반법적 내용을 담고 있다.

그 외에 분야별 법률로 ‘신용정보의 이용 및 보호에 관한 법률’, ‘금융실명거래 및 비밀보장에 관한 법률’, ‘통신비밀법’ 등이 있으며, 그 외 개인정보 보호를 목적으로 하지 않는 법률들에도 개인정보 보호와 관련된 조항이 일부 포함되어 있다.

현행 ‘공공기관개인정보법’은 개인정보처리의 기본원칙이 잘 규정되어 있지만, 실질적인 면에서 많은 문제점을 안고 있는 것도 사실이다. 특히 공공부문에서는 많은 정부기관들이 매우 민감한 개인정보들을 체계적으로 검색할 수 있는 다양한 DB들을 구축하고 있고, 정부 내 개인정보DB는 공익이라는 관점에서 언제든지 용이하게 통합될 수 있는 가능성이 항상 존재한다. 더욱이 2001년에 제정된 「전자정부법」은 이들 개인정보를 공동이용하도록 의무지우고 있다(제21조). 뿐만 아니라, 우리나라는 전 국민을 대상으로 단일 체계의 표준개인식별자(universal identifier)로서 주민등록번호를 강제로 부여하고 있고, 이 주민등록번호를 중심으

로 하여 정부 내의 모든 개인정보DB가 구축되어 있다. 이를 바탕으로 매우 포괄적인 개인정보 통합관리시스템의 구축이 언제든지 가능하고 그에 따라 정부는 개인의 총체적인 인격상을 손쉽게 파악할 수 있는 상태에 있다.

민간부문에서 '정보통신망법'은 개인정보보호의 일반법적 내용을 담고 있지만, 정보통신서비스제공자, 학원 항공 여객 숙박 등 몇몇 제한된 분야를 중심으로 적용되고 있어 한계가 있다. 또한 이 법은 목적 자체가 정보통신망 이용 촉진과 네트워크 보안, 개인정보 보호라는 서로 다른 문제들을 하나로 엮고 있어서 일반법으로 기능하기에 문제가 있다.

민간부문에서 정보통신부문과 신용정보부문에서 개인정보 보호를 위한 법률이 마련되어 있지만, 그 외의 영역에서는 별도의 개인정보 보호 법률은 부재한 상태이다. 뿐만 아니라, 개인정보관리의 원칙이 명확하게 규정되지 않아 어떤 경우에는 오히려 개인정보의 수집 및 이용의 현실적 필요성과 사회적 활용을 원천적으로 봉쇄하는 결과를 빚기도 한다.

국내의 개인정보 보호법제는 분야별 입법체계를 갖고 있다고 볼 수 있는데, 이러한 법률체계는 몇 가지 문제점을 지니고 있다.

우선 개인정보 보호의 사각지대가 많다. 예컨대, 의료정보나 사회복지정보, 부동산거래기록 등의 경우 각 분야별 법률에 '비밀을 지킬 의무'라는 단 하나의 조항에 의해 보호되고 있을 뿐, 개인정보의 보호를 위한 별도의 구체적인 절차와 규정은 없는 상태이다. 특히 정보주체의 다양한 권리들이 보장되지 못하고 있다. 또한 앞서의 개인정보보호 법률들이 주로 온라인상의 개인정보 보호 문제만을 다루고 있어, 오프라인상에서도 발생하는 다양한 개인정보 침해 문제에 대한 대처가 미흡한 실정이다.

현재 '공공기관의 개인정보보호에 관한 법률'은 2003년 8월 개정안이 예고된 상태이다. 그리고 민간부문의 개인정보에 관한 일반 법률을 염두에 두고, 정보통신부의 주도 하에 '민간부문의 개인정보에 관한 법률'(안)이 제정 논의 중이다. 그러나 이 법률안은 특히 개인정보보호기본법이 제정 논의 중인 상태에서 많은 비판을 받고 있다.

2.1.3.2. 개인정보보호 관련 법률의 주요 내용

(1) 공공부문 개인정보의 수집 및 이용 제한 원칙

1) 수집제한의 원칙

·사상, 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보는 수집 자체가 금지된다. 다만, 동의가 있거나 다른 법률에서 명시적으로 수집을 허용하고 있는 경우에는 수집 가능하다. (제4조)

·공공기관은 소관업무 수행에 필요한 범위 안에서 개인정보화일을 보유할 수 있다. (제5조)

- 보유절차: 공공기관의 장이 개인정보화일을 보유하고자 하는 경우에는 보유목적, 보유기관, 수집방법, DB수록항목 등의 사항을 행정자치부 장관에게 통보하고, 이를 연 1회 이상 관보에 게재하여 공고한다. (제6조, 제7조) (다만, 공공기관의 적정한 업무수행을 현저하게 저

해할 우려가 있다고 인정되는 때에는 대통령령이 정하는 바에 따라 당해 개인정보화일에 기록되어 있는 항목의 전부 또는 일부를 공고하지 아니할 수 있다.)

- 예외사항: 국가의 안전 및 외교상의 비밀 기타 국가의 중대한 이익에 관한 사항을 기록한 개인정보화일, 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보화일, 조세범처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한 사항을 기록한 개인정보화일, 컴퓨터의 시험운영을 위하여 사용되는 개인정보화일, 1년이내에 삭제되는 처리정보를 기록한 개인정보화일, 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보화일, 대통령령이 정하는 일정한 삭이내의 정보주체를 대상으로 하는 개인정보화일, 기타 이에 준하는 개인정보화일로서 대통령령이 정하는 개인정보화일

- 보유기관은 위 공고사항을 기재한 개인정보DB대장을 작성·비치해야 한다.

2) 이용제한의 원칙

· 목적구속의 원칙: 사전에 공시된 개인정보DB의 보유목적이 아닌 다른 목적으로 개인정보를 이용하거나 제공하는 것을 금지한다. (제10조)

- 예외사항: 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우, 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, 통계작성 및 학술연구등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우, 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, 범죄의 수사와 공소의 제기 및 유지에 필요한 경우, 법원의 재판업무수행을 위하여 필요한 경우, 기타 대통령령이 정하는 특별한 사유가 있는 경우. (법 제10조 제2항 본문 각호)

- 처리절차: 보유기관은 처리정보를 수령한 자에 대하여 사용목적·사용방법 기타 필요한 사항에 대하여 제한을 하거나 처리정보의 안전성확보를 위하여 필요한 조치를 강구하도록 요청하여야 한다. 보유기관은 정보주체의 권리와 이익을 보호하기 위하여 필요하다고 인정하는 때에는 처리정보의 이용을 당해 기관내의 특정부서로 제한할 수 있다. 처리정보를 이용하는 기관은 제공기관의 동의없이 당해 처리정보를 다른 기관에 제공하여서는 안된다.

3) 정보주체의 권리

. 열람 요구: 정보주체는 개인정보화일대장에 기재된 범위안에서 서면으로 본인에 관한 처리정보의 열람을 청구할 수 있다. 이에 보유기관은 15일이내에 열람할 수 있도록 하여야 한다.

- 처리정보의 열람제한: 다음 사항에 해당하는 경우에는 그 사유를 통지하고 당해 처리정보의 열람을 제한할 수 있다. 당해 업무의 수행에 중대한 지장을 초래하는 경우, 조세의 부

과·징수 또는 환급에 관한 업무, 교육법에 의한 각종 학교에서의 성적의 평가 또는 입학자의 선발에 관한 업무, 학력·기능 및 채용에 관한 시험, 자격의 심사, 보상금·급부금의 산정등 평가 또는 판단에 관한 업무, 다른 법률에 의한 감사 및 조사에 관한 업무, 기타 대통령령이 정하는 업무

. 정정 요구: 정보주체는 서면으로 처리정보의 정정을 청구할 수 있다. 이에 보유기관은 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다.

. 행정심판 청구: 정보주체는 위 청구사항에 대해 공공기관이 행한 처분에 의해 권리 또는 이익을 침해받을 경우 행정심판을 청구할 수 있다. 또한 대통령령이 정하는 바에 따라 대리청구가 가능하다.

(2) 민간부문 개인정보의 수집 및 이용 제한 원칙

1) 개인정보의 수집제한의 원칙

. 동의원칙: 이용자의 개인정보를 수집하는 경우 당해 이용자의 동의를 얻어야 한다. (제22조 제1항)

- 고지의무: 동의를 얻고자 하는 경우 미리 다음 사항을 고지하거나 이용약관에 명시해야 한다. (제22조 제2항) 개인정보관리책임자의 성명·연락처 등, 수집·이용목적, 제3자 제공시 제공받는 자·제공목적·제공할 정보내용, 이용자의 권리·행사방법, 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 운영 및 그 거부에 관한 사항(2004.1.29 신설)

. 수집범위의 제한:

-사상·신념·과거의 병력 등 개인의 권리 이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보는 수집 자체가 금지된다. 다만, 이용자의 동의가 있거나 다른 법률에 의해 수집대상 개인정보가 명시되어 있는 경우에는 가능하다. (제23조 제1항)

- 정보통신서비스 제공에 필요한 최소한의 개인정보를 수집하여야 한다. 또한 필요한 최소한의 정보 외의 개인정보를 제공하지 않는다는 이유로 서비스의 제공을 거부해서는 안된다. (제23조 제2항) 개인정보를 수집하는 경우 필수항목과 선택항목으로 구분하여 이용자가 선택적으로 자신의 개인정보를 제공할 수 있도록 해야 한다.

-만 14세 미만의 아동으로부터 수집할 때에는 부모의 동의를 받아야 함

- 위반시 1천만원 이하의 과태료

2) 개인정보의 이용 및 제공 제한의 원칙

. 목적구속의 원칙: 정보통신서비스제공자가 사전에 고지된 범위 또는 이용약관에 명시한 범위를 넘어 이용하거나 제3자에게 제공하는 것을 금지한다. (제24조 제1항)

- 예외사항: 다만, 이용자의 동의가 있거나 다음의 경우에는 예외로 한다. 서비스 제공에 따른 요금정산에 필요한 경우, 통계작성이나 학술연구와 시장조사 등 목적으로 특정 개인을 알

아볼 수 없는 형태로 가공하여 제공하는 경우, 다른 법률에 특별한 규정이 있는 경우

. 이용자의 동의가 있거나 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제공받은 목적외의 용도로 이용하거나 제3자에게 제공하는 것을 금지한다. (제24조 제2항)

- 고지의무: 이용자의 동의를 얻고자 할 때는 미리 이용자에게 개별적으로 서면, 전자우편, 전화 등으로 고지해야 한다. (이때 '개별적 동의'의 의미는 이용자 개개인의 동의 여부를 확인해야 하는 것으로, 서비스제공자의 편의를 위해 일괄적으로 동의 여부를 묻는 전자우편을 발송한 후 거부의사표시가 없을 경우 동의로 간주한다는 등의 '소극적 동의' 방식은 개별적인 동의로 볼 수 없다.)

- 이를 어길 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

. 영업양도등 개인정보의 이전: 영업의 양도, 합병, 상속 등으로 그 권리와 의무를 이전하는 경우 이용자에게 통지해야 한다.

- 통지방법: 서면과 전자우편으로 통지하거나, 인터넷 홈페이지 첫화면에 30일 이상 공지할 수 있다. (영업양도 및 합병 등의 경우에 일일이 이용자의 동의를 얻도록 하는 것은 현실적으로 많은 시간과 비용을 요하고, 기업결합 자체를 불가능하게 할 수도 있으므로 사업자의 입장을 고려하여 개인정보의 제3자 제공에 대한 예외규정을 두고 있다.)

. 개인정보의 보유 제한:

- 개인정보의 수집목적 또는 제공받은 목적을 달성한 때는 개인정보를 지체없이 파기해야 한다. 다만, 법령의 규정에 의해 보존할 필요성이 있는 경우, 보유기간을 미리 이용자에게 고지하거나 명시한 경우, 개별적으로 이용자의 동의를 얻은 경우 등의 경우에는 예외로 한다.

- 해지고객의 개인정보를 보유하고자 하는 경우 보유기간, 보유목적, 보유하는 개인정보 항목, 동의철회 등 이용자의 권리사항을 해지고객에게 구체적으로 고지하고 서면을 통해 별도의 동의를 받아야 한다. 이 경우에도 해지고객의 요청이 있는 경우 개인정보를 지체없이 파기해야 한다.

3) 이용자의 권리

. 동의철회: 이용자는 언제든지 동의를 철회할 수 있다. (제30조)

. 열람, 정정 요구: 이용자는 자신의 개인정보에 대한 열람 또는 개인정보를 이용하거나 제3자에게 제공한 내역을 요구할 수 있고, 자신의 개인정보에 오류가 있는 경우에는 그 정정을 요구할 수 있다. (개인정보이용명세청구권 신설 2004. 1.29) 정보통신서비스제공자는 이용자의 동의 철회가 있거나, 열람 내역과 정정 요구를 받은 경우 지체없이 필요한 조치를 취해야 한다.

. 손해배상청구권: 이용자는 서비스제공자등이 개인정보보호에 관한 사항을 위반한 행위로 손해를 입은 경우에는 손해배상을 청구할 수 있다. 이 경우 해당 서비스제공자는 고의 또는 과실이 없음을 입증하지 않으면 그 책임을 면할 수 없다. (제29조)

공공기관의개인정보보호에관한법률	
제정일	1994. 1. 7(공포), 1995. 1. 8(시행), 일부개정 1999. 1. 29
적용분야	공공부문
공공기관의 범위	국가행정기관·지방자치단체·학교·정부투자기관·특수법인
보호대상	컴퓨터에 의하여 처리되는 생존하는 자연인의 개인정보 (단, 개인정보DB에 수록된 개인정보만 보호)
적용제외 개인정보	·통계법에 의해 수집되는 개인정보 ·국가안전보장 목적으로 수집되는 개인정보
수집제한의 원칙	·사상신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보는 수집 자체가 금지됨(단, 동의가 있거나 다른 법률에서 명시적으로 수집을 허용하고 있는 경우에는 수집 가능) ·소관업무 수행에 필요한 범위 안에서 개인정보DB 보유 가능 ·보유절차: 공고사항(보유목적·수집방법·DB수록 항목 등)을 행정자치부 장관에게 사전통보 -> 연 1회 이상 관보게재 – 8가지의 광범위한 예외를 인정하고 있음 ·보유기관: 위 공고사항을 기재한 개인정보DB대장을 작성·비치
목적구속의 원칙	·원칙: 사전에 공시된 개인정보DB의 보유목적이 아닌 다른 목적으로 개인정보를 이용하거나 제공하는 것을 금지 ·예외: 8가지의 광범위한 예외를 인정하고 있음 – 소관업무 수행을 위해 이용할 상당한 이유가 있는 경우 – 범죄의 수사와 공소의 제기 및 유지에 필요한 경우 – 기타 대통령령이 정하는 특별한 사유가 있는 경우 등
시스템공개의 원칙	·원칙: 개인정보DB 내역을 관보게재, 개인정보DB대장 작성·비치 ·예외: 상당한 DB가 관보게재·DB대장수록·일반인의 열람에서 제외, 통계목적·국가안전보장목적의 DB는 아예 이 법의 적용을 받지 않음
정보정확성의 원칙	·보유기관의 장은 처리정보의 정확성·최신성 확보 노력
보안의 원칙	·보유기관의 장은 안전성확보에 필요한 조치를 강구하여야 함(선언규정) ·개인정보취급자는 개인정보의 누설 또는 부당목적 이용이 금지됨(형사처벌)
참여의 원칙	·정보주체는 개인정보DB에 기재된 범위 안에서 서면으로 열람·정정을 청구할 수 있음 ·일정 업무의 경우 업무수행에 중대한 지장이 있을 때 열람제한 가능
감독의 원칙	· 행정자치부가 법상의 집행기관이지만, 위법사실에 대한 감시·감독·집행의 권한과 기능을 가지지 못함.

〈표 2〉 ‘공공기관개인정보법’의 개인정보보호의 주요 내용

정보통신망이용촉진및정보보호등에관한법률	
제정일	1999. 2. 8(개인정보보호규정 신설), 1999. 7. 1(시행), 전문개정 2001. 1. 16 일부개정 2004.1.29
적용분야	민간부문 (온라인 일반 및 오프라인 일부)
규율대상기관	·영리목적의 정보통신서비스제공자 – 전기통신사업자 및 온라인정보제공·매개자 ·오프라인 민간사업자 – 여행업자, 호텔업자, 항공운수사업자, 학원·교습소, 기타 정보통신부령으로 정하는 자
보호대상	규율대상기관이 수집하는 생존하는 자연인에 관한 일체의 개인정보
수집제한의 원칙	·이용자의 개인정보 수집 시 사전에 동의를 얻어야 함 (22조) ·고지의무: 동의를 얻기 전에 일정 사항을 고지 또는 이용약관에 명시 – 개인정보관리책임자의 성명·연락처 등, 수집·이용목적, 제3자 제공시 제공받는 자·제공목적·제공할 정보내용, 이용자의 권리·행사방법 ·사상·신념·과거의 병력 등 개인의 사생활을 현저하게 침해할 우려가 있는 개인정보는 수집 자체가 금지됨(단, 이용자의 동의가 있는 경우에는 가능) ·서비스제공에 필요한 최소한의 개인정보를 수집하여야 함 ·만 14세 미만의 아동으로부터 수집할 때에는 부모의 동의를 받아야 함 ·위반시 시정명령, 과태료 또는 형사처벌
목적구속의 원칙	·원칙: 사전에 고지된 범위를 넘어 이용하거나 제3자에게 제공하는 것을 금지 ·예외: 이용자의 별도의 동의가 있거나 요금정산에 필요한 경우 ·영업의 양도·합병·상속의 경우 이용자에게 통지의무 ·수집목적을 달성한 때에는 당해 개인정보를 지체 없이 파기해야 함 ·위반시 시정명령, 과태료 또는 형사처벌
보안의 원칙	·처리기관은 안전성확보에 필요한 기술적·관리적 조치를 강구하여야 함 ·개인정보취급자는 개인정보의 훼손·침해 또는 누설을 금지함 (형사처벌)
참여의 원칙	·정보주체는 언제든지 동의를 철회할 수 있음 ·열람 및 정정청구권 인정. 처리기관은 이에 필요한 조치를 취하여야 함. ·손해배상청구권 인정. 고의 또는 과실에 대한 입증책임을 전환함.
감독의 원칙	·정보통신부가 위법사실에 대한 감시·감독·집행의 권한과 기능을 가짐. ·개인정보분쟁조정위원회가 분쟁조정기능 수행 ·한국정보보호진흥원의 개인정보침해신고센터가 고충처리·모니터링 수행

〈표 3〉 ‘정보통신망법’상의 개인정보보호의 주요 내용

2.1.4. 개인정보보호 법률 및 제도의 문제점

(1) 목적구속원칙의 형해화 가능성

우선 공공기관개인정보법은 다른 법률에 의해 보유목적 이외의 목적으로 보유기관 내부에서 이용하거나 제3자 제공을 허용하고 있는 경우에는 그에 따르는 것으로 되어 있다(제10조 제1항). 따라서 공공기관개인정보법이 선언하는 목적구속의 원칙은 다른 법률에 의하여 얼마든지 훼손될 수 있는 것이다. 또한 이 법은 예외사유를 광범위하게 인정하고 있다. 이러한 예외의 경우에는 사전에 공시된 보유목적에 구속되지 않고 얼마든지 다른 용도로 수집기관 내부에서 활용할 수 있으며, 또 정보주체의 동의를 받거나 통지함이 없이 임의로 제3자에게 제공할 수 있도록 되어 있다. 나아가, 2001년 시행된 전자정부법은 이들 예외의 경우에 보유하고 있는 처리정보를 공동 이용하도록 각 행정기관에 의무지우고 있다. 이처럼 광범위한 예외의 인정은 목적구속의 원칙을 무의미하게 만들 가능성을 지니고 있다.

정보통신망법의 경우에도 개인정보의 수집과 관련하여 이용자의 동의를 필요로 한다고 규정하고 있지만, 예외 규정의 범위가 매우 모호하고 포괄적이라는 문제가 있다. 특히 “정보통신서비스 이용계약의 이용을 위하여 필요한 경우” 라는 규정은 그 적용에 있어 서비스제공사업자의 자의성이 개입될 우려가 있다.

(2) 정보주체의 선별적 동의권 불인정

현행법은 일괄동의 방식을 채택하고 있어서 수집제한의 원칙과 목적구속의 원칙을 우회할 가능성이 있다. 따라서 ‘이용자의 동의’에 차별적인 성격을 부여하는 것이 필요하다. 특히 민간부문의 경우 서비스제공사업자가 서비스제공목적과는 전혀 연관성이 없는 민감한 개인정보를 다른 성명, 전화번호, 주소 등과 같은 일반적인 개인정보들과 동일한 수준에서 동의를 요구하는 방식을 규정함으로써 오히려 입법목적과 상반된 사실상의 수집을 가능하게 할 우려가 있다. 즉 민감한 개인정보의 경우 다른 일반적인 개인정보와 같은 포괄적 동의가 아닌 별도의 동의 절차를 통한 명확한 동의를 구하도록 동의의 수준에 차별을 둘 필요가 있다.

(3) 제3자 이전 시 개인정보보호 규정의 미비

공공기관정보보호법은 정보주체 이외의 제3자에게 개인정보를 제공하는 경우 정보주체의 동의를 받거나 통지하도록 요구하고 있지 않다. 현행법은 위 보유목적을 넘어선 제3자 제공에 대한 절차를 달리 규정하고 있지 않다. 다만, 법 시행령에서 보유기관이 임의로 제공할 수는 없고, 수령기관이 그 이용목적 및 이용하고자 하는 처리정보의 범위를 명시하여 보유기관의 장에게 문서로 요청하도록 하고 있다. 따라서 현행법상의 제3자 제공의 절차는 정보주체의 인식명

확성이라는 자기결정권을 심각하게 제약하고 있다고 볼 수 있다.

한편, 정보통신망법에서는 합병이나 영업양도에 의하여 이용자의 개인정보가 제3자에게 이전하는 경우에 사전 동의를 받는 대신 통지만을 하도록 규정하고 있다(26조). 그러나 통지 시기에 대해서는 아무런 규정이 없어 사전통지와 사후통지 모두 가능한 것으로 해석될 수 있다. 이는 이용자가 동의한 범위를 벗어난 것일 뿐만 아니라, 이용자들의 개인정보를 보관, 관리, 이용하는 주체가 변경되는 경우이기 때문에, 자신의 개인정보가 제3자에게 이전되는 것을 원치 않는 이용자 입장에서는 그의 권익을 이미 침해당한 것과 다름없는 결과를 가져온다.

또한 개인정보를 보유 활용하는 서비스 제공자에게서 개인정보 취득 경위에 대한 설명이 전혀 없는 경우가 많다. 다만 스팸메일의 경우에 한해서 정보취득 경위 설명 규정이 마련되어 있을 뿐이다. 이 때문에 개인정보가 정상적으로 유통된 것인지, 불법적으로 유통된 것인지 확인하기 어렵고, 따라서 정보주체들이 권리 구제를 위한 적절한 행동에 나서는 것은 매우 어려워지고 정보유출에 대한 우려만을 증폭시킬 뿐이다.

(4) 개인정보 보호의 실효성 문제

사실 현행법률들의 경우 외국 사례에 비추어보아도 개인정보의 수집 및 이용제한의 원칙은 잘 마련되어 있다고 볼 수 있다. 그러나 여전히 개인정보침해 사례가 해마다 늘어나고 있고 개인정보 보호의 실효성이 떨어지는 문제점이 있다. 이것은 단지 법 조항의 명시적 기술의 문제만도 아니고, 처벌조항의 강화만으로도 해결할 수 없다. 특히 처벌조항의 강화 방안은 많은 반발이 따를 수 있고, 정부기구가 모든 기업들을 다 모니터링하거나 감독할 수 없기 때문에 실효성의 문제가 발생할 수 있다. 국가가 개인정보의 보호 및 관리를 위한 모든 역할을 다 하는 데는 한계가 있다. 감독 및 집행기구의 역할은 정보기술의 발달에 의해 대응의 어려움이 있고 수많은 기관들 및 기업들을 모두 모니터링하는 것은 현대사회에서 거의 불가능에 가깝기 때문에, 그 역할과 기능은 한정될 수밖에 없다.

따라서 시민사회 및 기업의 자율규제에 의해 개인정보 보호의 역할이 보완될 필요가 있다. 첫째, 시민들의 프라이버시 의식을 제고하는 방향으로 개선되어야 하고, 둘째, 시민사회의 감시기능과 함께 독립적인 프라이버시 위원회의 기능을 강화하는 방안을 검토할 필요가 있다.

2.1.5. 해외 사례의 검토

OECD는「프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인」(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980)을 통해 회원국에 대하여 개인정보 침해의 우려가 있는 공공부문과 민간부문에 있어서 컴퓨터에 의한 개인데이터의 처리 등을 포함하는 개인정보보호법의 제정을 촉구하고 있다. 특히 수집제한의 원칙

(Collection Limitation Principle), 정보정확성의 원칙 (Data Quality Principle), 목적구체성의 원칙 (Purpose Specification Principle), 이용제한의 원칙 (Use Limitation Principle) 등 8대 원칙을 규정하고 있다. 개인정보의 수집 및 이용의 기본 원칙을 규정하는 데 있어서 이러한 가이드라인은 역사적으로 중요한 의미를 지닐 뿐만 아니라, 현재에도 유용한 방침이 되고 있다.

유럽연합이사회는 1981년에 제정한 Council of Europe Convention on Privacy 협약에서 데이터보호의 기본원칙을 정하고 있다. 개인데이터는 적법하고 공정하게 수집, 처리되고, 특정하고 적법한 목적으로 저장되며, 그 목적에 부합하지 않는 방법으로 사용하지 못한다. 그리고 저장 목적을 초과하는 기간 동안 보유할 수 없다. 또한 인종과 정치신념, 성생활이나 형벌기록과 같은 민감한 개인데이터를 국내의 적절한 보호장치가 없이 자동처리를 금한다고 정하고 있다.

유럽연합은 1995년에 European Union Data Protection Directive에 의해서 1998년까지 회원국의 프라이버시에 관한 국내입법을 동 협약의 수준으로 상향조정을 결정하여 오늘날 유럽연합의 전체 회원국은 프라이버시보호입법을 시행하고 있다. 이 EU 지침은 프라이버시 보호와 유럽연합 국가 내에 정보의 자유로운 흐름을 제한하는 것을 방지하고자 하는 두 가지 목적을 명시하고 있다.

프라이버시 보호에 관하여 유럽국가들은 포괄적인 입법을 통해 행정기관에 의한 감시나 독립적인 기구를 설치하여 개인정보의 취급을 통제하며, 이를 위반할 시 강력한 집행수단을 동원하고 있다.

프랑스의 정보처리자유에 관한 법률은 공공기관이 법률에 명시되지 않은 개인정보 파일을 축적하고자 할 때는 정보처리와자유위원회의 허가를 받아야 하며, 민간의 경우에도 위원회에 신고를 하도록 되어 있다. 또한 정확성 유지의 원칙을 엄격하게 적용하고 있으며, 법정 저장기간을 초과하여 개인정보를 보유하는 것을 금지하고 있다. 그 외에 정보수집자에게는 민감한 정보의 제외, 안정성 확보의 의무를 규정하고 있으며, 정보주체의 권리로서 동의권, 고지받을 권리, 수집 여부를 확인할 권리, 열람 정정 삭제 청구권, 피해를 보상받을 권리 등을 인정하고 있다.

독일의 연방정보보호법은 정보보호책임자의 지정을 명문화하고 있다는 점이 특징적이다. 개인정보수집자들은 수집하는 개인정보를 정보보호감독관에게 등록하도록 규정하고 있다. 개인정보와 관련하여 규정된 정보주체의 권리는 양도불가능함을 명문화하고 있으며, 정보주체의 권리로서 고지 및 동의권, 열람 정정 삭제 청구권을 규정하고, 정보수집자의 의무로 목적 외 사용 금지를 규정하고 있다.

영국의 데이터보호법은 동의권이 분명하게 인정되지 않고 있다. 대신 민감한 정보의 수집을 금하고 있으며, 불필요하게 오랫동안 개인정보를 보유하여 정보주체에게 불이익을 주는 것을 금지하고 있다. 또한 직접 마케팅 목적으로 개인정보를 사용하려고 할 때 정보주체가 거부권을 행사할 수 있도록 규정하고 있다. 그 외 정보주체의 권리로 열람 정정 삭제 청구권과 피해보상

을 받을 권리를 규정하고, 정보수집자의 의무로 수집 목적 제시와 데이터감독관에 대한 신고 의무를 규정하고 있다.

미국의 프라이버시법은 정보수집에 있어 정보주체의 동의권과 고지받을 권리, 열람 정정 삭제 청구권 및 보상받을 권리 등을 명시하고 있으며, 정보수집자의 의무 사항으로 수집에 관한 현황 공개를 규정하고 있다. 그러나 목적 명확성, 안정성 확보, 정확성 유지 등의 원칙등은 명시하지 않고 있는 상태이다. 또한 이 법은 연방 공공기관에만 적용되며, 민간영역에 적용되는 일반법이 없다.

프랑스, 영국, 스웨덴에서는 정부규제방식을 채택하고 있으며, 독일은 양자의 절충형을 취하고 있다. 프랑스는 국가정보자유위원회, 영국은 데이터보호등록관, 스웨덴은 데이터감독위원회, 독일은 연방데이터담당관을 두고 있다. 이들 감독기구에서는 첫째, 정보파일의 신고 및 등록의 접수, 심사, 허가. 둘째, 개인정보의 수집과 이용 관리에 대한 조사, 지도, 감독 및 위반시 시정명령 및 사법기관에의 고발. 셋째, 개인정보보호제도의 발전을 위한 연구, 보고, 조언 등의 기능을 한다.

반면에 미국은 행정감시기구를 설치하지 않고 업계의 자율규제를 허용하거나 정보주체인 개인에게 사법적 구제수단을 부여함으로써 프라이버시를 보호하려는 방식을 취하고 있다. 미국 정보정책위원회 보고서(1995.6.)는 '개인정보의 제공 및 이용에 관한 원칙'에서, 개인정보의 이용이 사회에 가져다 주는 이익을 중요한 요소로 꼽고 있으며, 프라이버시는 절대적인 것이 아니라 법적 책임 필요성, 표현의 자유, 적법한 법집행 행위의 필요성, 기타 다른 법률로써 요구되는 사회적 이익 등과 비교하여 균형 맞추어야 함을 인정하고 있다. 특히 통지 및 동의라는 기본적 요건을 충족시키기만 한다면 개인과 정보이용자 사이의 '계약에 의한 프라이버시의 보호' 방식을 더 선호하고 있다.

일본의 통산성 가이드라인(1997.1.)은 '충분한 수준의 개인정보보호'가 보장될 경우에 한하여 개인정보를 국가로 유출할 수 있도록 하고 있다. 첫째, 사회적 차별 요인이 되는 '특정의 민감한 정보'를 '인종 및 민족, 가문 및 본적, 종교, 정치적 견해 및 노동조합에의 가입여부, 보건의료 및 성생활' 등 구체적으로 예를 들어 규정하고, 그러한 민감한 개인정보의 수집, 이용, 제공의 원칙적 금지를 명시하고 있다. 둘째, 정보주체에 대한 문서에 의한 통지 등 개인정보의 수집, 이용 및 제공시 요건을 명확히 하였다. 셋째, 개인정보의 정정, 삭제권의 명시와 이 권리행사에 대한 기업측의 대응규정을 명시하였다. 그러나 이것은 행정부의 지침으로서 행정지도가 갖는 한계가 있다는 점과 개인정보 침해에 대한 벌칙이 없기 때문에 실효성을 확보하는 데 어려움이 있다.

2.1.6. 종합 대안

(1) 정보주체의 자기결정권 강화 방안

현대사회에서 국가가 ‘정보보호의 관점’에서 정보주체 개개인을 대신하여 개인정보 권리를 지켜주는 것은 한계가 있다. 시민단체의 역할 역시 공익적 입장에서 문제를 판단하고 해결하기 때문에 개인의 개별적 이익을 일일이 보장하기가 어려운 점이 있다. 따라서 개인정보의 보호를 위해서는 정보주체의 자기정보결정권이 핵심적이라 할 수 있다. 특히 자기 정보가 어떻게 수집, 이용, 가공, 제공되는지 등 정보처리과정을 모티터링할 수 있고 그 과정에 적극적으로 개입할 수 있어야 한다.

개인정보의 수집 및 이용 시 개개의 목적 혹은 목적변경 사항에 대해 부분적으로 동의를 거부할 권리를 최대한 보장할 필요가 있다. 특히 공공기관개인정보법에는 컴퓨터 네트워크 결합 등에 의한 개인정보통합을 금지하거나 규제하는 취지의 장치가 마련되어 있지 않으며, 오히려 전자정부법에 의하여 공공기관 간에 정보의 공동이용을 의무화하고 있다. 문제는 개인의 명확한 인식이나 동의 없이 이러한 정보 공유가 가볍게 처리되고 이에 대한 규제 조항도 미비한 상태라는 점이다.

민간부문에서도 급변하는 경제 상황에서 전략적 제휴나 기업의 합병 매각 등의 형태로 서비스제공자가 서로의 정보를 공유하거나 이전하는 경우가 늘어나고 있다. 하지만 현행법에는 개인정보의 제3자 이전이 정보주체의 명확한 인식과 사전 동의에 의해서가가 아니라 형식적인 통지만으로 가능하도록 규정하고 있다. 현행법은 동의에 대해 별도로 정의하고 있지 않다. 그나마 ‘개인정보보호지침’의 규정은 구체적이지 못할뿐더러 법적 효력을 제대로 발휘하지 못하기 때문에 현행 법률 내에 동의에 대한 적절하고 명확한 정의가 규정될 필요가 있다.

서비스제공자가 다수의 이용자를 상대로 동의를 구하는 방법은 이용자의 의사가 반영되는 수준에 따라 ‘적극적인 동의’와 ‘소극적인 동의’로 분류할 수 있다. 서비스제공자는 고지하는 내용에 따라 동의의 방법을 결정해야 하며, 정보의 제 3자 제공 및 공유의 문제와 같은 민감한 사안은 반드시 이용자의 적극적인 동의를 구할 필요가 있다.

(2) 공공기관 개인정보처리 현황보고의 인터넷 공개 방안

현재 공공기관에서 개인정보처리 과정에 문제가 있을 경우, 개별적으로 개인정보침해에 대한 행정심판을 요구하거나 혹은 시민단체등을 통해 소송을 제기함으로써 공공기관의 개인정보 보호조치에 대한 감시와 평가가 이루어지고 있다고 할 수 있다. 그러나 이것은 사후적이고 개별적이어서 그 실효성에 문제가 있다. 따라서 보다 적극적이고 사전적인 감시와 평가 방법을 개발할 필요가 있다. 특히 개인정보처리 과정에 대한 민원제기가 어떻게 처리되는지를 실시간으로 보여주는 것은 공공기관의 개인정보 보호에 대한 민감성을 높이고 구속력을 부여할 수 있는 좋은 장치가 될 것이다.

현재 개인정보처리 업무 현황 등을 행정자치부에 보고하도록 되어 있는 규정을 보다 강화하여, 각 해당기관별로 자신의 인터넷 홈페이지에 주기적으로 게시하고, 이에 대한 총괄 및 종

합적인 통계 업무는 주무부서인 행정자치부 홈페이지에 게시하도록 하는 방안을 제시할 수 있다. 이를 통해 시민사회에 의한 공개적인 감시와 평가가 이루어짐으로써, 추후 공공기관들이 보다 세심하고 철저한 개인정보관리의 방향으로 나아갈 수 있는 계기가 될 수 있다.

(3) 민간부문의 자율적 규제 및 프라이버시 기술 개발 방안

민간부문에서의 개인정보처리 과정은 다방면에서 이루어지고 있고 점차 방대한 규모로 늘어나는 추세여서, 어떤 한 기관이 모든 과정을 모니터링하고 감독할 수 있기에는 많은 한계를 가지고 있다.

미국의 경우에는 민간부문을 감독하는 별도의 행정감시기구는 없으며, 업계의 자율규제가 이루어지고 있다. 산업별로 자체 규제기구가 있어 공동의 기준 설정 및 공동 규제를 강화하고 있는 것이다. 공동 규약의 작성에는 기업뿐만 아니라 국가와 이용자가 함께 모여 공동의 안을 마련해야 할 것이다. 여기에 더하여 기업이 공동 출연하여, 프라이버시 관리 기술을 개발하는 방안을 적극 모색해야 할 것이다. 물론 기업자율로만은 개인정보 보호가 충분치 않고 제대로 감시가 이루어지 않을 수 있기 때문에, 여기에는 국가가 감독하고 지원하는 체계로 뒷받침될 필요가 있다. 특히 우리나라의 경우 자체 공동기구를 마련할 사업자단체의 발달이 지체되어 있는 상태이기 때문에, 이러한 자율 규제 방안이 제대로 적용될 수 있을지는 미지수이다. 따라서 특히 정보기술 및 인터넷 사업 영역에서 당분간 국가가 사업자단체에 대한 인큐베이터의 역할을 담당함으로써 이러한 자율규제의 기반을 마련하는 것이 필요하다.

(4) 개인정보 보호 및 감독을 위한 독립기구의 필요성

현행법의 경우 개인정보의 이용 촉진과 동시에 규제 사항이 규정되어 있음으로써 법 목적이 혼재되어 있을 뿐만 아니라, 거기에 따라 각 담당부서에 이중적 역할이 부여되어 있다. 특히 행정자치부나 정보통신부는 자신의 영역에서 개인정보의 보호 및 감독을 위해 자기 산하의 기존 기구를 강화하는 방안을 제시하고 있다. 그러나 이것은 정보 이용 촉진과 보호 임무 등 두 역할을 동시에 갖는 것을 의미한다. 이렇게 실행 및 집행부서가 감독의 권한까지 갖는 것은 권한의 집중을 불러일으키고, 따라서 개인정보처리의 감독 역할을 제대로 수행할 수 없는 상태를 야기한다. 즉 ‘창과 방패를 동시에 갖게 해서는 안된다’. 오히려 외부에 규제 권한을 부여함으로써, 해당 공공기관에 대한 경쟁과 견제의 역할을 수행할 수 있도록 해야 할 것이다. 즉 개인정보 보호 및 감독을 위한 독립기구를 설치 마련함으로써 견제와 균형이 이루어질 수 있도록 할 필요가 있다.

2.2. 행정정보 공동이용에 대한 가이드라인 수립

2.2.1. 행정정보공동이용의 현황

현대사회가 정보사회로 이행됨에 따라 행정정보[1]의 공동이용은 전자정부를 추구하는 사회에서는 특히 중요한 부분을 차지하게 되었고, 정보의 다양화와 기술발달로 정보공유가 가능한 단계로 발전하게 되었다.

정부는 1998년 3월에 「행정정보공동이용에관한규정」 및 동시행규칙을 제정하여 중앙부처, 지방자치단체 등에서 960여종의 데이터베이스를 구축·활용하였다[2]. 그리고 1998년에는 여권발급민원전산망을 구축하여 주민, 신원, 병적 데이터베이스 등을 공동이용 하였으며, 국토정보센터를 구축하여 지적, 주민, 지가자료를 통합, 부동산실명제를 도입할 수 있는 기반을 마련하였다. 그리고 2000년 5월에서 12월에는 생산적 복지정보공동이용시스템[3]을 구축하여 국민기초생활보장제도의 기틀을 마련하여 시군구의 복지담당공무원이 생활보호대상자를 신속·정확히 선정하고 관리할 수 있는 체계를 구축하였다. 동시에 시군구의 보유 정보 외에도 행정자치부의 국토정보망, 국세청의 국세통합전산망, 노동부의 고용정보망, 국민연금·건강보험·근로복지공단의 데이터베이스와 연계 및 공동이용하고 있다.

이후 정부는 행정정보공동이용을 도입하기 위해 2000년 7월 전자정부 실현을 위한 행정정보 공동이용의 기본계획을 수립하였고, 2001년 3월 「전자정부구현을위한행정업무등의전자화촉진에관한법률」(이하 전자정부법이라 한다) 제정 및 시행(2001년 7월)으로 제도적 기반을 마련하였다. 전자정부법은 전자정부 구현을 위한 행정정보의 공개원칙, 행정정보공동이용의 원칙 명시, 개인정보보호 원칙 규정 등의 운영상의 세부 원칙을 포함하고 있다. 그리고 2002년 11월, G4C시스템을 통해 주민, 호적 등 20종[4]의 행정정보공동이용을 시작하였으며, 이를 통해 1종 이상 감축되는 민원은 총 614종에 이르고 있다. 민원처리를 위한 행정정보의 공동이용은 공동이용시스템을 통해 내부적으로 확인가능하고, 민원인은 별도의 구비서류를 제출하지 않으며, 민원처리 담당 공무원은 행정 내부적으로 확인할 수 있는 사항에 대해 민원인으로부터 별도의 구비 서류를 받을 필요가 없어졌다. 현재의 20종에 대한 공동 활용에서 04년 26종, 05

---

1) 여기서 말하는 행정정보는 전자정부구현을위한행정업무등의전자화촉진에관한법률 제1장 제2조 4에서 정의하는 것을 뜻한다. 즉 "행정정보"라 함은 행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것을 의미한다.

2) 이에 해당하는 960여종의 정보는 부록에서 참고할 수 있다.

3) 보건복지부에서는 국방부, 국가보훈처, 공무원연금관리공단, 사학연금관리공단에서 보유한 퇴직군인연금, 국가유공자관련연금, 공무원연금, 사학연금 등의 정보를 이용하여 생산적복지정보공동이용시스템을 구축하였다.

4) - 행정자치부(4종): 주민등록등(초)본, 토지(임야)대장, 지방세 납세증명서, 지방세세목별과세(납세)증명서(자동차)
- 건설교통부(6종): 개별공시지가확인서, 건축물대장등본(일반/집합), 사용승인서(주택건설사업사용검사필증), 자동차등록원부(갑/을), 이륜자동차사용신고필증, 건설기계등록원부(갑/을)
- 대법원(4종): 건물등기부등본, 토지등기부등본, 법인등기부등본, 호적등본
- 국세청(6종): 국세납세증명서, 사업자등록증, 소득금액증명, 납세사실증명, 휴업사실증명, 폐업사실증명

년 34종, 06년 39종까지 확대할 계획을 가지고 있다. 또한 보다 적극적인 공동이용 확대를 위한 업무재설계(BPR) 및 정보화전략계획(ISP) 작업을 행정자치부와 정보통신부 주관으로 2003년 9월부터 2004년 5월에 거쳐 시행하였다. 정부는 이 작업을 통해 행정정보 공동이용 대상을 민원구비서류 감축과 행정업무 효율 향상 효과가 높은 정보를 대상으로 확대하고, 단계적 연계 활용계획을 수립하기로 하였다.

2.2.2. 행정정보 공동이용의 가이드라인 수립의 필요성

2.2.2.1. 행정정보 공동이용의 필요성

행정정보가 정부 혹은 공공부문에서 공동으로 활용되어야 하는 배경은 크게 두 가지로 나누어 볼 수 있다. 첫 번째는 미국을 중심으로 하는 선진국의 행정중심체계가 고객지향성(Customer Oriented)을 강조하고 있으며, 이는 정보화를 통한 전자정부구현의 핵심적인 기준(Criteria)이 되고 있다. 따라서, 정부 혹은 공공기관은 국민의 불편을 초래하지 않도록 내부에서 보유한 정보를 최대한 공유하고 활용해야 한다. 두 번째로는 정보기술의 발달이다. 계속적인 정보기술의 발전은 과거 불가능하다고 여겨졌던 정보의 공유, 원거리에서의 정보이용, 정보이용자에 대한 권한부여와 이용범위의 제한 등을 가능하게 하고 있다. 또한, 과거 기술의 발전이 상용화되어 정부 및 공공부문에 활용되는 시간의 차이(Time Gap)가 민간부문에 비해 늦었던 반면 최근 정보기술의 발달은 그 갭을 점차 줄이고 있다. 이러한 정보기술의 발달은 국민편익 증진과 공공부문의 생산성 향상을 위한 정보공동활용의 당위성을 제공한다.

우리나라의 행정정보공동이용은 이러한 필요에 따라 “국가기본정보 공동활용체계 구축방안 연구”(한국전산원 연구보고서, NCA Ⅲ -RER- 99021, 1999. 7.), "미국의 정보공동활용 정책사례에 대한 과정 중심적 분석“(한국전산원 연구보고서, NCA Ⅲ -RER- 99072, 2000. 1.), "정보공동활용의 경제성 분석”(NCA Ⅲ -PER-99-42/ 1999.11.), "정보공동활용 연계·통합모델 및 추진절차에 관한 연구“(한국전산원 연구보고서, NCA Ⅲ -RER-99073, 1999. 12.) 등 과거 많은 연구가 이루어졌다.

2.2.2.2. 행정정보 공동이용을 위한 개인 프라이버시 보호의 필요성

행정정보 공동이용이 필요함에도 불구하고 신중한 접근이 이루어져야 하고, 추진 단계가 보다 합리적이고, 체계적이어야 함을 주장하는 이유는 공유정보의 가치와 그 중요성에서 찾아볼 수 있다. 정부 및 공공부문에서 공유되고 활용되어질 정보는 국민의 인적정보와 국가적으로 중요한 정보들을 대상으로 한다. 이중 인적정보는 개인 프라이버시와 관련된 정보로서, 그 활용의 범위와 목적에 따라 심각한 프라이버시 침해에 관한 문제를 야기할 수도 있기 때문이다. 인

적정보의 중요성은 최근 발생하는 온라인(On-line) 및 오프라인(Off-line)상의 범죄에서 볼 수 있듯이 개인에게 치명적일 수 있으며, 사회적 문제로도 이슈화될 수 있기 때문이다. 인적정보의 중요성에 비해 현재 논의되고 있는 대응방안으로는 시스템 보안만을 이야기하는 의견도 상당수가 존재하고 있다. 그러나, 시스템적인 보안문제 이외에도 발생할 수 있는 인적정보 침해 요인은 매우 다양하다고 볼 수 있다.

2.2.2.3. 행정정보를 공동이용 함에 따라 발생할 수 있는 개인 프라이버시 문제점

행정정보 공동이용을 위해 주관기관에서 종합정보를 수집하고 관리하고, 각 정부부처 및 공공기간에서 종합된 인적정보를 이용함에 따라 발생할 수 있는 문제점은 우선 크게 나누어 두 가지로 볼 수 있다.

첫째, 해킹에 의한 인적정보의 유출이 가능하다. 최근 발생하고 있는 해킹문제에 따라 각 민간 기업 및 공공기관의 서버에 보안시스템을 강화하고 있는 상황이다. 또한, 이러한 해킹기술은 계속적으로 발달하고 있으며, 세계 어디에서든지, 온라인에 접속하여, 원하는 기관의 서버에 접속하여 해킹을 시도할 수 있다. 이렇게 해킹된 정보는 각종 신용관련 정보를 포함하고 있고, 우리나라의 경우 주민등록번호를 통해 개인의 많은 정보에 접근할 수 있어 특히 그 영향력은 매우 크다고 할 수 있다.

둘째, 정부 및 공공기관에서 인적정보를 공유하고 활용함으로써 의도적 불법유출 또는 의도적이지는 않지만 우연에 의한 유출이 발생할 가능성이 존재한다.

최근 전자정부의 도입에 따른 업무처리절차개선 작업이 지속적으로 수행되고 있지만, 현재까지의 업무처리절차는 공공부문의 업무대상이 넓어지고, 국민대상 서비스가 세분화됨에 따라 다양한 정보를 활용하는 경우가 많다. 이러한 과정에서 발생 가능한 불법유출에 의한 국민의 피해는 정보공동이용을 통해 국민의 편익을 증대하고, 국가 생산성 향상을 이룩하고자 하는 목적과는 다르게 국민권리와 이익을 침해하는 수단으로 활용될 수 있다는 측면에서 보다 신중하게 다루어져야 할 것이다.

2.2.3. 현행 법률 및 제도의 현황

현재 행정정보의 공동이용을 규율하는 기본법은 전자정부법이고, 법의 목적은 행정업무의 전자적 처리를 위한 기본원칙 · 절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성 · 투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것이다. 직접적으로 행정정보의 공동이용과 관련 있는 법 조항은 다음과 같다.

– 전자정부법 제11조: 행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동 이용하여야 한다.

– 전자정부법 제12조: (개인정보보호의 원칙) 행정기관이 보유 · 관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다.

– 전자정부법 제21조: 행정기관은 민원사항의 처리를 위하여 필요한 행정정보 등을 공동이용 하여야 한다.

– 전자정부법시행령 제41조: 행정기관의 장은 행정정보의 공동이용을 통하여 구비서류에 대한 정보를 확인할 수 있는 경우에는 그 확인으로 구비서류에 갈음할 수 있다.

– 민원사무처리법시행령 제8조: 민원을 접수·처리함에 있어 행정정보로 내용확인이 가능한 경우 민원인에게 관련증명서류의 제출을 요구할 수 없으며, 당해 민원사무를 처리하는 공무원이 직접 확인·처리하여야 한다.

– 공공기관의 개인정보 보호에 관한 법률 : 1994년 제정되어 1999년, 2004년 일부 개정되어 공공기관의 개인정보 활용에 관한 지침과 방향성을 제시하고 있다.

2.2.4. 해외 사례의 검토

선진국의 사례를 통해 시사점을 도출하기 위해 아래에서는 각국의 법률·제도적 측면을 대상으로 사례연구를 수행하였으며, 추가적으로 추진체계 및 전략의 구성과 실행측면을 중심적으로 살펴보았다. 기술적 측면은 계속해서 발전하고 있으며, 연구결과에 따른 실질적인 수행단계에서 가장 앞서있는 기술의 도입이 가능하며, 국가별 특성에 적용타당성을 검토한 후 논할 수 있기에 본 사례연구에서는 최소화하였다.

(1) 미국

미국에서 개인 프라이버시의 보호는 문화적 특성으로 인해 전자정부의 추진이전에 추진되었으며, 전자정부의 추진체계가 구성되고(NPR에서 OMB로 변화) 시행이 되면서, 전자정부 추진과 관련된 프라이버시 보호에 관한 법률로 확대 시행되고 있다. 1974년 프라이버시 보호법(Privacy Act)이 명문화되었으며, 정보기술의 발달과 함께 1984년 10월 10일 기존의 프라이버시 보호법을 대폭 수정하여, 컴퓨터의 연결과 프라이버시 보호법(Computer Matching and Privacy Protection Act : Matching Act)을 제정하였다. 이후 기술의 발전과 함께 부분적인 개정은 계속되었으며, 1989년에는 국민의 인적정보를 활용하기 위해서 컴퓨터연결과 프라이버시 보호법에 의한 절차를 수행해야 하며, 이를 위한 가이드라인으로서 Federal Register, OMB, "Guidance on Computer Matching(54 Fed. Reg. 25818, June 19, 1989)를 작성하

여 각 부처에 지원하였다. 또한, 1995년에는 OMB Circular A-130, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals." 과 함께 문서작업감축법(PRA: Paperwork Reduction Act)에 충족할 수 있도록 업무수행지침을 전달하기도 하였다.

이와 같이 미국에서는 인적정보 활용과 함께 공공부문의 생산성 향상을 위한 법률적 제도를 동일한 수준에서 제정하고 있으며, 이를 통해 다음의 기준으로 프라이버시를 보호하고 있다.

- 개인의 동의 : 인적정보를 활용하기 위해서 주관기관은 문서에 의한 개인의 동의를 득 해야 한다.
- 유출금지 : 정보의 활용을 위해 사용하기 위해서는 OMB에서 정한 지침에 적합한 수행절차를 따라야 하고, 그 절차에 의해서 활용되어야 한다. 따라서, 정보의 활용을 위한 유출은 극히 제한적으로 수행된다.
- 정확도의 유지 : 공공부문에서 활용되는 인적사항은 허가 및 유지, 징세 등에 활용될 것이다. 따라서 개인의 정보는 개인이 접근이 가능하며, 새롭게 변경사항을 기록할 수 있어야 하고, 그 정확성을 유지할 수 있도록 해야 한다.
- 보안유지 : 인적정보관리기관은 적합한 보안유지요원의 보유 및 기능을 자체적으로 보유해야 한다. 이러한 과정에 대한 신뢰도를 위해 그 내용과 적절한 설명은 개인에게 제공되어야 한다.
- 최소 정보의 사용 : 각 기관은 인적정보 활용에 필요한 업무절차를 개선하여, 인적정보를 활용함에 있어서, 최소화하여 활용할 수 있어야 한다.
- 기술적 신뢰성의 유지 : 주관기관은 사용되어지는 프로그램을 언제나 최상의 상태로 유지하고, 업무절차를 개선함으로써 인적정보가 사용되어지는 업무절차 및 기술수준이 신뢰성을 줄 수 있도록 한다.
- 프라이버시 효과 평가 : 2001년부터 시행된 PIA(Privacy Impact Assessment)에 의해 인적정보의 활용에 대한 효과를 평가하고, 그 침해에 대한 예방적인 활동을 수행하도록 한다.

년 도	법 안 명	내 용
1971	Fair Credit Reporting Act(15 USC 1681)	금융신용보고, 업체에 관련된 개인의 권리를 보장
1973	Crime Control Act	범죄 판정 기록에 대한 보호
1974	Privacy Act of 1974(5 USC 557a, P.L. 93-579)	연방정부의 기록보전시스템내의 프라이버시 보호
1974	Family Educational Rights and Privacy Act(5 USC P.L. 94-380)	연방교육기관내에 보관되는 학생기록에 대한 프라이버시 보호
1974	Minnesota, Arkansa, Utah 등의 주법	Privacy Act of 1974법을 실현시키기 위해 각 주에서 제정한 Fair Information Practices Laws
1978	Right to Financial Privacy Act	은행정보의 부정노출 방지
1989	The Computer Matching and Privacy Protection Act	개인 신상의 컴퓨터 조회에 따른 프라이버시 보호를 위한 절차와 요구사항을 정의

<표 4> 미국 프라이버시 문제해결을 위한 주요법안[5)]

(2) 영국

다른 선진국가와 다르게 영국에서는 오래전부터 주거침입, 저작권 침해, 비밀의 침해 등을 대상으로 각 개별법에 따라 프라이버시보호를 수행하였으나, 정보기술의 발달과 인적정보의 유출로 인한 피해가 예상되는 시점에서부터 컴퓨터를 이용한 인적정보의 유출을 막기 위해 데이터보호법을 제정하였으며, 이 법을 기반으로 전자정부 추진과정에서 기술적 진보에 따라 세부내용이 계속적으로 개정되고 있다.

영국의 전자정부 추진을 위한 정부백서로서, 1999년 발간된 “정부 현대화 계획(Modernizing Government)"에서 개인 프라이버시 보호를 위한 필요성과 구체적 추진전략을 제시하였다. 추진 전략에는 정보공동이용에 따른 개인 프라이버시 보호를 위한 추진 모델로 아일랜드 전자정부 연구조직인 Reach의 개인정보보호 모델을 적용하도록 제안하였다. Reach모델에서는 다음과 같은 내용으로 개인정보보호에 관한 사항을 제안하고 있다.

1) 법률·제도측면

법률제도 측면에서 세부적인 사항까지 규정하고, 발생되는 신규업무에 대하여 지속적인 개정이 필요하다.

5) 인적정보의 공동활용에 따른 기술적・제도적 프라이버시 보호대책, 1997.12 한국전산원 (NCA Ⅳ-RER-97089/1997.12)

2) 운영측면

- 규정제정과 운영기관의 선정 : 종합적인 운영 및 관리·감독기관의 필요성 강조
- 투명성 강화 : 정보제공자에게 활용되는 절차와 프라이버시 침해 차단 방법에 대한 홍보
- 관리·감독 강화 : 개인 프라이버시의 유출은 치명적인 결과를 초래하기 때문에 이를 관리·감독하는 기관을 지정하고, 외부 민간단체를 위촉하여 계속적인 점검체계를 구축
- 개인정보의 최소화 사용 : 개인은 정보제공을 선택할 수 있어야 하며, 정보제공 이후 운영주체는 업무절차를 개선하여 최소화된 정보를 사용할 수 있도록 해야 함

영국정부는 수립된 추진전략에 따라 2000년 10월 23일 개통된 정부차원의 지식공유시스템(HM Treasury의 CMF : Capital Modernization Fund에 의해 1,000만 파운드를 투입하여 구축한 시스템으로 14개 부처가 연결되어있으며, 54,000명의 공무원이 사용)의 접근 권한과 사용 자료의 DB화, 권한의 부여와 사용 후 결과에 대한 명확한 Feedback 시스템의 설계 등을 추진하였다.

연 도	법안 및 내용
1962~1970	프라이버시 법안에 제안되었으나, 정부 측의 반대로 무산 1960년대 후반 이후 컴퓨터를 이용한 정보처리와 프라이버시 문제발생으로 인해 데이터감시 및 개인정보보호에 관한 논의(데이터베이스 설치의 신고제, 공공 및 기관보유 기록에 대한 개인 당사자의 열람, 정정 청구권 인정, 정보은행 심판소의 허가규정 등)
1970	프라이버시 위원회가 발족하여 권고대책 발표
1975	내무부에서 컴퓨터와 프라이버시에 대한 백서출간(감독기관의 설치 등만을 제안함으로써 프라이버시 침해에 대하여 간과)
1976.7	데이터보호위원회 설치, 내무부 발간백서를 보완한 보고서 제출
1984.7	데이터보호법 제정
현재	1970.6월 시행된 전자계산기 처리정보의 남용에 의한 프라이버시 침해방지에 관한 법률, 데이터보호법(1984.7월 제정) 등을 계속적으로 개정하여 프라이버시 보호

〈표 5〉 연도별 영국 프라이버시 보호관련 입법과정[6)]

2.2.5. 종합 대안

6) 인적정보의 공동활용에 따른 기술적·제도적 프라이버시 보호대책, 1997.12 한국전산원 (NCA Ⅳ-RER-97089/1997.12)

행정정보 공동이용에 따른 문제점은 정보유출에 의한 개인 프라이버시의 침해로 이어질 수 있으며, 그 방식으로는 해커에 의한 정보유출, 그리고 공동이용에 따른 의도적 또는 의도하지 않은 유출로 나누어 볼 수 있다. 또한, 선진국에서는 개인정보의 활용에 관하여 여러 가지 방면에서 발생 가능한 문제를 사전에 해결하고, 체계적이고 구체화된 계획을 통해 정보공동이용 추진을 수행함으로써 국민 개인의 프라이버시를 보호하고, 행정 생산성 향상을 도모할 수 있는 방향으로 정책을 추진하고 있다. 또한 기술적인 도입도 계속적으로 이루어지고 있는 상태이다. 이러한 측면에서 선진국에서 제시하고 있는 행정정보를 공동이용 함으로써 발생하는 개인정보 유출의 문제점을 해결하고 있는 방안 등을 토대로 그 개선방안을 다음 4가지 관점에서 제시하고자 한다.

(1) 법률·제도 측면

선진국에서는 행정정보 공동이용에 의한 개인정보보호를 위한 첫 번째 단계로서, 인적정보보호에 의한 프라이버시 침해를 보장하는 법의 제정을 들고 있다. 또한, 단순히 법의 제정에서 그치는 것이 아니라, 이후 계속되는 개정을 통해 발생가능한 모든 예상문제에 대하여 법률적으로 개인 프라이버시를 보장하고 있다. 이 측면에서 우리나라는 1994년 공공기관의 개인정보보호에 관한 법률이 제정된 이후 2번의 개정이 이루어졌지만, 정보공동이용에 따라 발생 가능한 개인정보의 유출에 충분히 대비하지 못하고 있는 측면이 있다. 특히, 정보공동이용에 따라 새롭게 발생하는 업무처리절차는 매우 복잡하고, 권한과 의무에 대한 규정이 매우 어려울 수 있다. 따라서 주관기관에서 관리해야하는 권한과 의무에 대해 보다 명확히 규정지어야 하며, 이용 가능한 정보의 범위와 내용에 대하여 보다 세부적으로 규명해야 할 것이다.

(2) 투명성 측면

국민은 당사자의 정보가 정부 및 공공기관에 어떠한 형태로 축적되어있으며, 그 활용현황과 활용방안 및 절차, 그리고 이용 가능한 기관의 권한과 의무에 대하여 알 권리가 있다. 또한, 이러한 정보의 공유에 대한 철저한 관리가 이뤄지고 있는 체제에 대해서도 알 수 있어야 한다. 이는 국민에게 인적정보를 정부 및 공공기관에서 이용함에도 불구하고 개인 프라이버시 침해를 차단할 수 있는 체제를 보유하고 있으며, 이를 지속적으로 개선해나가고 있음을 알려주는 동시에 내부적으로는 시민단체 등에 의한 감시에 의해 보다 견고한 프라이버시 침해 차단체계를 구축하는데 그 의의가 있다.

(3) 관리 및 감독 측면

행정정보의 공동이용에 의해 발생할 수 있는 개인 프라이버시의 침해는 정보의 유출에 의

하거나, 고의성 여부와 상관없이 잘못된 사용에 의해 발생할 수 있다. 이러한 유출과 잘못된 사용에 대하여 관리 감독하는 주관기관이 존재해야 하며, 주관기관은 개인에게 정보공동이용을 위한 승인을 득 해야 한다. 승인된 정보에 한하여 공동이용에 사용되며, 철저한 관리 감독(제도적, 기술적)이 수반되어야 할 것이다. 또한, 주관기관에 의한 관리, 감독 이외에 시민단체 등에 의한 주기적 점검 및 옴부즈맨 제도의 도입 등을 통해 다양한 방법으로 관리, 감독이 수행되어야 할 것이다.

(4) 국민의 정보제공 선택권 측면

국민은 기본정보를 제외한 기타 정보에 대하여 공동이용 할 수 있는 정보로 제공하는 것을 선택할 수 있어야 한다. 또한, 제공된 정보는 각 부처 및 공공기관의 업무에 따라 최소한으로 사용되어야 할 것이다.

개인의 인적정보는 주민등록번호를 포함하여 많은 양의 정보로 구성될 수 있다. 하지만, 정부 및 공공기관에서 활용되는 정보는 기본정보를 기반으로 업무에 따라 다양하게 필요할 것이다. 이런 측면에서, 정보공동이용을 위해 필요한 최소정보를 규정하고 이외의 정보(예 : 카드계좌, 부동산 정보, 급여 정보 등)에 관해서는 개인의 선택에 따라 입력할 수 있고, 정보공동이용에서 제한될 수 있어야 한다.

공동정보이용에 따라 기존 업무처리절차도 지속적으로 개선되어야 것이며, 개선된 업무처리절차에 따라 각 업무에 필요한 최소한의 정보만을 사용하는 것이 규정되어야 하고, 관리, 감독되어야 할 것이다. 이는 권한을 업무에 따라 단계적으로 부여는 방식으로 추진되어야 할 것이다.

이외에 인적정보에 대해 수시로 수정할 수 있는 권한, 활용결과에 대한 Feedback 시스템, 인적정보 활용에 대한 효과평가, 수행절차에 대한 성과평가 등의 문제들에 대해서도 검토할 필요가 있을 것이다.

<참고 1> 우리나라 행정기관의 보유 데이터베이스 현황 및 공동이용 현황(2001년도 기준)

- 행정정보DB: 960종

구 분	DB 종류	DB 수
중앙행정기관	법령심사정보, 국유재산정보, 지적·주민, 공시지가 등	294종
지방자치단체	자치법규, 개별공시지가 산정, 도로전용료 관리, 지방세 관리 등	589종
시·도교육청	검정고시 합격자화일, 학원관리, 도서관리, 박물관 소장자료 등	77종

- 개인정보DB: 388종

구 분	DB 종류	DB 수
중앙행정기관	국가유공자 취업관리, 학적화일, 입원환자 파일, 소득조회 파일 등	90종
지방자치단체	종합토지세 파일, 재산세 파일, 호적·제적관리, 의료보호 파일 등	107종
각급 학교	학적관리, 입시관리, 도서관리 파일 등	21종
정부투자기관	연금급여관리, 재해자 파일, 산업재해 근로자, 용지 매수자 파일 등	170종

<출처: 전자정부구현을 위한 법안 심사보고서 - 행정자치위원회. 2001. 2. p.15>

– 행정정보 공동이용 현황(27개 기관, 79종 DB 상호활용

제공기관	제공정보(DB)	이용기관	용도
국가보훈처	교육보호, 보상금관리, 취업관리 등 6종	정보통신부, 공무원연금관리공단 등 6개 기관	이체이뢰 등
외교통상부	여권분실정보	법무부	출입극시 위조여부 검사
재정경제부	세입·세출 결산자료	국세청, 관세청, 정보통신부, 정부회계관서 등	세입자료입력, 지출액 정리 등
법무부	재·출소 증명원, 수형자 석방통보, 가석방 통보 등 4종	검찰, 경찰, 국민연금관리공단 등	수사자료 및 업무용
국방부	장군현황, 군인대부현황, 군인연금현황 등 7종	행정자치부, 국회, 감사원, 재정경제부 등	
행정자치부	주민등록정보, 종합토지세자료 등 2종	국세청, 감사원, 경찰청, 서울시 및 지방자치단체	종합토지세부과용 DBrn축, 주민 DBrn축
교육부	기관코드	병무청	병무업무전산화
농림부	전국유통정보, 가락동유통정보 등 3종	해양수산부, 유통공사, 농림수산정보센터 등	기관 게시, 보관, 정책자료, 보도용
산업자원부	등록자료현황	각 시도 광업관련부서	광업업무처리
보건복지부	면허정보	행정자치부, 의료인협회 등	비상대비자원관리
환경부	대기오염도자료, 수질오염도 자료 등 3종	건교부, 서울시, 행자부, 지자체 등	오존경보, 물관리 종합대책자료
건설교통부	공시지가자료, 자동차등록자료, 토지거래자료 등 3종	행자부, 환경부, 경찰청, 국세청 등	차적조회, 환경개선부담금, 지가검색 등
해양수산부	원양생산통계	통계청	통계자료집 발간
국세청	종합소득자료 등 5종	행자부, 재경부 등	주민세 과세, 보험료 산정 등
관세청	수출입통관자료 등 4종	국세청, 감사원 등	원산지증명발급, 수출입동향분석 등
조달청	외자구매요구서 등 10종	조달요청기관, 조달업체	입찰정보제공 등
통계청	통계정보시스템	모든 기관	통계자료활용
검찰청	피의자인적사항, 검사처분내용 등 4종	법원, 보호관찰소 등	법원판결에 참조
병무청	제1국민역 및 징병검사대상자	경찰청	운전면허 발급가부 결정
기상청	기상관측, 예보·특보자료, 북한DB, 기후DB 등 4종	행정자치부, 농수산부, 해군, 항공사, 언론사 등	정부기관 자료 제공 및 연구·보고자료
농촌진흥청	농업기술종합정보	농림수산정보센터	농업인정보제공

제공기관	제공정보(DB)	이용기관	용도
산림청	임업통계	통계청	통계자료제공
해양경찰청	사건사고정보	해양수산부	상황관리
특허청	출원·등록파일, 초록 및 전문명세서	특허기술정보센터	대민서비스
식품의약품안전청	수입식품관련자료, 의약품허가자료 등 3종	관세청, 6개 지방청	수입식품검사업무, 통관업무, 의약품허가관리 등
헌법재판소	헌법판례정보	대법원	헌법판례검색
법원행정처	기여금내역, 등기신청부본, 형사소송자료 등 7종	법제처, 세무서, 검찰청, 경찰청, 연금관리공단, 금융기관	종합법률정보제공, 세금, 연금관리 등

<출처: 전자정부구현을 위한 법률안 검토보고
– 정부 측, 행정자치위원회 수석전문위원 박봉국. 2000. 12. p.31-32>

2.3. 신용정보의 이용 및 보호에 관한 법률 제정

2.3.1. 신용정보의 특성과 보호 필요성

신용정보란 금융거래등 상거래에 있어서 거래상대방에 대한 식별·신용도·신용거래능력 등의 판단을 위하여 필요로 하는 정보로서, 이와 관련한 정보는 신용정보주체의 식별정보, 신용불량정보, 신용거래정보, 신용능력정보, 그리고 공공기록정보로 분류된다.

우리 사회는 산업의 고도화와 경제규모의 확대로 점차 신용사회로 진행하고 있다. 이러한 가운데 금융회사, 신용카드업자, 할부판매회사 등 신용제공자는 소비자의 신용능력을 정확히 평가하여 적정한 신용을 제공함으로써 과잉여신이나 과다한 채무에 따른 소비자 파산 등의 사회적 문제를 완화할 필요가 있다. 신용제공자는 채권 회수의 안전성을 확보하고, 소비자의 신용능력에 대한 평가를 신속한 절차와 용이한 방법으로 행함으로써 신용제공에 따르는 비용을 최소화할 수 있다. 이에 따라 소비자 신용정보를 체계적이고 효율적으로 관리·운영할 수 있는 제도적 장치가 필요하게 된다.

그러나 한편으로 소비자 신용정보체계의 운영과정에서 소비자의 개인정보가 무분별하게 수집·이용·제공됨에 따라 정보주체의 인격적 이익이 무단히 침해될 수 있고, 또 부정확하고 오래된 신용정보에 의하여 잘못된 신용결정이 내려짐으로써 신용계약의 거절·중단과 같은 예기치 않은 경제적 피해를 소비자가 입을 수도 있다.

신용정보법은 이러한 상충하는 사회적 이익, 즉 신용정보의 효율적 이용과 소비자의 개인정보자기결정권을 적정하고 조화롭게 조정하기 위한 필요에서 마련된 것이다. 다만, 신용정보가 정보주체에게 있어서 가지는 중요성에 비추어 개인정보의 자기결정권에 보다 비중을 두는 보완이 필요한 실정이다.

2.3.2. 사회적 쟁점 및 현안 사례

공공기관이나 신용정보업자등에 의하여 소비자의 신용정보가 정보주체의 동의 없이 무분별하게 수집·이용·제공됨에 따라, 신용정보의 유출과 남용 같은 사회적 문제가 여러 차례 발생했다.

. 신용카드사 고객정보 유출사건(2001.7): 신용카드업체들이 고객들의 개인정보를 '업무제휴' 명목으로 보험회사에 제공한 후 수수료를 받아온 사실이 서울지검 컴퓨터수사부에 의해 적발되었다. 이들이 보험회사에 제공한 개인정보는 이름, 주소, 전화번호, 주민등록번호뿐만 아니라 소득, 재산, 카드, 결제계좌번호, 카드이용한도액, 유효기간 등 신용정보까지 포함되어 있었다. 신용카드업체는 고객의 동의 없는 정보제공으로 매달 수천만원에서 수억원의 이득을 챙겨왔으며, 이들에게 고객의 개인정보는 더 이상 보호의 대상이 되지 못했다.

. 정부기관의 과다한 금융거래 및 신용정보의 요구와 유출(2003.5.): 국세청, 법원, 검찰,

지방자치단체 등이 금융기관에 무차별적으로 금융거래 정보를 요구할 뿐만 아니라 이렇게 제공된 개인의 신용정보가 줄줄이 새나가고 있다. 국회재정경제위원회에 따르면, 15개 은행이 2001년 하반기부터 2002년 상반기까지 정부기관에 제공한 정보건수는 310만2000여건에 이르렀다. 이 과정에서 금융실명법 등이 제대로 지켜지지 않았을 뿐만 아니라 법의 테두리를 벗어난 자료 요청이 남발되고 있다. 심지어는 일부 기관의 관리 소홀로 이 정보가 민간 사채업자 등에게 흘러들어간 것으로 알려졌다. 이처럼 금융거래 정보에 대한 엄격한 관리가 아직 부족한 실정이다.

. 개인신용정보를 부정 사용한 삼성생명에 손해배상 판결(2003.12): 지난 2002년 4월 삼성생명이 고객의 신용정보를 임의로 조회, 정리하여 영리 목적에 이용하기 위해 보험모집인에게 배포한 것에 대해 참여연대가 소송을 제기한 바 있었으며, 이에 대해 법원은 경제적 피해가 없어도 개인정보 침해로 인정한 적극적 판결을 내렸다. 이는 금융기관의 개인 동의 없는 신용정보의 이용 관행에 제동을 거는 계기가 되었다.

2.3.3. 현행 법률 및 제도의 현황

「신용정보의이용및보호에관한법률」(이하 ‘신용정보법’이라 한다)은 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 기하며 신용정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 하여, 1995. 1. 5. 법률 제4866호로 제정·공포되어 여러 차례 개정되고 최근 2001. 3. 28. 개정(법률 제6428호), 그리고 2002.8.26 일부개정(법률 제6705호)을 통해 지금까지 시행되고 있다.

이 법률은 신용정보 관련업체를 신용정보업자, 신용정보집중기관, 신용정보 제공·이용기관으로 구분하고 있다. 신용정보업자는 신용조사업, 신용조회업, 채권추심업 등을 영위할 수 있는 업체로 100억원 이상의 자본금 혹은 기본재산을 갖추어야 하며 또한, 재정경제원의 허가를 받아야 한다. 이 법률은 신용보증기금, 기술보증기금 및 금융기관이 공동출자한 법인(한국신용평가, 한국신용정보) 등의 업체를 신용정보업체로 지정하고 있다.

신용정보집중기관은 신용정보를 집중하여 관리할 수 있는 기관으로 금융기관 이외의 기관들이 보유하고 있는 정보를 집중관리하는 기관으로 나누어진다. 여기서 금융기관 이외의 기관에는 백화점 등 유통업체, 자동차 등 할부판매업체 등이 포함되며 이들 업체들은 협회 등을 구성하여 신용정보집중기관으로 등록할 수 있다. 신용정보집중기관은 회원기관간의 원활한 정보유통을 위하여 ‘신용정보 공동전산망’을 구축할 수 있는데, 이는 동종업종 간에는 집중된 개인 신용정보를 광범위하게 교환, 활용할 수 있다는 의미가 된다.

신용정보 제공·이용기관은 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻어지거나 만들어낸 신용정보를 신용정보업자나 신용정보집중기관에게 제공하거나 이들로

부터 신용정보를 지속적으로 제공받아 자신의 영업에 이용하는 업체를 지정한다. 이러한 업체에는 동종업체간의 신용정보를 교환 및 활용에 필요한 금융기관 및 백화점 등과 같이 채권추심의 위임이 필요한 기관(중소기업, 보험회사, 증권회사, 신용금고 등)이 포함된다.

구분	전국은행연합회	한국신용정보	한국신용평가
주요 정보원	신용정보법 시행령상의 금융기관(은행, 단자, 종금, 기금, 보험, 리스 등)	전국은행연합회, 신용공여기관(백화점, 가전, 자동차, 할부금융, 중장비, 렌탈 등 350여 업체)	전국은행연합회, 신용공여기관
정보내용	불량거래정보, 금융거래정보	불량거래정보, 금융거래정보, 신용거래정보, 조회처정보	불량거래정보, 금융거래정보, 신용거래정보, 조회처정보
정보활용기관	신용정보법 시행령상의 금융기관 및 신용정보업자	신용공여기관	신용공여기관
정보제공방식	온라인, M/T 제공	온라인, M/T, 문서	온라인, M/T, 문서

〈표 5〉 주요 개인신용정보기관의 운영형태
출처: 황윤경, 「신용정보체계의 이해 및 현황」, 한국정보법학회 세미나

개인신용정보의 보호 규정과 관련하여, 신용정보법의 주요 내용은 다음과 같다.

(1) 신용정보의 수집제한 규정

신용정보업자는 수집목적의 정당성, 수집범위의 필요최소성, 수집방식의 합리성에 의하여 신용정보를 수집해야 한다고 규정되어 있다.(제13조) 특히 수집범위의 필요최소성 요건을 구체화하여, 신용과 무관한 사생활 관련 정보와 불확실한 개인신용정보의 수집 조사를 금지한다.(제15조 제1항)

(2) 신용정보이용의 제한

신용정보 제공자·이용자가 금융거래 내용에 관한 정보, 개인 질병에 관한 정보, 기타 대통령령이 정하는 개인 신용정보를 신용정보업자에게 제공하고자 할 때는 금융감독위원회가 정하는 바에 의하여 신용정보의 내용과 제공 대상자 등을 명기한 서면 동의를 받도록 하고 있다.(제23조)

또한 개인정보는 당해 개인과의 신용거래 관계설정 및 유지 여부 등의 판단목적으로만 제공 및 이용될 수 있다. (제24조 제1항) 신용정보업자와 신용정보업 관련자는 업무상 알게 된 개인의 신용정보 및 사생활 등 개인적 비밀을 업무목적 외로 누설 또는 이용하여서는 안되며, 신용정보업자 등으로부터 신용정보를 제공받은 자는 타인에게 그 신용정보를 제공할 수 없다. (제27조)

(3) 정보열람권 및 정정청구권

정보 주체는 신용정보업자 등에 본인에 대한 신용정보의 열람을 청구할 수 있다. 본인의 신용정보가 사실과 다른 경우에는 1차적으로 신용정보업자 등에게 정정을 청구하고, 그 결과에 대하여 이의가 있는 경우에는 처리결과의 통지를 받은 날로부터 15일 이내에 재정경제원 장관에게 시정을 요청할 수 있다. (제25조 제1항)

(4) 공개원칙의 준수

신용정보업자와 신용정보 집중기관은 관리정보의 종류, 이용목적, 제공대상 및 신용정보 주체의 권리 등에 대하여 정기적으로 언론매체를 통하여 공개하여야 한다. (제22조)

(5) 정보운용 체계의 수립

신용정보업자 등은 정보수집, 처리에 대한 보안대책 등에 관한 내부 관리규정을 마련하여야 한다. (제35조) 그리고 신용정보의 정확성과 최신성을 유지하기 위하여 신용정보업자에게 적절한 관리의무를 부과하고 있고, 개인의 불이익을 초래할 수 있는 오래된 신용정보는 대통령령이 정하는 바에 따라 그 기록을 삭제하도록 규정하고 있다.(제18조)

(6) 손해배상청구권

신용정보업자 등이 고의나 과실로 신용정보 주체에게 피해를 입힌 경우에는 정보 주체에게 손해배상의 책임을 져야 한다고 규정하고 있다.(제28조 제1항)

2.3.4. 신용정보법의 개인신용정보 보호의 문제점

신용정보법의 문제점을 지적하는 견해는 크게 두 가지로 구분된다. 첫째, 신용정보의 효율적 이용을 촉진하는 데 있어서 현행법상의 신용정보체계가 부적절하거나 불충분한 부분이 있

다는 것이다. 둘째, 이와는 다른 시각에서 개인신용정보의 보호를 위해서 신용정보주체의 권리가 더욱 강화될 필요가 있다는 견해이다.

우선, 신용정보업자 등은 기업신용정보와 개인신용정보가 통합 운영됨으로써 신용정보체계의 실제적 운영에서 문제점이 발생하고 있다고 지적한다. 특히 기업신용정보는 개인신용정보와는 달리 개인의 프라이버시 침해 위험성이 발생하지 않을 뿐만 아니라 오히려 신용정보이용자인 투자자 보호를 위하여 보다 공개적으로 활용되어야 함에도 불구하고, 현행 법령에서는 개인신용정보체계와 거의 동일한 책임과 의무를 부여하고 있다는 것이다. 또한 우량정보의 공유 제한으로 인해 기업 및 소비자 신용평가의 문제가 발생한다고 지적한다. 특히 고객의 거래실적 등 거래 관련 상세정보를 영업비밀로 간주하여 개별금융기관이 제공을 꺼리는 실정이어서, 채무상환실적이나 신용카드 결제실적 등 우량정보가 공유되지 않음으로써 고객의 신용능력에 대한 정확한 평가 및 판단이 제약받고 있다는 것이다.

위와 같이 기업 및 개인 신용정보의 이용 활성화를 위해서 신용정보체계의 문제점을 지적하는 견해에도 일리는 있으나, 신용정보 수집 및 제공에 있어서 동의 절차 등 정보주체의 권리가 강화되지 않는 상태에서는 프라이버시 침해에 대한 우려와 사회적 논란만을 더욱 증대시킬 뿐이다. 오히려 신용정보 활성화라는 목적을 위해서도 신용정보주체의 자기정보결정권 등을 더욱 명확하게 법률로 규정하는 것이 필요하다.

(1) 자의적 법 적용 가능성

현행법은 신용정보의 처리와 관련된 상당 부분을 시행령이 아닌 ‘금융감독위원회가 정하는 바j’에 따라 처리하도록 규정하고 있어, 매우 자의적인 법집행이 가능하도록 하고 있다. 이에 따라 동일 법률 조항을 자의적 판단에 따라 시기별로 다른 해석을 하거나 업종별로 달리 적용하는 경우가 존재한다. 예컨대 신용정보법 제26조 제7항의 ‘정당한 사유없이 채무자의 관계인에게 연체사실을 통보하는 행위 금지’ 조항을 두고, 2002년 5월 카드사 규제대책 발표 시에는 철저한 처벌을 강조하다가, 2003년 3월에는 카드사 부실 심화를 이유로 카드사에는 적용하지 않는 경우도 있었다.

(2) 신용정보의 수집 시 정보주체의 명시적 동의 부재

이 법률은 신용정보의 수집과 관련하여 금융거래 관련 정보, 질병 관련 정보 등 일부 정보에 대해서만 사전 동의를 의무화하고 있을 뿐, 정보주체의 동의, 혹은 고지 받을 권리를 제대로 보장하지 않고 있다. 신용정보 수집 시 사전 동의를 원칙으로 하고 불가피한 경우에 사후 동의를 얻도록 하는 규정이 필요하다.

또한 신용불량자의 등재 등 신용거래의 안정을 위해 법률에 의해 동의 없이 신용정보를 수

집 제공하도록 되어 있다. 그러나 이 경우에 당사자에게 고지를 하지 않는다면, 정보주체가 이 사실을 모르고 있다가 예상하지 못한 피해를 입을 수 있다.

(3) 신용정보의 제공 및 이용 시 선택적 동의권 불인정

현행법은 개인신용정보 제공에 대한 동의 절차가 형식적으로만 규정되어 있다. 물론 금융기관에서 수집한 신용정보를 신용정보업자등 제3자에게 제공할 때 정보주체의 동의를 거치도록 정하고 있지만, 실제로는 금융계약 관련 서류와 동의서를 통합하여 정보 제공에 동의하지 않으면 금융 서비스 자체를 이용할 수 없도록 만드는 경우가 빈번하다. 따라서 신용정보 제공 및 활용 동의서를 금융거래 계약서류와 분리하고, 동의 여부를 제공 조건으로 삼을 수 없도록 지금처럼 금융감독위원회의 지시 사항으로서가 아니라 법률에 구체적으로 규정할 필요가 있다.

나아가 현행법은 개인신용정보를 제3자에게 제공하거나 목적 이외의 용도로 이용할 경우 동의 기준이 명확하지 않다. 다만 관행적으로 해당사실을 고지하는 행위만으로 동의를 받았다고 여기는 경향이 있다. 명백하게 거부의사를 밝힌 고객을 제외하고는 모두를 동의한 것으로 간주한다는 것이다. 이런 동의 방식이 형식적이고 일괄적인 동의 방식이어서 정보주체의 선택적 동의권이 인정되지 않고 있다. 따라서 동의 절차를 명확히 하고, 또한 신용정보 제공 대상기관별로 따로 동의할 수 있도록 보장할 필요가 있다.

(4) 신용정보의 수집목적 외 관행적 이용

신용정보가 실명확인 등 수집목적 이외의 용도로 관행적으로 사용되고 있다. 이런 문제를 개선하기 위해서 신용정보의 수집 및 이용 범위를 제한하고, 그에 대한 동의 절차를 명확히 할 필요가 있다.

2.3.5. 해외 사례의 검토

신용정보 보호를 위한 법률 체계는 크게 세 가지로 구분된다. 첫째, 별도의 법률로 소비자신용정보를 보호하는 법률이 있는 미국의 경우를 들 수 있다. 둘째, 대부분 유럽 국가들의 경우 신용정보를 별도로 규율하는 법률이 없고, 모든 형태의 개인정보에 대한 일반 법률로써 신용정보를 규율하는 체계를 채택하고 있다. 셋째, 일본과 같이 신용정보와 관련한 일반 상거래에 관한 법률 또는 행정부서의 지침 등을 통해 신용정보를 간접적으로 규율하는 체계로 나눌 수 있다.

미국은 1968년부터 시작하여 몇 차례 법률을 추가하는 과정을 통해 집대성된 소비자신용

법을 통해 신용정보의 보호와 관리 등을 다루어 왔다. 특히 개인신용정보의 보호와 직접 관련된 법률로서 공정신용보고법(Fair Credit Reporting Act)이 1970년 제정되었다. 그 주요 내용으로 신용정보기관의 신용정보제공 업무로 인해 발생하는 소비자의 프라이버시 침해문제와 오류 정보내용의 정정 절차 등을 규정하고 있다. 이 법은 소비자신용조사보고에 대한 범위를 설정하였는데, 대상정보는 소비자의 신용가치, 신용도, 신용능력, 소비자의 성격, 생활형태 등을 포함하였다. 그러나 정보수집 시 특별한 규제가 없어서 개인에 관한 포괄적인 정보수집을 가능하게 하고, 목적 외의 불필요한 정보의 수집에 대해서도 거의 통제가 없었다. 또한 신용보고업자들이 유지 관리하는 정보에 관하여 정보주체의 동의 없는 공개를 금지하였지만, 예외조항이 모호하다는 비판이 제기되었다. 따라서 프라이버시 보호보다는 정보의 정확성에 초점을 맞추고 있다는 비판을 받았다.

이후 이 법은 1996년 개인신용정보의 보호 조치를 강화한 소비자신용보고개혁법(Consumer Credit Reporting Act)으로 대체되었다. 그 주요 내용을 보면, 신용정보를 제공받을 수 있는 기관의 자격 요건, 오래된 정보의 경우 제공 회피, 제공할 정보의 정확성 확인, 신용정보 이용에 대한 정보주체에의 고지 의무, 이의에 대한 재조사 의무 등을 규정하고 있다. 특히 법체계에 예외조항의 모호한 부분을 배제함으로써 개인신용정보 보호의 실효성을 높이고 있다.

이외에도 금융프라이버시법(The Financial Privacy Act, 1978)을 통해 개인의 신용정보에 대한 보호를 규정하고 있다. 이 법은 은행과 기타 금융기관에 대해 정보주체가 자신에 관한 기록에 접근할 수 있도록 허용하고, 정부로부터의 적법한 제출명령 또는 법원의 영장이 없는 한 정부기관에 대하여 금융정보 또는 기록을 공개할 수 없도록 만든 법률이다. 그러나 정부기관만을 공개금지대상으로 정하여 다른 민간주체에 대한 정보공개는 규제하지 않는 한계가 있다.

영국의 경우는 1974년 소비자신용법(Consumer Credit Act)을 제정하여, 신용정보업자에 대해서 본인정보의 열람 및 정정 등에 관한 소비자의 권리를 규정하고 있다. 이후 1984년 개인정보보호의 일반 법률인 데이터보호법에 의하여 부분적으로 규제되고 있다.

대부분 유럽 국가들은 신용정보를 직접적으로 규율하는 법률은 없으며, 개인정보보호의 측면에서 독일의 연방데이타보호법과 같은 개인정보보호 일반법에 의해 부분적으로 규제되고 있다. 따라서 자기정보통제권에 충실하게 보호할 수 있다는 장점이 있는 반면, 신용정보 활용의 측면에서는 한계가 존재한다.

일본의 경우는 개인신용정보에 관한 직접적 규제 법률은 없으며, 다만 일반 상행위를 규제하는 법령이나 관련 주무관청의 행정지시 등에 의하여 간접적으로 규제되고 있다. 1984년 할부판매법과 1986년 3월 대금업의 규제등에 관한 법률 등의 개정으로 신용정보의 적정한 사용 등에 관한 조항을 신설하였다. 또한 대장성이나 통상산업성 등의 통첩(소비자신용정보기관등에 있어서 소비자 신용정보의 관리, 1986년)에 의하여 신용정보기관의 업무 운영, 신용공여기관의 신용정보취급에 관한 사항을 규정하고 있다.

그러나 개인정보에 관하여서는 정보의 이용 및 유통이 급속히 확대되면서 개인에 대한 프

라이버시 침해 가능성에 대한 보호대책이 강구되어야 한다는 사회적 필요성이 증대됨에 따라 법률 및 지방자치단체의 조례 등을 제정하여 개인정보를 보호하고 있다. 1988년 12월에는 '행정기관이 보유하는 전자계산처리에 따른 개인정보의 보호에 관한 법률' 이 제정 시행되었다. 최근 개인정보보호 일반법 제정 논의와 동시에 신용정보에 대한 별도의 법률을 제정하려는 논의가 계속되고 있다.

	미국	일본	한국
법 규	.공정신용보고법(1970), 소비자신용보고법(1996) 제정, 그러나 신용정보 보호에 대한 포괄적인 근거법률 없음	.포괄적인 근거법률 없음 .일반 상거래 및 행정부서의 통달 등에 의해 간접적 규제.	.신용정보의 이용 및 보호에 관한 법률(1995년) .그외 신용정보업무운용규정(금감위), 금융기관의신용정보교환 및 관리규약(은행연합회)
신용정보기관 설립 요건	없음	없음	허가
신용정보기관의 정보수집 및 축적	.본인동의 .회원이 제공한 정보 .공적기록	.본인동의 .회원이 제공한 정보 .공적기록	.본인동의 .회원이 제공한 정보 .공적기록
정보의 제공 및 이용	.목적 외 이용금지(신용정보기관과 이용자간의 계약)	.목적 외 이용금지(신용정보기관과 이용자간의 계약)	.목적 외 이용금지
정보의 유지 관리	.정확성을 확보하기 위한 합리적인 조치	.정확성, 최신성 유지 .비밀유지, 누설, 멸실, 임의 정정방지를 위한 안전대책	.정확성, 최신성 유지 .비밀유지 .제재금 부과
수집 및 제공 금지 정 보	·금지 규정은 없음 ·그러나 신용정보기관의 내부규정(code of ethics)등에 의거 상거래목적 이외의 정보는 취급하지 않음	·통산성 통달 등으로 일부 금지	·국가안보, 기밀정보 ·개인 사생활정보 ·불확실한 개인신용정보
본인정보 열람	·본인정보열람 ·정정, 삭제 요구가능	·본인정보열람 ·정정, 삭제 요구가능	·본인정보 열람 ·정보처리의 중지, 정정, 삭제 요구가능
벌 칙	·민사재판(손해배상) ·형사재판(벌금 또는 징역) ·그러나 소비자와의 계약에 의거하기 때문에 신용정보업자에 대하여 민형사상의 벌	·관련규정 없음 ·그러나 신용정보업자에 대하여 민형사상의 벌칙이 실제로 부과된 사례는 거의 없음	·민사재판(손해배상) ·형사재판(벌금 또는 징역)

	칙이 실제로 부과된 사례는 거의 없음(소송은 다수 제기됨)		
감독기관	·공정거래위원회(聯邦) ·주 법무장관(州)	·통상산업성	·금감위, 금감원
특 징	·소비자보호와 신용정보기관의 발전을 도모 ·기업신용정보에 대하여는 규제가 거의 없음	·개인의 권리 및 신용정보기관의 사회적 역할에 대한 충분한 장치 미흡 ·기업신용정보에 대하여는 규제가 거의 없음	·신용정보산업의 육성과 소비자 보호 ·신용정보의 효율적이고 체계적인 이용 도모 ·소비자신용정보 및 기업신용정보에 모두 규제가 적용

〈표 6〉 미국, 일본, 한국의 신용정보 법률체계

출처: 금융감독원,「주요국의 신용정보 관리제도」

2.3.6. 신용정보법의 개인정보보호 종합 대안

첫째, 신용정보의 수집 및 조사의 원칙(제13조)을 개정하여, 신용정보 수집 시 정보주체의 사전 동의를 원칙으로 하고 불가피한 경우 사후 동의 절차를 규정해야 할 것이다. 특히 신용불량자의 등재 등 법률에 의해 동의 없이 수집할 필요가 있는 경우에도 당사자에게 사후 고지를 의무화할 필요가 있다.

둘째, 개인신용정보의 제공 및 활용에 대한 동의 조항(제23조)을 개정하여, 신용정보에 대한 동의 여부를 금융서비스 제공의 전제조건으로 삼는 행위를 금지하는 조항을 명시할 필요가 있다. 금융거래 개설 서류와 개인정보 제공 및 활용 동의서를 분리하고, 동의서에는 정보제공 대상기관들, 제공 항목, 제공 목적 등을 구체적으로 명시해야 하며, 각각의 제공 대상기관들에 대해 따로 동의 여부를 선택할 수 있도록 해야 한다.

셋째, 재정경제부 및 금융감독위원회 등 행정부서의 자의적 지침에 따라 개인신용정보를 처리하도록 한 규정들을 정비하여 법률로써 구체적으로 규정해야 할 것이다. 향후 개인정보보호법에 의해 설치될 '개인정보보호위원회'로 권한을 위임하여 신용정보보호의 역할을 담당하도록 하는 방안을 적극 고려할 필요가 있다.

2.4. 노동 감시에 대한 규제 법률 제정

2.4.1. 정보사회의 노동감시와 규제 필요성

정보사회의 발전과 그에 따른 다양한 정보통신기술의 발달은 경제 영역에서 효율성과 생산성 향상을 의미하는 것이지만, 다른 한편에서는 노동자에 대한 통제와 감시의 증대를 의미하는 것이기도 하다. 최근 작업장에서 급증하고 있는 노동감시 기술의 도입은 그 이전의 노동통제의 과정과는 다른 새로운 양상을 띠고 있다. 작업장에서 노동행위에 대한 통제가 한층 강화되었을 뿐만 아니라, 개인별 작업수행의 매우 미세한 점까지도 일일이 기록되는 등 노동통제는 세밀하고 일상적으로 벌어지고 있다. 최근 전자감시통제는 작업장뿐만 아니라 식당, 휴게실 등 일상생활 영역에까지 확산되고 있으며, 사무직으로까지 확대되어 이메일이나 홈페이지 이용에 대한 감시를 통해 노동자 개인의 성향에 대해서도 파악하는 일이 늘어났다.

그러나 최근 이러한 전자기술은 엄밀한 중립성과 객관성을 표방하기 때문에 노동자는 기술 앞에서 투명해질 것을 요구받고 있다. 최근 공사업무의 혼용, 기업기밀의 누출 방지라는 이유로 감시체계가 강화되고 있다. 이 때문에 노동감시를 둘러싼 논쟁은 단순히 노동통제의 문제가 아니라 개별 노동자의 양심과 책임의 문제로 환원되는 양상을 보이고 있다. 따라서 작업장 감시 기술의 문제는 노동자의 직접적인 저항에 부딪히거나 쉽게 사회적 문제로 부각되지 않는 것이다. 오늘날 정보기술에서 '감시 기술'을 따로 분리해 내기란 쉽지 않으며, 대개의 경우 생산성 향상과 작업 효율성 증진이라는 목적의 명분 하에서 도입된다. 노동자들은 그러한 기술이 도입된 이후에야 그 기능을 알 수 있고 따라서 사후적으로만 대응 가능한 것이 되고 만다.

그러나 작업장에서 이루어지는 노동 감시기술은 고용주에 의해 단일 목적으로만 사용되는 것이 아니고, 바로 노동자의 프라이버시를 위협하는 경로로 사용된다는 데 문제가 있다. 즉 생산 현장에 생산성 향상·안전사고 방지·기밀유출 방지 등의 목적으로 여러 첨단 기술들이 도입되고 있지만, 이들 기술이 작업장 내 노동자들의 프라이버시를 침해하는 한편 감시와 통제의 목적으로 활용되고 있는 것이다. 첨단 기술을 이용한 최근의 노동감시는 인터넷, 이메일 등 컴퓨터 업무의 감시, 전화 송수신 감시, CCTV 감시, 전자신분증과 생체정보를 이용한 출입과 동선 감시, ERP(전사적자원관리) 시스템을 이용한 밀착감시 등의 형태로 나타나고 있다.

2.4.2. 사회적 쟁점 및 현안 사례

2.4.2.1. 노동감시 실태와 인식 현황

2003년 모 포털사이트의 여론 조사에서 직장인 10명중 4명은 자신이 다니는 회사에서 인터넷 이용을 감시당하고 있다고 생각하는 것으로 나타났다. 1998년 한국노총과 민주노총이 작업장감시조사연구팀과 함께 조사한 결과에 따르면, 조사대상 108개 사업체 가운데 37.1%가

CCTV를 도입했는데, 최근 5년 이내 도입된 경우가 18.6%로 CCTV 감시가 급속도로 확산되고 있는 양상을 보여주었다. 특히 작업공간 이외인 휴게소와 화장실 등에 CCTV가 설치된 비율이 35%에 달해 충격을 주었다.

또한 2003년 '노동자감시 시스템 실태 및 노동자 인식 조사결과' (노동자감시근절연대모임 위탁, 한길리서치센터 조사)를 보면 , 노동자에 대한 감시 시스템 설치 비율이 89.9%로 높게 나타나고 있는데, 이는 노동자에 대한 전자 감시가 우리 사회에서 일반적으로 행해지고 있음을 시사하는 것이다.

그리고 노동자에 대한 감시 시스템을 도입할 경우 두 가지 이상을 도입하는 비율이 높아서, 노동자에 대한 과도한 감시가 이루어질 가능성이 있음을 보여주고 있다. 더욱이 시스템 도입 근거를 보면, '문제발생 시 객관적 근거 마련' (30.6%), '생산과정 모니터링 및 경영혁신' (26.4%), '노동자 기물파손 절도방지' (16.7%) 등으로 나타나 회사의 시스템 도입의 주요 목적이 제대로 달성되지 않고 있으며 실질적으로는 노동자에 대한 감시와 통제를 위한 것임을 보여주고 있다.

그리고 시스템 도입 시 회사와 노동조합 및 현장노동자 사이의 마찰 실태와 시스템 도입 후 노동자 인식 조사를 살펴보면, 주로 작업시간 통제(57.1%), 사생활침해(51.7%), 작업량 증가(42.5%) 등 프라이버시 문제와 노동강도 문제에 대한 우려가 높았다. 이렇게 생산성 향상(16.5%)과 같은 긍정적 변화보다는 부정적 영향이 더욱 큼에도 불구하고, 시스템 도입 과정과 시스템 관리·운영에 노동자와 노동조합이 참여할 제도적 장치(단체협약, 법제도 등)가 없어 노동자의 불안도가 높고, 노동조합의 활동이 위축되는 상황이 벌어지고 있음을 알 수 있다.

2.4.2.2. 작업장 노동감시의 사례

최근 정보기술에 의한 노동통제 및 감시는 다양한 방식으로 이루어지고 있는데, 대체로 인터넷 등 통신이용에 대한 감시, 감시카메라(CCTV)의 설치, 스마트카드 사용, 통합정보시스템의 도입, 최근에는 생체정보기술, 위치추적시스템 등을 이용한 노동감시의 사례 유형이 나타나고 있다.

(1) 정보통신 이용의 감시

직장에서의 컴퓨터와 인터넷, 이메일과 메신저, 그리고 각종 전자장비는 정보처리를 통해 업무를 도와주지만 동시에 작업자의 업무 시간과 작업 진행과정, 행동 등을 낱낱이 기록해서 전달하는 등 업무를 모니터하는 용도로 사용되기도 한다. 또한 정보통신기술의 활용에 대한 통제가 이루어지고 있는데, 여기에는 직접적 감시 이외에도 검색 및 차단 프로그램의 사용 등 정보기술 자체에 의한 감시가 이루어지는 특징이 있다.

. 인터넷 홈페이지 차단: 발전노조(2002.3.-10.), 한국전자통신연구원 노조의 인터넷 홈페이지 접속 차단(2003.3)

. 인터넷과 이메일 사용의 모니터링: 삼성그룹의 시민단체 게시판 글 게시 직원 해고(2001), 스카이라이프 직원 이메일 불법 열람(2002.4), 김포 통진중고등학교 교사의 인터넷 감시(2003.5-7), 한국전자통신연구원 네트워크 불법 모니터링(2002.12), 한국산업기술평가원 노동조합 홈페이지 방문 로그자료를 이용한 직원 감시(2002.11)

(2) 폐쇄회로TV(CCTV)에 의한 작업장 감시

경영자는 생산성 향상, 위험 예방, 고객서비스 등을 명분으로 감시카메라를 작업장에 설치 도입하고 있지만, 실제로는 많은 노동자들이 감시카메라에 녹화된 장면을 근거로 징계나 해고를 당하고 있으며, 노동조합 활동의 탄압에까지 영향을 미치고 있다.

. 외국계 은행 지점에 고성능 CCTV 도입, 직원감시 논란(문화일보, 1998.5.)
. 노동자 CCTV 감시 기승(한계레신문, 20002.8.4.)
. 하에텍 알씨디 코리아의 직장 내 감시카메라 설치, 노조활동 탄압 논란(2002.5.)

(3) 스마트카드등 사용을 통한 노동자감시 및 개인정보축적

스마트카드는 IC메모리와 CPU가 내장되어 암호처리, 접속대상의 인증, 기억데이터의 관리 등 큰 정보처리 용량과 보안기능이 뛰어난 특징을 지니고 있어 신분증명카드, 은행카드, 유료방송수신카드 등으로 사용되고 있다. 그러나 이 스마트카드는 출퇴근 여부, 특정장소 출입 여부, 출입시간 등의 정보가 자동 기록되어 근무통제시스템으로 이용됨으로써, 노동자의 개인정보 보호에 부정적 영향을 미치고 있다는 비판이 제기되었다.

. 창원롯데백화점(2003), 창원시청 청소용역 노동자(2002), 보쉬기전(2003.8), 한국산업기술평가원(2002.11) 등에서 지문인식기, 스마트카드와 같은 출입통제시스템 도입 논란

(4) 전사적자원관리시스템(ERP) 등 통합정보시스템 도입에 의한 노동감시

전사적자원관리시스템은 기업이 보유하고 있는 자재, 설비, 자금, 인력, 정보 등 각종 유무형의 자원을 전사적으로 통합 관리하는 소프트웨어를 도입하여 기업의 전체 업무와 자원을 통합적으로 관리하는 경영방식 또는 통합정보시스템을 의미한다. 이러한 시스템의 도입은 경영자와 관리자의 모니터 화면에 생산된 제품의 실시간 정보를 나타나게 함으로써 모든 노동자의 개인별, 팀별로 생산된 정보와 일일 생산량을 확인하게 할 뿐만 아니라, 성과의 달성자와 미달성

자에 대한 차별구조의 확립으로 이어진다.

. 전북대 병원의 ERP 도입 논란(2003.7)

(5) 생체정보를 이용한 노동감시

생체정보기술은 정맥인식, 지문인식, 홍체인식, 얼굴인식, 음성인식, 서명인식, 유전자정보 등을 포함한다. 이 기술은 외부인의 무단 이용을 통제하고 운영의 효율성을 꾀한다는 명목으로 작업장 및 식당, 휴게실 등에 도입되었지만, 이 역시 노동자의 업무행위에 대한 통제로 이용되고 있다.

. 정맥인식기 등 생체인식기술을 통한 노동자 감시, 부산 F공장 사례(한국일보, 2001.7.26.)

(6) 위치추적시스템을 이용한 노동감시

최근 이동전화나 PDA 등 위성위치확인시스템(GPS)을 이용한 위치추적시스템은 개인이나 사물의 위치를 파악함으로써 개인의 활동영역과 활동내용을 파악할 수 있다. 고객서비스 강화나 서비스 품질의 개선이라는 명목으로 개인의 위치정보가 직장에서 근무평정 등에 활용되어 노동강도를 높이게 될 가능성이 높다. 뿐만 아니라 개인의 위치정보를 실시간으로 수집하여 분석함으로써, 노동자의 성향 파악이나 노조활동의 통제에 이용될 우려를 낳고 있다.

. 택시 등의 위성위치추적시스템을 통해 현재 위치와 속도, 손님 유무, 요금계산 유무 등의 실시간 추적 감시
. 삼성SDI, 직원 휴대폰 불법복제 통한 위치정보 추적 피소(한겨레신문, 2004.7.)

2.4.3. 현행 법률 및 제도의 현황

현재 노동자의 개인정보 처리나 작업장 감시 시스템과 관련하여 이를 특별히 규정하고 있는 포괄적인 법률은 아직 없고, 다만 노동관계법과 다른 법률에서 부분적으로 규정되고 있을 뿐이다.

헌법 17조에서 모든 국민은 사생활의 비밀과 자유를 침해받지 않는다고 규정하고 있다. 넓게 보아 초상권과 명예권도 여기에 포함되므로 작업장에서 CCTV에 의한 무단감시 행위도 위반행위가 될 수 있다. 또한 18조에서 통신의 비밀을 침해받지 않는다고 규정하고 있는데, 통신

에 해당하는 모든 유형의 노동행위에 대한 사용자의 감시행위는 불법이라고 해석할 수 있다.

통신비밀보호법에서 감청범위는 유선전화, 이동전화, 무선호출, 통신 등이 포함된다. 따라서 작업장 내에서 동의없는 이메일 감시행위는 동법 2조7호에 의한 감청행위로 간주되어 7년 이하의 징역에 처해질 수 있다.

정보통신망이용촉진등에관한법률에서는 고용주가 종업원의 전자우편을 열람하는 행위에 대해 동법28조에 의거하여 5년 이하의 징역, 5천만원 이하의 벌금에 처해질 수 있다

한편 노동관계법은 노동자의 프라이버시 보호를 구체적으로 명시하지 않고 있으나, 인격, 인권 침해에 대한 방지 의무를 부과하고 있다.

작업장 내의 노동자감시가 헌법에서 보장하고 있는 노동자로서의 존엄과 프라이버시권, 그리고 노동3권을 침해할 수 없도록 이를 구체적으로 규제하는 규제 입법이 이루어질 필요가 있다. 이를 위해서는 노동관계법률을 정비하는 한편, 독자적인 노동자감시의 규제 입법화도 고려해야 할 것이다.

2.4.4. 현행 노동감시 규제 법률 및 제도의 문제점

(1) 노동감시 규제입법의 필요성

현재 노동자의 프라이버시 보호 및 인권을 위한 구체적인 입법은 거의 없는 실정이다. 예컨대 현재 사업장에서 행하는 다양한 노동감시 시스템은 그 수단의 다양성과 다른 법률과의 관계로 인하여 현행 법체계로는 노동자의 효과적인 프라이버시 보호를 기대할 수 없는 실정이다. 따라서 노동자에게 특수한 개인정보 보호 조치와 집단적 참가 등 강력한 규제를 바탕으로 하는 관련 법률의 입법추진을 통해 사업주와 노동자간의 이해를 조정할 필요가 있다. 또한 통신비밀보호법 등 다른 법률에서 미처 규정되지 못한 CCTV나 생체정보기술 등 다양한 노동감시 수단을 포괄하는 독자적인 노동감시 규제입법이 요구된다고 하겠다.

(2) 정보주체인 노동자의 개인정보통제 권리 및 참여 배제

직장 내 감시 기술에 대한 정확한 정보 공개가 이루어지지 않고, 기술의 도입과 운영에 있어 정보 주체인 노동자의 참여가 배제되어 있기 때문에 노동자들은 감시의 대상으로 전락하고 있다. 특히 정보관리시스템의 도입 시 자신에 대한 정보가 어떻게 수집, 처리, 관리, 재가공되는지를 명확하게 알 수 있어야 한다. 따라서 인권침해 종류의 기록금지, 개인정보수집방법의 제한, 개인의 의사에 반하는 입력의 금지, 개인정보의 무제한 축적의 금지, 자기파일에 대한 접근권의 보장, 개인정보의 정정권 보장, 개인정보에 대한 남용 금지 등이 명시될 필요가 있다.

(3) 집단적 참가 및 역감시권의 부재

현실적으로 기업이 개별 정보주체에 비해 압도적인 정치적, 경제적 힘을 행사할 수 있는 권력 불균형 상태가 존재하기 때문에, 노동자의 자기정보통제권을 실현할 책임을 개별 정보주체에 완전히 맡기는 것으로는 불충분하다. 개인정보의 수집 및 노동감시 장비의 도입 시 단체협약 등 명시적인 집단적 협의 조항이 없는 상태이다. 따라서 고용주의 개인정보 수집 및 처리 행위에 대해 집단적으로 협의하고 감독할 권리가 보장될 필요가 있다. 즉 보다 적극적인 권리로서 역감시권은 사용자의 권력에 대하여 반대를 주장하고 철회를 요구, 관철시킬 수 있는 권리를 말한다. 이를 위해서는 정보수집자에 대항하여 정보주체들이 집단적으로 권리 행사를 할 수 있게 해야 하며, 정보주체 단체를 구성할 권리를 가져야 한다.

2.4.5. 해외 사례의 검토

(1) 노동감시 실태

국제노동기구(ILO)는 1993년 각국의 작업장내 전자노동감시 실태를 조사 보고한 바 있다. 이 보고서에 의하면, 미국의 경우 이미 노동자의 1/6에 해당하는 2천만명이 전자장치의 감시를 받고 있는 것으로 나타난다.

미국 경영자연합(AMA)은 2001년 조사에서 미국 기업의 77.7%가 노동자의 전화사용, 이메일, 인터넷 이용, 그리고 컴퓨터 파일 등을 감시한다고 발표했다. 이 수치는 1997년 35.3%에 불과했던 것에 비해 급격히 늘어난 것이다. 감시방법 중에서는 인터넷 접속이나 이메일 감시가 각각 62.8%와 46.5%로 가장 많았고 통화에 대한 정보기록 43.3%, 비디오 촬영 37.7%, 직원 컴퓨터 파일 검토 36.1% 등이 뒤를 이었다. 2002년 11월 발표한 최근 조사에서 전체 감시 수치는 82%로 올라갔다.

미국의 민간단체인 프라이버시재단에서도 2001년 미국 온라인 노동자는 35%(1천4백만명)이, 전세계의 경우 27%(2천7백만명)가 현재 온라인 감시를 받고 있다고 밝혔다. 인적관리협회(the Society for Human Resource Management)와 웨스트그룹(the West Group)의 조사에서는 2001년 72%의 기업이 노동자의 이메일 이용을 감시하고 있었으며, 51%의 기업은 전화를 감시하고 있는 것으로 나타났다.

일본의 경우 2002년 조사에서 일본 제조업체 42%가 노동자들의 이메일을 감시하고 있으며 38%가 도입할 계획을 갖고 있어 약80%의 기업이 이메일을 감시하거나 감시할 예정으로 나타났다.

(2) 각국의 입법

국제노동기구(ILO)의 ‘노동자의 개인정보 보호에 대한 행동강령’(1995)은 노동자의 존엄성과 프라이버시를 보호하기 위한 국제적 기준을 제시하고 있다. 특히 노동자 자신이 누가 어떤 정보를 어떤 목적으로, 그리고 어떤 조건 하에서 사용할 것인지를 결정할 수 있는 기본적인 권리를 보장하고 있다. 여기에는 고용주가 노동자의 정치성향등에 관한 사항을 국가기관에 넘기거나 노동자의 전화통화를 감시하는 등의 행위가 사생활 침해에 해당된다고 규정되어 있다. 또한 합리적인 선에서 작업장 내 노동자의 행동을 감독하는 것은 허용되지만, 카드나 배지 등을 강제로 착용시켜 작업장 내의 모든 움직임을 세밀하게 통제 감시하는 행위도 위반이라고 규정하고 있다.

1) 프랑스

프랑스 노동법은 "어느 누구도 개인의 권리를 제한할 수 없다. 이를 제한하기 위해서는 그 제한이 정당하고 적절한 범위 내여야 한다"라고 되어있어 프라이버시권을 침해하는 사용자에 대해 법적 조치를 취할 수 있다. 특히 노동자에게 알리지 않은 방법으로 노동자의 개인정보를 수집하는 것을 금지하고 있다. 또한 노동조합 활동에 관한 감시를 엄격히 금지하고 있다. 사용자는 은밀한 감시로 알아낸 노동조합 활동 사실을 근거로 노동자를 해고하거나 징계할 수 없다.

노동자의 프라이버시를 침해하는 행위가 적법하려면 매우 엄격한 판단을 거쳐야 한다. 프라이버시 침해행위가 적법하기 위해서는 문제되는 프라이버시 침해행위가 노동자가 수행하는 업무와 관련성이 있어야 하고, 그 방법은 목적에 합당한 것이어야 한다. 프라이버시권은 가장 핵심적인 권리이기 때문에 고용관계에서도 희생되어서는 안된다는 것이다. 따라서 노동자가 동의를 하였다거나 침해적인 감시행위를 묵인했다는 사실만으로 프라이버시권의 침해가 정당화될 수는 없다.

또 1991년 통신비밀법에 의하면, 사용자는 사법부의 영장에 의하지 않고는 작업장에서 노동자의 개인적인 통신에 접근할 수 없다. 프랑스 대법원은 노동자에게는 프라이버시권이 있고 이것은 사업자가 노동자에 의해 송수신된 개인적 메시지의 내용에 접근할 수 없다는 의미라고 판시한 바 있다. 프랑스 민법 제9조는 사업장에서 비밀스런 감시 도구의 사용을 금지하는 것으로 해석된다. 나아가 사용자는 위법하게 수집한 정보를 가지고 노동자를 징계하거나 해고할 수 없다. 안전 목적으로 감시가 적법하게 이루어지는 경우에도 안전 문제와 무관한 모든 말과 행동을 감시하는 경우에는 위법이다.

노동자 프라이버시권을 보호하는 기관은 '국립정보자유위원회'이다. 국립정보자유위원회는 정보프라이버시법(1978)에 의해 설립되었는데 작업장 프라이버시 문제에 대해 법률적으로 구속력이 있는 의견제시와 권고를 하고 있다. 특히 공공부문 사용자가 전자적인 사업장 감시 시스템을 설치하고자 하는 경우 국립정보자유위원회의 사전 승인을 얻어야 한다. 노동자 11명

이상의 사업장에서는 '노동자위원회'가 노동자 프라이버시 보호의 책임을 맡는다. 사용자는 새로운 기술을 도입하거나 감시도구를 비롯해 노동자의 활동을 통제할 수 있는 수단을 도입할 경우 미리 노동자위원회에 알리고 협의를 해야 한다. 만약 사용자의 대응이 부적절하거나 합의하지 못할 경우 노동자는 노사심판소에 조정신청을 할 수 있고 심판소는 가처분 결정이나 금전배상을 명할 수 있다.

2) 독일

독일 연방노동법원은 헌법상의 인격권 조항에 따라 노동자의 프라이버시권을 인정하고 있으며 이는 노동자평의회와 회사의 단체협약에 의해서도 보호되고 있다. 공공부문 노동자는 작업성과를 측정하거나 노동자 행동을 감시할 수 있는 도구를 도입하거나 운영하는 문제를 결정하는데 참여할 권리가 있다. 이메일이나 인터넷 사용을 감시할 수 있는 도구를 도입할 때도 마찬가지이다. 또 경영조직법에 따라 사용자와 노동자평의회는 정보통신기술의 활용으로 노동자의 프라이버시가 침해되는 데 대해 보호 수단을 마련할 의무를 갖는다. 단체교섭에서 노동자 감시에 대해 합의가 이루어지지 않을 경우 사용자와 노동자평의회는 노동자 감시 도구의 도입이 가져올 문제점에 대해 전문가의 도움을 받아 합의해야 한다. 연방노동법원은 그 도구가 직접 노동자의 행동을 감시하기 위한 것이건 결과적으로 그러한 것이건 노동자를 감시하는 도구가 도입될 때는 사용자와 노사평의회가 공동으로 결정해야 한다고 명시했다. 한편 독일에는 직장에서 유전자검사를 금지하는 법률이 제정되어 있다.

3) 영국

영국은 2000년 8월에 통과된 '조사권한규제법'에 의해 사업자가 통신의 송신자와 수신자 양쪽의 동의를 구하지 않고 전화와 이메일을 감청하는 것을 위법이라고 규정하고 있다. 이외에도 작업장내 프라이버시 보호와 관련한 법률로 데이터보호법(1998)이 있으며, 영국정보보호위원회에서는 사업자와 노동자의 관계에서 개인정보이용에 관한 실무규정 초안을 만들어 협의중에 있다. 이 실무규정의 주요 내용으로 ①사업자는 개인정보 수집에 있어서 정당한 사유와 분명한 목적 하에서만 수집하고 사전에 노동자에게 알리고 동의를 구해야 하며 ②노동자는 사업자를 통해 그가 보유하고 있는 자신에 대한 데이터의 내용, 용도, 의도를 정기적으로 통보받아야 하며 ③특별히 민감한 데이터는 해당법의 특별한 통제를 받는다. ④노동자의 범죄기록, 유전자 검사는 특별한 제한을 두며 ⑤작업장 감시는 정당한 사유를 가지고 사전에 통보하며, 감시장치는 눈에 보이는 곳에 설치할 것 등에 대해서 규정하고 있다.

4) 미국

미국의 연방 및 주헌법이 보장하고 있는 프라이버시권은 정부행위에 의한 침해를 전제로 하기 때문에 민간부문에 대해서는 원칙적으로 적용되지 않는다. 이메일 검색과 관련된 연방법으로는 1986년 제정된 전자통신프라이버시법이 있다. 이 법률은 전자통신의 도청을 금지하는 법으로 해석되어 이메일에 적용되기도 하지만, 직장에서 고용주의 이메일 검색행위에 적용될 수 있는지는 논란이 되고 있다. 이외에 코네티컷주의 EMAUP, 의회에 상정된 법률안으로서 전자모니터링 고지법, 전자통신 프라이버시법 개정(2000) 등이 작업장 프라이버시 보호와 관련해서 언급되고 있다. 미국의 경우 전자적 모니터링 등 노동자의 프라이버시 관련 문제들은 많은 판례들에 의해 다루어지고 있다.

5) 그 외의 국가들

벨기에, 덴마크는 노동자 의료정보와 의료검진에 대해 특별보호규정을 두고 있다. 핀란드에는 노사관계에서의 프라이버시 보호에 관한 특별입법이 제정되어 있다. 이탈리아에는 노동자에 대한 감시와 모니터링을 제한하는 특별규정이 있다. 노동자의 이메일 내용에 사업자가 접근하기 위해서는 사법부의 명령이 있어야 한다. 네덜란드는 노동법에서 노동조합에 정보를 제공하고 동의를 받아야 한다고 규정하고 있다. 스웨덴은 카메라 감시장비를 도입할 경우 노동조합 대표와 협의해야 한다는 법률규정이 있으며 노동자의 작업수행을 감시할 때는 당사자에게 알려야 하고 사전에 의무적으로 노동조합 대표의 의견을 들어야 한다. 노르웨이의 경우도 직장을 감시하는 경우는 이를 단체협약사항으로 노동조합의 대표에게 알리고 협의를 거쳐야 한다.

2.4.6. 노동감시의 규제 종합 대안

(1) 관련 법률의 개정 및 독자적 입법화

첫째, 노동조합및노사관계조정법을 개정하여, 노동자 감시기술의 도입을 단체협약의 필수협의사항으로 명문화할 필요가 있다.

둘째, 근로기준법을 개정하여 채용, 구직, 취업, 재직, 퇴사의 경우와 작업과정 및 사외활동 등에서 노동자의 개인정보 보호를 위한 규정을 명문화할 필요가 있다.

셋째, 노사정위원회법의 개정을 통해 노동자 감시기술을 협의대상 목록으로 명문화할 필요가 있다.

넷째, 이러한 노사관계법의 개정 이외에도 시민사회단체등이 제안하고 있는 ‘노동자감시근절과개인정보보호를위한특별법’(안)을 제정할 것을 신중히 검토할 필요가 있다.

(2) 노동감시의 규제를 위한 실질적 방안

첫째, 노동관계법의 개정이나 독자적인 입법화를 통해 노동자의 개인정보에도 일반적인 개인정보 보호의 원칙이 적용될 수 있어야 하며, 동시에 회사에 고용관계로 매여 있는 노동자의 특성에 대한 충분한 고려가 이루어져야 할 것이다. 즉, 목적명확성의 원칙, 당사자 참여의 원칙, 목적 외 사용 금지의 원칙, 안전보장의 원칙, 책임의 원칙 등 기본적인 원칙은 물론, 사업장에서의 집중 감시의 금지, 불이익 금지, 입사 및 퇴직 시 개인정보의 보존 한계 등이 구체적으로 명시되어야 한다. 이는 채용, 구직, 근로계약 등의 모든 과정에서 보장될 수 있어야 한다.

둘째, 노동자감시에 관한 기술적 사항 일체는 단체협약에서 우선협상대상으로 인정되어야 한다. 경영기법의 일환으로 도입되었다 할지라도 결과적으로 노동자감시와 통제에 이용될 수 있는 기술 등은 단체협상에서 논의되어, 이 기술에 따른 노동자 탄압과 차별이 일어나지 않도록 보장해야 할 것이다.

셋째, 노동자의 개인정보 보호를 위한 회사의 책임이 보다 명확해져야 할 것이다. 개인정보의 수집, 보관, 활용 모든 곳에서 부당한 처우나 불법적 활용에 수집정보가 활용될 수 없도록 해야 하며 수집 활용되는 모든 정보에 대해 정보 주체인 노동자들이 직접 확인하고 관리할 수 있도록 보장하여야 한다.

넷째, 프라이버시 영향평가 제도를 도입할 필요가 있다. 특히 작업장에 도입되는 기술이 감시 등 노동 조건에 중대한 영향을 끼칠 우려가 있을 경우 그러한 기술의 도입 전에 사전 프라이버시 영향평가를 제도적으로 보장하고, 기술의 도입 및 운영에 대한 의사결정 과정에 노동자의 참여를 보장해야 할 것이다.

3. 프라이버시 보호를 위한 현안 문제

3.1. 스팸메일의 규제

3.1.1. 스팸 메일의 정의 및 범주

3.1.1.1 스팸 메일의 정의

스팸 메일이란 수신자의 의사와 관련 없이 일방적으로 전달되는 광고성 전자우편을 뜻한다. 일반적으로 스팸 메일은 “발신자가 동의 없이 일방적으로 수신자에게 원치 않는 메시지를 전송한 것”으로 볼 수 있다. 또한 ‘정보통신망이용촉진및정보보호등에관한법률’ 50조에서는 수신자의 거부의사에 반하여 전송되는 영리목적의 광고성 전자우편 및 수신자의 동의 없이 전송되는 영리목적의 광고성 전자우편을 스팸 메일로 규정하고 있다. 따라서 발신자가 동의 없이 일방적으로 수신자에게 원치 않는 메시지를 전송한다는 의미에서 스팸 메일은 프라이버시 침해 등의 법적 문제가 발생하게 되는 것이다(강장묵 외. 2003).

이러한 일반적인 개념으로 스팸 메일을 살펴볼 때, 스팸 메일은 다음과 같은 기본적인 특성을 내포하고 있다.

– 원하지 않음

스팸 메일의 가장 중요한 핵심은 메시지를 수신자가 원하지 않고 있다는 것이다. 즉 수신자가 메일이나 메시지의 수신을 동의하지 않았거나 수신자가 상대방에게 수신 거부 의사를 밝힌 경우를 뜻한다.

– 상업적

메일이나 메시지의 내용이 재화나 용역의 판매를 목적으로 이루어진 것이라면 이 메시지도 스팸 메일로 간주될 수 있다. 그러나 아직 상업적인 용도의 의미에 대해서 논란이 많은 실정이어서 이에 대한 가이드라인을 설정할 필요가 있다.

– 대량

실제적으로 수신자가 느끼는 현실적인 것은 메일이나 메시지의 내용보다는 그 대량성에 있다고 해도 과언이 아니다. 현재 대량의 스팸 메일 발송은 기술적 방법을 통해 판별해내기가 어려울 정도로 정교화 되었기 때문에 대량성 판단을 위한 기준이 필요한 실정이다.

즉 스팸 메일이란 상업성을 가진 원하지 않는 전송 정보 및 원하지 않는 대량의 전송 정보를 의미한다.

3.1.1.2. 스팸메일의 유형

통신 기술의 발달로 무선 인터넷, 팝업창, 메신저, 휴대폰 등 불건전 정보가 유통되는 경로가 다양화되었다. 이에 이 연구에서 사용하는 스팸 메일은 단순히 인터넷으로 유통되는 것만을 뜻하는 것이 아니라 휴대폰 문자 메시지 및 메신저 팝업창, 전화, FAX 등에서 유포되는 정보 연구대상으로 포함한다. 뿐만 아니라 현재는 외국어 스팸을 비롯해 P2P, 게시판 등 새로운 매체를 통한 스팸도 확산되고 있는 시점이어서 국내 뿐 아니라 국외적으로도 이에 대한 대응이 필요한 시점이다.

3.1.2. 주요 현안

스팸 메일은 전자 상거래 업체 등 메일 발송자들이 적은 비용으로 영업을 할 수 있다는 이점을 가지고 있으나 스팸 메일을 지우는 시간과 이용자의 양해를 구하지 않고 이용자가 통제할 수 없는 방식과 양으로 이용자의 메일계정으로 쏟아져 들어온다는 점과 본인의 메일 계정이 본인도 모르고 있는 사이에 팔리고 있다는 점에 대해 정보주체는 아무런 통제권이 주어지지 않는다. 그리고 스팸 메일은 여러 가지의 제도적, 규제적, 기술적 제재를 가하고 있음에도 불구하고 일방적인 방향성을 지니고 있어 개인에게 지속적인 프라이버시 침해를 야기 하고 있다. 또한 여러 정보통신 매체의 발달로 인해 위에서 살펴보았듯이 다양한 채널을 통해 더더욱 확산되고 있다.

3.1.2.1. 스팸 메일 현황

. 해고 앙심 500만통 스팸 메일을 불특정 다수에게 발송하였다(영국 사례, 한겨레, 2004. 7. 15).

. 스팸 메일 급증 – 4월 한달 간 3만6000건 발생하였다(세계일보. 2004. 6. 23).

. 전체 메일의 76% 스팸 메일(한겨레. 2004. 6. 10. 뉴욕/AFP 연합외신)

. 스팸 메일로 인한 피해는 연 5조 9억원. 스팸 메일 지우는 시간 비용은 1인당 13만원 꼴로 조사되었다. 그리고 4월 21일, 나라리서치가 인터넷 사용자 679명을 대상으로 스팸 메일 사용에 관해 실태조사를 한 결과 연간 스팸 메일을 수신하는데 1조 7494억원, 저장하는데 668억원, 삭제하는데 3조 1849억원이 소요되어 인터넷상의 광고 메일로 인한 연간 손실이 5조 9억원에 이르는 것으로 나타났다(세계일보. 2004. 4. 22).

. 스팸 메일 사회적 비용 年2조 6000억로 그 중 30%가 음란물인 것으로 나타났다(동아일보. 2004. 2. 26).

. 수사검사 휴대폰에까지 스팸 메시지를 무차별로 발송한 폰팅업체를 무더기로 적발하였다

(한국일보. 2004. 1. 20) : 불특정 다수에게 휴대폰 폰팅 메시지 발송을 남발하여 10억~37억 원을 벌어들인 혐의로 폰팅업체 대표 구속하는 사례가 발생하였다.

. 2002년도 4월에 발표된 <함께하는 시민행동>의 조사에서 약 6,500명의 응답자 중 82.6%가 수신동의하지 않은 광고메일은 무조건 혹은 대부분 읽지 않고 삭제한다고 답하였다(진보네트워크. 2002).

. 스팸 메일의 유통현황에 대한 통계자료를 살펴보면 다음과 같은 추이과정을 알 수 있다.

구분	2001년	2002년	2003년 4월
연간 총 유통건수	329억통	2,816억통	1,343억통
1일 평균 수신건수	4.7통	34.8통	39.4통
음란 스팸 수신건수	0.9통	21.3통	24.8통

<표 6> 스팸 메일 유통현황(추정)
출처: 한국정보보호진흥원 자료

스팸메일의 연간 총 유통건수는 2년 사이에 1,000억 통 가까이 늘었으며, 1일 평균 수신건수에서 음란 스팸이 차지하는 비율도 2001년 18.5%에서 2003년 63%로 크게 증가하고 있음을 살펴볼 수 있다.

또한 2004년 4월 기준으로 한국정보보호진흥원 스팸대응연구팀에 접수된 상담 및 신고건수는 3만 5,982건으로 지난 1월 2만 4,022에 비해 50% 이상 급증하였다. 뿐만 아니라 4월 신고 메일 가운데 외국인 신고건수도 1만 4000여건이 넘는 것으로 집계된 상태이다(세계일보. 2004. 6. 23).

그리고 하루 700만통, 연간 25억 5,000만통의 휴대폰 스팸 메시지 가운데, 80%인 20억통이 폰팅업체에서 발송되는 것으로 조사되었으며, 휴대폰 스팸 메시지의 삭제 과정 및 발송 비용에 있어 사회적 손실이 연 3,000~4,000억원으로 추산되는 것으로 나타났다(한국일보. 2004. 1. 20).

3.1.2.2. 스팸 메일 규제 사례

최근 늘어나고 있는 스팸 메일에 대해 정보통신부는 과태료 및 제도 개선, 기술 개발 등으로 스팸 메일을 규제하고 있다. 그 사례는 다음과 같다.

. 스팸 메일 차단기술 개발과 스팸 메일 과태료 금액 상향 조정 등으로 스팸 메일 수신량 50% 감소할 것으로 예상된다(정보통신부) - 2004. 7. 13(연합뉴스. 개인정보보호 관련법 대폭 정비).

. 현재 스팸 메일에 대해서는 옵트 아웃(선택적 거부), 문자 메시지에 대해서는 옵트 인(선

택적 수용) 방식 사용하고 있다(경향신문, 2004. 7. 10)

. 스팸 뿐 아니라 단문 메시지 및 유·무선 전화도 포함하여 수신 거부 미확인 스팸 메일에 과태료를 부가하였다(세계일보. 2004. 7. 7) - '전자상거래 등에서의 소비자보호에 관한 법률' 개정안을 확정, 올 가을 정기국회에 상정할 예정이다.

. 휴대폰 · 팩스 스팸 광고 3000만원 과태료..정통부, 내년부터 수신자 동의 의무화할 예정이다(세계일보. 2004. 4. 22).

3.1.3. 현행 법률

스팸 메일과 관련된 법령은 "정보통신망이용촉진및정보보호등에관한법률"에서 살펴볼 수 있는데, 그 구체적 사항은 다음과 같다.

·제50조(광고성 정보전송의 제한) ①누구든지 수신자의 명시적인 수신거부의사에 반하는 영리목적의 광고성 정보를 전송하여서는 아니된다.

②제1항의 규정에 의한 영리목적의 광고성 정보를 전자우편으로 전송하고자 하는 자는 정보통신부령이 정하는 바에 의하여 다음 각호의 사항을 전자우편에 명시하여야 한다.

1. 전송목적 및 주요내용
2. 전송자의 명칭 및 연락처 등
3. 수신거부의 의사표시에 관한 사항

3.1.4. 시민단체 및 정부의 입장

정보통신망을 활용하는 기술의 발전에 따라 인터넷 이용자들이 겪는 프라이버시 침해도 차츰 더 심각해지고 있다. 시민단체는 스팸 메일 뿐 아니라 위에서 지적하였던 휴대폰 단문 메시지, 팩스 등을 이용한 광고가 야기하는 물질적·정신적 피해는 이미 오래 전부터 지적하여 왔다. 그러나 이에 대해 정보통신부 뿐 아니라 다른 정부 부처, 그리고 구체적 수준에까지 대책을 마련하고 있는 추세이나 그럼에도 불구하고 여전히 스팸 메일이 줄어들지 않는 것은 기본적으로 정보통신망이용촉진및정보보호등에관한법률 50조가 옵트 아웃(선택적 거부) 방식을 인정하고 있기 때문이다.

이에 대해 정보통신부에서는 정보통신망이용촉진및정보보호에등에관한법률의 개정안을 마련하여 국회에 상정하기로 결정하였다. 개정안에는 2005년부터 휴대폰 및 팩스를 통해 수신자의 사전 동의 없이 광고를 하면 3,000만원 이하의 과태료 및 옵트 인(선택적 수용) 제도를 도입하도록 하고, 오후 9시부터 그 다음 날 오전 9시까지는 동의를 받았더라도 발송을 금지하도록 하는 내용이 포함되어있다. 또한 이메일 주소 추출기 등 불법 스팸 메일 전송을 조장하는 기

술 물론 전자우편주소를 수집해 이를 판매·유통하는 행위도 전면 금지하고 이를 위반할 경우 1,000만원 이하의 벌금을 물도록 규정하였다.

또한 정보통신부는 전자정부전문위원회와 협의해 “정보통신망및컴퓨터등으로처리되는개인정보보호에관한법률”을 제정하기로 했다고 2004. 7. 13일 밝혔다. 정보통신부는 특히 법 적용 대상을 온라인에서 유통되는 개인정보 뿐 아니라 컴퓨터, CCTV 등 정보기기를 활용해 처리, 이용하는 개인정보까지 확대하기로 하였다. 그리고 개인정보보호 의무 대상자를 정보통신서비스 제공자에서 영리목적으로 개인정보를 취급하는 사업자로 확대하여 그동안 정보인권의 사각지대를 해소하기로 하였다.

3.1.5. 해외사례의 검토

(1) 미국

미국은 주 및 연방 차원에서 스팸 메일 방지 관련 법안을 시행하고 있다. 이 법안은 자율 규제를 통해 마련된 것으로 소비자 단체, ISP, 전자상거래업체, 광고마케팅 업체 간의 협상을 통해 이루어졌다. 이러한 협상에서 결정된 사항은 다음과 같다. 첫째 무단 상업적 전자우편의 전송요건과 라우팅 관련 금지사항과 위반에 대한 조치 사항을 규정하였다. 둘째 무단 상업적 전자우편을 발송할 때에는 반드시 반송주소를 포함하고, 전자우편에 있어서 무단 상업적임을 표시해야 하며, 수신거부 의사에 더 이상 전자우편을 발송하지 않을 것임을 명확히 하고 수신 거부 할 경우에는 더 이상 전송해서는 안된다(옵트 아웃(선택적 거부) 제도). 셋째, 무단 상업적인 메일로 인해 발생한 실제적인 금전 손실액 또는 위반 건수마다 500달러, 총액 50,000달러의 금액을 받기 위한 소송을 제기할 수 있으며, 악의적, 고의적, 반복적인 위반을 했을 경우 위 금액의 3배까지 가능하도록 규정하였다.

<참고 2> 미국 아리조나 주법, 텍사스주법, 국내 스팸법과의 비교(이상헌. 2003)

원하지 않은 영리목적의 전자우편 전송 시 전자 우편의 제목을 특정한 단어나 문장으로 시작하도록 제한하고 있다는 점에서는 세 개의 법이 모두 동일한 특징을 가지고 있다. 국내법은 전자우편주소의 불법 생성, 불법 수집에 대한 규제를 하고 있으며, 미국의 두 개 스팸법에서는 국내법에서는 존재하지 않는 민사소송에 관한 규정이 있다. 옵트 아웃(선택적 거부) 방식에 있어서, 국내법은 수신자의 수신거부를 택하고 있으며, 아리조나 주 법과 텍사스 주 법은 전송자의 전자우편 목록에서 수신자 전자우편주소의 삭제에 중점을 두고 있으며, 삭제 기간까지 명시한 점이 특이하다. 옵트 인(선택적 수용) 방식과 관련된 법은 국내법 뿐 아니라 두 개의 미국 주법에도 없는 것으로 나타났다.

(2) 호주

호주는 자율적인 노력을 강구하는 방식으로 인터넷 사업자 연합회의 지침을 마련하였다. 이 지침의 내용은 스팸 메일을 발송 혹은 조장해서는 안되고, 메일 수신에 대해서는 옵트 아웃(선택적 거부) 선택권을 부여하고 있으며 인지된 메일에 대해서도 불건전한 정보를 포함해서는 안된다. 각 회원사는 스팸 메일 방지에 대한 정책을 수립하고 있어야 하며, 스팸 불만 신고 연락처 명시 및 메일 릴레이에 대한 보호 장치를 설치해야 함을 고지하고 있다.

호주, 미국, 영국의 경우, 호주 통신청(ACA)과 호주 경쟁소비자위원회(ACCC), 미국 연방거래위원회(FTC), 영국 통상산업부(DTT), 영국 정보 커미셔너, 영국 공정거래청(OFT)과 협력하여 각 국을 드나드는 스팸 메일에 대한 대책을 마련하고 있다.

(3) 유럽연합

유럽연합은 1995년 “The European Union Directive95/46/EC” 제정과 1997년 “Directive 97/66/EC of The European Parlia ment and of the Council of 15 December 1997”을 통하여 정보통신부문에 있어서 개인 정보처리 및 프라이버시보호에 관한 지침을 마련하였다. 하지만 이 법 조항 내에 스팸 메일에 대한 지침은 존재하지 않았다. 그러나 2002년 개정지침(2002/58/EC)에서는 소프트 옵트 인 방식의 스팸 메일 지침을 발생하였다. 이 지침은 미국의 옵트 아웃보다 강력한 스팸 메일 규제 방식이다. 이 방식은 전자우편을 통해 직접적인 마케팅을 할 경우 규제 방식을 옵트 아웃(선택적 거부) 방식에서 소프트 옵트 인 방식으로 변경하는 것을 의미한다. 그리하여 다이렉트 마케팅의 목적으로 자동발신 시스템, 팩스에서 전자우편까지 가입자의 사전동의를 받도록 규제를 확대하여 실시하였다.

즉 유럽연합은 메일 뿐 아니라 휴대폰 단문 메시지에 대해서도 메일 발송자가 메일링리스트에 수신자 주소를 포함시키기 전 미리 허가를 받게 하는 옵트 인(선택적 수용) 방식의 규정을 법제화하였다.

(4) 스페인

스페인은 수신자가 이전에 원치 않았거나 명백히 허가하지 않은 전자 우편 또는 유사한 전자적 수단에 의해 선전 또는 광고성 통신의 배포는 금지하였다. 또한 전자 우편 또는 유사한 전자적 통신수단에 의해 보내진 상업적 통신은 광고라는 문구를 반드시 삽입해야 한다.

(5) 포르투갈

포르투갈에서는 자동송신장치나 팩스를 이용하여 보내는 판매 행위 관련 메일은 수신자의 사전 동의를 필요로 한다. 또한 가입자는 자동송진장치나 팩스 이외의 다른 수단을 통해서 발생하는 원치 않는 판매 요구(전화)를 거부할 권리를 가지고 있다고 규정하고 있다.

3.1.6. 종합 대안

앞에서 논의한 “정보통신망이용촉진및정보보호등에관한법률”의 제50조의 사항은 기본적으로 스팸 메일 자체를 인정하고 있어 규제에 어려움이 존재한다. 현행법은 스팸 메일의 옵트 아웃(선택적 거부) 방식(자유롭게 광고성 메일을 전송할 수 있고 이용자의 수신거부 요청이 있을 경우에만 보내지 않는 방식)을 인정하고 있다. 즉 메일을 받을 것인지 받지 않을 것인지에 대한 선택권이 정보주체에게 주어져 있는 것이 아니라 메일을 보낼 것인지 보내지 않을 것인지에 대한 선택권이 메일발송자에게 있을 뿐이라는 이야기이다.

그러므로 현재 법령상에 존재하는 옵트 아웃(선택적 거부) 제도를 옵트 인(선택적 수용) 제도로 바꾸어 명백히 동의 의사를 밝히지 않는 이메일을 ‘거부’로 간주하여 스팸 메일 발송을 원칙적으로 금지하도록 해야 한다. 즉 메일 수신에 대한 선택을 정보주체에게 준다는 의미에서 보다 프라이버시를 보호하는 방안이 된다.

또한 전자 상거래 업체 등 발송자가 무단 이메일 주소 추출 및 판매 유통에 대한 처벌 및 위반 시 과태료 부과 및 처벌 사항의 강화가 필요하다.

3.2. 통신비밀의 보호 개선방안

3.2.1. 통신비밀 보호의 필요성

정보기술이 발달한 현대사회에서 통신비밀을 보호하는 것은 모든 생활영역에서 개인의 프라이버시를 수호함과 동시에 인간의 존엄과 가치를 보장하는 커뮤니케이션의 자유, 표현의 자유를 보호하기 위한 것이다. 그러나 이 같은 통신비밀은 법령의 허술함이나 국가 공권력에 의한 잦은 제도적 침해를 통해 온전히 보호받지 못한 것이 사실이다.

최근의 다양한 사례를 통해 들여다 본 우리나라 통신비밀 보호 현황은 관련 법률의 낙후성과 국가 기관에 의한 제도적 침해 그리고 통신비밀에 대한 시민들의 낮은 인식이 가장 큰 문제점들로 드러나고 있다.

현행 헌법은 제18조를 통해 '모든 국민은 통신의 비밀을 침해받지 아니한다' 라고 규정함으로써 '통신수단을 이용함에 있어서 통신의 형태, 통신의 내용, 통신 당사자 및 배달의 방법 등이 본인의 의사에 반해서 공개되지 않아야 한다' 는 사실을 포괄적으로 지지하고 있다. 그러나 현재 국내 통신비밀 보호에 직접적으로 관련된 '통신비밀보호법' 은 제도적 허점과 국가기관에 의한 프라이버시 침해를 예방하지 못한다는 논란을 낳고 있어 이에 대한 범사회적 논의와 대책 마련이 시급한 실정이다.

3.2.2. 사회적 쟁점 및 현안 사례

3.2.2.1. 최근의 주요 현안 사례

(1) KT, 외교부 통화자료 요청 거부 (2004. 7)

외교통상부는 김선일씨 피랍사건과 관련해 AP통신으로부터 피랍여부를 확인하는 문의 전화를 받았다고 진술한 사무관 2명의 통화내역 자료 제출을 KT에 요청했으나, KT측은 통신비밀보호를 이유로 자료 제출을 거부해 논란.

(2) 정통부 해킹/스팸메일 수사권 확대에 대한 시민단체 '인권침해' 반발(2004. 5)

정통부가 정보통신망이용촉진 및 정보보호 등에 관한 법률상 개인정보 유출과 네트워크 해킹, 스팸메일, 불건전정보 유포 등을 정통부의 사법경찰권 단속대상에 포함시키는 방안을 추진하겠다고 밝히자, 경찰청과 시민단체측은 '인권침해' 소지가 있다며 즉각 반발.

3.2.2.2. 관련 통계

(1) 2003년 수사기관의 통화내역 조회수 : 16만 7천 41건(전년대비 36.3% 증가)
(2) 2002년 수사기관의 통화내역 조회수 : 12만 2천 5백 41건

3.2.3. 현행 법률 및 제도의 현황

- 헌법 제18조
: 모든 국민은 통신의 비밀을 침해받지 아니한다.

- 통신비밀보호법

제3조 (통신 및 대화비밀의 보호) 누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다. 다만, 다음 각호의 경우에는 당해 법률이 정하는 바에 의한다. [개정 2000 · 12 · 29]

1. 환부우편물등의 처리 : 우편법 제28조 · 제32조 · 제35조 · 제36조등 의 규정에 의하여 폭발물등 우편금제품이 들어 있다고 의심되는 소포우편물(이와 유사한 우편물을 포함한다)을 개피하는 경우, 수취인에게 배달할 수 없거나 수취인이 수령을 거부한 우편물을 발송인에게 환부하는 경우, 발송인의 주소 · 성명이 누락된 우편물로서 수취인이 수취를 거부하여 환부하는 때에 그 주소 · 성명을 알기 위하여 개피하는 경우또는 유가물이 든 환부불능우편물을 처리하는 경우

2. 수출입우편물에 대한 검사 : 관세법 제256조 · 제257조 등의 규정에 의한 신서외의 우편물에 대한 통관검사절차

3. 구속 또는 복역중인 사람에 대한 통신 : 형사소송법 제91조, 군사법원법 제131조, 행형법 제18조 · 제19조 및 군행형법 제15조 · 제16조등의 규정에 의한 구속 또는 복역중인 사람에 대한 통신의 관리

4. 파산자에 대한 통신 : 파산법 제180조의 규정에 의하여 파산자에게 보내온 통신을 파산관재인이 수령하는 경우

5. 혼신제거등을 위한 전파감시 : 전파법 제63조의2의 규정에 의한 혼신제거등 전파질서유지를 위한 전파감시의 경우

제4조 (불법검열에 의한 우편물의 내용과 불법감청에 의한 전기통신내용의 증거사용 금지) 제3조의 규정에 위반하여, 불법검열에 의하여 취득한 우편물이나 그 내용 및 불법감청에 의하여 지득 또는 채록된 전기통신의 내용은 재판 또는 징계절차에서 증거로 사용할 수 없다.

제13조 (통신사실 확인자료제공의 절차)

① 검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 ‘전기통신사업자’라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 ‘통신사실 확인자료제공’이라 한다)을 요청할 수 있다.

② 정보수사기관의 장은 국가안전보장에 대한 위해를 방지하기 위하여 정보수집이 필요한 경우 전기통신사업자에게 통신사실확인자료제공을 요청할 수 있다.

③ 검사 또는 사법경찰관이 제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 미리 서면 또는 이에 상당하는 방법으로 관할지방검찰청 검사장(검찰관 또는 군사법경찰관이 통신사실확인자료 제공을 요청하는 경우에는 관할 보통검찰부장을 말한다)의 승인을 얻어야 한다. 다만, 관할 지방검찰청 검사장의 승인을 얻을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체없이 그 승인을 얻어야 한다.

④ 제1항 및 제2항의 규정에 의한 통신사실 확인자료제공의 요청은 요청사유, 해당 가입자와의 연관성, 필요한 자료의 범위를 기재한 서면(이하 “통신사실 확인자료제공요청서”라 한다)으로 하여야 한다. 다만 사면으로 요청할 수 없는 긴급한 사유가 있는 때에는 통신사실확인자료제공요청 후 지체 없이 전기통신사업자에게 통신사실 확인자료제공요청서를 제출하여야 한다.

⑤ 검사, 사법경찰관 또는 정보수사기관의 장은 제3항 또는 제4항의 규정에 따라 통신사실 확인자료제공을 받은 때에는 당해 통신사실확인자료제고요청사실 등 필요한 사항을 기재한 대장과 통신사실확인자료제공요청서 등 관련자료를 소속기관에 비치하여야 한다.

⑥ 지방검찰청 검사장 또는 보통검찰부장은 제3항의 규정에 따라 통신사실 확인자료제공요청을 승인한 현황과 관련된 자료를 보존하여야 한다.

⑦ 전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장에게 통신사실 확인자료를 제공한 때에는 자료제공현황 등을 연 2회 정보통신부장관에게 보고하고, 당해 통신사실 확인자료 제공사실 등 필요한 사항을 기재한 대장과 통신사실 확인자료제공요청서 등 관련자료를 통신사실확인자료를 제공한 날부터 7년간 비치하여야 한다.

⑧ 정보통신부장관은 전기통신사업자가 제7항의 규정에 의하여 보고한 내용의 사실여부 및 비치해야 하는 대장 등 관련 자료의 관리실태를 점검할 수 있다.

* 기타조항 생략

3.2.4. 통신비밀보호와 관련한 문제점

현행 통신비밀보호법과 관련하여 사회적 논란이 되고 있는 부분들은 첫째, 국가기관을 통한 공익 명분의 통신정보수집 행위에 대해 제도적 보호대책이 미흡하다는 점이다. 특히 주요 수사기관을 중심으로 행해지는 불법 통신정보수집 행위는 인권 침해의 주요 사례로 거론되고 있다.

둘째, 민간에 의해 이루어지는 광범위한 불법 통신정보수집 행위에 대해 단속이 미비하며 기술적인 보호대책이 전무하다는 사실이다. 통신비밀보호법 위반 사례에 있어서 국가기관에 의한 위반 사례보다는 개인 또는 기업에 의한 사례가 더욱 높은 빈도를 나타내고 있다. 특히 전자통신 도/감청을 위한 각종 소프트웨어의 개발로 인해 고용주에 의한 피고용인의 통신비밀보호 침해 위험이 더욱 높아지고 있다.

셋째, 현행 통신비밀보호법을 둘러싸고 정부와 민간에 있어서 포괄적인 인식의 차가 존재한다는 점이다. 이 같은 인식의 차는 현행 통신비밀보호법이 앞서 언급했던 국가 주요 수사기관의 통신비밀 보호 침해를 제도적으로 막지 못한다는 점과 동시에 정당한 수사 행위에 대해 민간이 법적으로 규정된 협조를 거부하는 사례들을 낳고 있다.

3.2.5. 해외 사례의 검토

(1) 미국

미국에서는 프라이버시가 다소 모호하고 복잡한 개념으로 논의되는 경향이 있다. 한편에서는 개인정보 수집이 합법적으로 용인되는가 하면 다른 한편에서는 프라이버시의 침해로 인정되는 사례가 빈번하게 존재한다. 이 같은 다양성 때문에 모든 영역에 공통적으로 적용될 통일적인 프라이버시 보호정책은 채택하기 어렵고, 통신비밀 보호와 관련해서도 개인 또는 근로자보다 국가안보나 경영이익 보호에 우선하는 판례가 쉽게 발견된다. 따라서 미국에서는 통신비밀 보호와 관련하여 여러 개의 단행법에 의해서 복합적으로 적용되는 부분(sectoral) 접근방법이 도입되고 있으며 종합적·포괄적 입법은 고려되지 않고 있는 것으로 알려져 있다. 통신비밀보호와 관련한 미국의 관련 법령들은 다음과 같다.

- 통신비밀 보호와 관련된 연방법
·Electronic Communications Privacy Act of 1986
·Privacy Protection Act of 1980
·Privacy Act of 1974
·Fair Credit Reporting Act of 1970
·Right to Financial Privacy Act
·Telephone Consumer Protection Act of 1991
·Federal Records Act
·Communications Assistance for Law Enforcement Act

한편 미국 IITF의 정보정책위원회는 1997년 4월, 정보통신상의 프라이버시 보호를 위해

정부와 민간부문이 취해야 할 조치의 대안을 마련할 목적으로 '국내정보 인프라상 프라이버시보호 촉진을 위한 대안' (Options for Promoting Privacy on the National Information Infrastructure)이라는 보고서 발표하기도 했다. 보고서를 통해 IITF는 프라이버시를 연방정부기록 프라이버시, 통신 프라이버시, 의료기록 프라이버시, 시장 프라이버시 등 네 가지 영역으로 분류하고 각 영역별로 문제점 분석을 시도한 바 있다. 한편 미국에서의 개인정보보호 노력은 예방적, 예견적이라기보다는 일반적으로 사후적, 조건 반사적인 조치인 경우가 많다.

(2) EU

EU는 1997년 12월, '정보통신부문에 있어서 개인정보의 처리 및 프라이버시보호에 관한 지침' (Directive of the European Parliament and the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector)을 채택하며 통신비밀 보호와 관련한 규정을 마련했으나 이는 주로 ISDN(the Integrated Services Digital Network)나 디지털 이동 네트워크(public digital mobile networks)를 통한 정보통신 서비스(telecommunications services)에 주로 적용되는 한계가 있다.

(3) 일본

일본은 통신사업법, 유선통신법 등에 의해 통신비밀 보호를 규정하고 있다. 민간부문을 대상으로 한 통신비밀 보호에 관한 포괄적인 입법은 없으며 현재 정부지침·고시와 민간의 자율규제에 의존하는 실정이다. 그러나 일본 내 정보화의 진전, EU의 개인정보보호에 관한 입법 등 국내외 환경변화의 영향으로 1997년 3월에는 통산성이 상기 지침을 '민간부문에 있어서 전자계산기처리에 관계된 개인정보의 보호에 관한 가이드라인'으로 명칭을 변경하고 그 내용을 대폭 수정·보완한 바 있다. 아울러 1991년에는 우정성이 '통신사업에 있어서 개인자료의 보호에 관한 지침'을 제정하여 개인정보 보호를 위해 통신사업자들이 지켜야 할 가이드라인 제시했다. 또한 1996년에는 개인발신자의 전화번호 및 기타 정보를 제공해 주는 통신서비스와 관련하여 '개인발신자 데이터보호를 위한 발신자ID 서비스 이용에 관한 지침'을 제정·고시하기도 했다.

3.2.6. 종합대안

첫째, 현재 국가 수사기관에 의한 통신비밀 침해 사례를 제도적으로 방지하기 위해 통신비밀 보호에 관한 헌법 규정을 포괄적으로 준수하는 유관 하위법률의 재정비가 필요하다. 특히

통신정보 수집의 조건을 ‘수사 또는 형의 집행을 위해 필요한 경우’로 규정된 법적 조항을 ‘충분한 범죄혐의가 인정되는 경우’로 제한해 법리의 확대 해석을 막는 한편 엄격한 영장주의의 집행을 강화해야할 필요가 있다.

아울러 현행법이 규정하는 ‘통신의 비밀’에 대한 명확한 법리 개념 규정이 필요하다. 통상적으로 통신의 비밀에는 통신의 내용뿐만 아니라 통신 상대의 인적사항, 통신의 시간, 장소 등도 포함된다. 따라서 이 같은 자료의 공개를 청구할 경우에도 원칙적으로 영장주의가 적용되어야 할 필요가 있다. 그러나 현행법은 이러한 것들을 모두 법원의 판단없이 검사장의 승인을 통해 열람하거나 제출을 요청할 수 있게 하고 있어서 ‘통신 비밀’의 확대해석을 통한 인권침해의 여지를 낳고 있다. 현행법은 통신사실확인자료 요청의 요건을 ‘수사 또는 형의 집행을 위하여 필요한 경우’에는 열람이나 제출을 요청할 수 있도록 규정하고 있으나 이 역시 충분한 범죄혐의가 인정되고, 통신 비밀 열람 외에 다른 방법을 통해서는 수사가 불가능하다는 충분한 ‘보충성’이 인정되는 경우에만 통신사실확인자료의 이용이 가능하도록 하여야 할 것이다.

둘째, 민간에 의해 광범위하게 이루어지는 불법 통신비밀 보호 침해 사례를 막기 위해 경찰청 사이버수사대를 비롯한 현행 수사기관을 통해 민간에 의한 통신인권 침해 감시 활동을 강화할 필요가 있다. 또는 민간에 의한 통신비밀 침해 사례를 개인정보보호위원회 등 상대적으로 독립적인 기관들이 보다 적극적으로 감시하고 예방에 나서야한다는 의견도 귀 기울일 필요가 있다. 한편에서는 정보통신부를 비롯한 통신 관련 주무 부처들의 수사권 신설을 논의하고 있으나 이는 비 수사기관의 수사권 확보가 또 다른 정보인권 침해로 이어질 수 있다는 점에서 주의가 매우 주의가 요구되는 부분이다. 물론 보다 근본적으로는 정보보호진흥원 등 국내 정보보호 유관 기관들을 통해 정보보호 및 통신 프라이버시에 대한 대국민 인식을 증진시킬 수 있는 프로그램들을 마련할 필요가 있다.

셋째, 통신비밀보호법에 대한 정부와 민간간 인식의 차로 인해 정당한 수사가 이루어지지 않는 사례를 막기 위해 유관 법률의 모호한 조항들을 보다 구체적으로 규정해야 한다. 대표적으로 통신비밀보호법의 보호대상이 전송중의 전기통신에 한하는지, 아니면 송수신 과정의 전기통신에 한하는지 아니면 이미 송수신이 완료된 것까지 포함하는지에 관해 정부와 민간간 법리해석에 다소 이견이 드러나고 있다. 이는 전화 수신기에 녹음된 메시지, 서버에 저장된 전자우편, 수신자의 컴퓨터에 저장된 전자우편 등을 당사자의 동의없이 채록하는 경우 통신비밀보호법 위반으로 볼 수 있는가 하는 점이다.

3.3. CCTV 사용 규제

3.3.1. CCTV 등의 사용 규제 필요성

최근 각 지자체 및 경찰청이 설치하고 있는 CCTV에 대한 논의가 활발하게 벌어지고 있다. 즉 CCTV 설치 및 이용에 대해 효율적인 범죄 예방 및 범죄 수사 등의 목적을 위해 반드시 필요하다는 주장과 이러한 것들이 모든 사람들을 잠재적 범죄자로 취급한다는 점을 들어 인권침해의 가능성이 높다는 주장이 팽팽하게 대립대고 있다는 것이다. 이렇듯 각 양측의 주장이 제기되고 있으나 현실에서의 각 지자체 및 경찰청, 교육기관 등에서는 지속적인 CCTV 도입이 확산되고 있다.

이러한 확산은 위에서 언급한 효율적인 범죄 예방 및 범죄 수사 등을 할 수 있다는 이점도 지니고 있으나, 국회가 제정한 법률이 아닌 지방자치단체나 경찰서장의 재량에 의해 이루어지고 있다는 점과 무인단속장비의 성능 향상으로 인해 CCTV 설치지역, 운영방법에 따라 국민의 기본권인 프라이버시를 침해한다는 문제점 역시 안고 있다. 이에 대해 국가인권위원회는 행정자치부 장관과 국회의장에게 CCTV 등의 설치 및 운영에 대한 법적 기준을 마련하도록 권고하였다.

판례에서는 공익 목적 및 비례의 원칙 등 총체적 합법성이 갖추어진 경우, CCTV 등 촬영도구를 이용한 공공장소에서의 공적 촬영행위를 적법하다고 판시하고 있어 촬영 자체의 위법성보다는 촬영된 사진이나 영상의 공표에 대한 통제와 감시가 필요하다는 입장이다.

그러나 앞에서도 언급했듯이, 문제는 CCTV 설치로 인해 모든 사람들을 잠재적 범죄자로 취급한다는 것으로 이것은 가장 기본적인 프라이버시를 침해하고 있다는 점이다. 이러한 점에서 선행되어야 할 점은 아무런 지침 및 법령 없이 이루어지고 있는 지방자치단체 및 경찰청의 CCTV 설치 및 운용에 대한 규제 마련일 것이다.

본 보고서에서는 공공영역에서의 CCTV 및 디지털 카메라 설치 및 운용에 관한 것으로 한정하기로 한다.

3.3.2. 사회적 쟁점

앞에서 언급했듯이 CCTV 등 매체 활용은 긍정적 측면과 부정적 측면 모두를 담고 있다. 즉 CCTV 등 매체의 활용은 효율적인 범죄 예방 및 범죄 수사 등의 공공의 이익, 재산보호, 증거 확보를 위한 목적으로 사용될 수 있으나 모든 국민을 잠재적 범죄자로 취급한다는 점 등은 CCTV 등 매체 활용의 문제점으로 제기될 수 있다. 그 중에서도 가장 문제가 되고 있는 것은 주택가 및 도로에 설치되는 방범용 CCTV라 할 수 있다. 왜냐하면 이러한 CCTV는 비교적 넓은 공간에서 사람을 대상으로 촬영하기 때문에 그만큼 프라이버시 침해 가능성이 다른 목적의 CCTV 촬영보다 높기 때문이다.

CCTV 등의 매체의 설치 및 이용에 대해 사회적으로 쟁점이 된 사례는 CCTV 등의 매체를 사용하는 주체에 따라 다음과 같이 살펴볼 수 있다.

(1) 지방자치단체

현재 여러 지방자치단체는 범죄 예방을 목적으로 CCTV 도입 및 설치를 활발하게 진행하고 있다. 특히 이러한 CCTV는 목적에 따라 크게 3가지로 나누어 살펴볼 수 있는데, 그것은 교통법규위반 단속용 무인 카메라, 쓰레기 무단 투기 단속용 CCTV, 방범용 CCTV이다.

. 강남구의 경우, 골목 300미터 마다 CCTV를 설치하였다.(종로구, 관악구에도 CCTV 설치)
. <호남권> 전주 주택가 CCTV설치 논란(경향신문. 2004. 7. 22)
. “인권침해” 말 많은 주택가 CCTV 증설 논란(국민일보. 2004. 5. 11)
. 富村 성북동 주민 CCTV 고민(국민일보. 2004. 6. 1)
. 강남구 CCTV 방범센터 설치-종합상황실 마련(동아일보. 2004. 2. 19)
. 강남구 CCTV 설치이후/“혹시 찍힐라” CCTV 범죄예방 “몸값”(한국일보. 2004. 2. 16)
. 등·학교길 형사 배치 폭력감시 - 주요 통학로에 CCTV 설치(문화일보. 2004. 3. 2)
. 강남구청 CCTV 설치 이후 첫 절도범 검거
. 강남구 CCTV 272대 설치(2004. 8. 24)

(2) 경찰청

현재 경찰청에서는 교통흐름조사용 CCTV와 교통법규위반 단속용 무인카메라를 사용하고 있다. 7개 도시 경찰청에서 설치·운용하고 있는 교통흐름조사용 CCTV는 총 446대이다. 그 중 서울156대, 부산 98대, 그 외 지역은 각각 50대 미만의 CCTV가 설치되어 있는 것으로 조사되었다. 이러한 CCTV는 시대 주요 구간의 교통상태를 파악하기 위한 것으로 실시간 모니터링을 하면서 대략 200미터에서 250미터 정도의 범위를 촬영할 수 있다.

또한 교통법규위반 단속용 무인카메라는 총 727대로, 서울 238대, 부산 142대, 나머지 지역은 90개 미만으로 이 무인카메라의 목적은 속도위반, 신호위반 등의 교통법규 위반 차량을 단속하기 위한 것이다. 이 무인카메라에 찍힌 사진은 범칙금 부과를 위한 것이기 때문에 일정기간 보관하고 있고, 경찰청의 “교통단속처리지침”에서는 10년간 보관하도록 되어 있다(전국정보운동포럼. 2004).

. CCTV가 교통사고 심판관'(서울신문. 2004. 2. 19)

. “주차단속 장갑차” 첫선, CCTV 탑재. 7월 인천에(경향신문. 2004. 2. 7)

3.3.3. 현행 법률 및 제도의 현황

3.3.3.1. 현행 법률

공공영역에서의 CCTV 및 디지털 카메라 등의 영상 커뮤니케이션 규제에 대한 현행 법률은 존재하지 않는다.

3.3.3.2 유관법률

직접적으로 CCTV 등의 영상 커뮤니케이션 매체를 다룰 수 있는 현행 법률은 존재하지 않으나, 이를 간접적으로 포괄할 수 있는 유관 법률은 존재한다. 그 내용은 다음과 같다.

- 헌법

제10조 모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.

제17조 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.

- 시민적 및 정치적 권리에 관한 국제 규약

제17조 1. 어느 누구도 그의 사생활, 가정, 주거 또는 통신에 대하여 자의적이거나 불법적인 간섭을 받거나 또는 그의 명예와 신용에 대한 불법적인 비난을 받지 아니한다.

2. 모든 사람은 그러한 간섭 또는 비난에 대하여 법의 보호를 받을 권리를 가진다.

- 공공기관의개인정보보호에관한법률

- 공공기관의기록물관리에관한법률시행규칙

제37조(비밀기록물 전용서고) 전문관리기관의 장은 영 제29조 제5항의 규정에 의하여 비밀기록물 전용서고를 설치한 때에는 이를 통제구역으로 지정하고, 청원경찰·방호원 또는 감시카메라 등에 의하여 모든 출입사항이 상시 감시·기록되도록 하여야 한다.

- 성폭력범죄의 처벌 및 피해자보호 등에 관한 법률

제14조 (통신매체이용음란) 자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화 · 우편 · 컴퓨터 기타 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건을 상대방에게 도달하게 한 자는 1년 이하의 징역 또는 300

만원 이하의 벌금에 처한다.

제14조의2 (카메라등이용촬영) 카메라 기타 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 타인의 신체를 그 의사에 반하여 촬영한 자는 5년 이하의 징역 또는 1천만원이하의 벌금에 처한다.

- 정보통신망이용촉진및정보보호등에관한법률

61조 사람을 비방할 목적으로 정보통신망을 통하여 공연히 사실 또는 허위의 사실을 적시하여 타인의 명예를 훼손한 자는 처벌을 받는다.

3.3.4. 시민단체 등의 문제제기

2002년 12월 서울시 강남구청과 강남경찰서가 강남구 논현1동 일대에 범죄예방을 위한 CCTV 5대를 시범 설치·운영하였다. 이후 2004년 8월 강남구청은 총 272대의 CCTV를 설치하고 첫 절도범을 CCTV를 이용하여 검거하였다. 이러한 CCTV 설치·운영을 통해 절도범 등과 같은 범죄인의 단속에 긍정적인 효과를 보여주는 사례도 있으나, 이는 불특정 다수의 촬영을 진행하고 있다는 점에서 개인정보인권침해 여부에 대해서도 여러 단체가 주목하고 있다. 이러한 방법용 CCTV 설치 및 운용의 문제점은 현재 CCTV 설치에 관한 법률 없이 지방자치단체 및 경찰청의 재량에 따라 진행되고 있는 실정이다.

뿐만 아니라 이러한 영상 커뮤니케이션 매체는 기존의 아날로그 방식에서 디지털 방식으로 급격하게 변화하고 있다. CCTV 확산, 확장된 네트워크, 특정인물의 검색, 추적 기술 등이 결합하게 되면 프라이버시 침해 가능성이 보다 크게 발생하게 된다. 그리고 이미 광범위하게 퍼져 있는 사적 커뮤니케이션 매체까지 네트워킹이 가능해진다면, 더 큰 프라이버시 침해가 일어날 소지가 존재한다.

3.3.5. 해외 사례의 검토

CCTV 등의 영상 커뮤니케이션에 대한 해외 사례는 국가마다 약간의 차이를 보이고 있으나, 대부분 국가에서는 OECD 8원칙에 맞추어 CCTV 설치 및 운용에 대한 기준을 정립하고 있다.

(1) 영국

최근 영국에서는 공중전화, 대중교통 등과 같은 공공장소 뿐 아니라 개인의 자산 보호, 가정폭력, 아동 학대 방지 등의 목적을 위해 집안 내의 카메라 설치도 확산되고 있는 추세이다.

영국은 1998년 정보보호법 내에서 CCTV의 설치 및 운용에 관하여 여러 요건만 갖춘다면 적법적이고 적합한 것으로 규정하고 있다. 그 요건은 경찰이나 지역 정부 등의 적절한 주체에 의한 설치되었느냐에 대한 것, CCTV 설치 및 운용에 대해 정보보호감독관에게 통지하였는가에 대한 것, CCTV가 되었다는 사실을 표시하였는가에 대한 것이다.

그 이후 200년 CCTV와 관련된 데이터 보호법 시행령을 실시하고 있다. 이는 정보보호법에서보다 보다 상세하고 구체적인 기준 및 요건을 제시하고 있음을 말해준다. 첫째 CCTV 설치 시에 이를 알리는 표지판을 달고, 이 표지판에 대한 크기까지 구체적으로 제시하고 있다. 둘째 CCTV를 설치하려는 목적을 분명히 하고, 최초 설치 시의 목적을 벗어나 CCTV를 사용하지 못하도록 규정하고 있다. 셋째 CCTV가 촬영할 수 있는 범위를 제한하고 있다. 넷째 CCTV로 촬영된 정보에 대해 법이 명시적으로 밝혀진 경우를 제외하고 제3자의 공유를 금지하고 있다. 다섯째 촬영된 영상물을 필요 이상으로 보유하는 것을 제한하고 있다. 예를 들어 도심, 공공도로는 31일, 은행은 3개월 동안만 보관하며, 보유기간이 지나 삭제할 경우에도 그에 대한 기록을 남기도록 규정하고 있다. 여섯째 이 영상물에 대한 접근에 있어서도 관리 책임자, 지정된 인원에 대해서만 가능하도록 하였다. 마지막으로 CCTV 설치의 목적, 관리 주체, 책임자 연락처 등을 공지하고, 개인이 CCTV 관련 내용에 대해 이의를 제기할 수 있도록 개인의 권리를 보장하고, 이에 대해 관리 책임자는 반드시 이러한 이의 사항에 대해 검토하도록 제시하고 있다.

그러나 이러한 내용은 공공기관 및 경찰청에서 설치한 CCTV만 해당되는 것으로 직장 내 CCTV 사용과 자택 자산 보호를 목적으로 집에 설치한 보안 장치, 저널 및 문학적 목적을 위한 카메라 사용, 특정 목적을 위해 사용된 매체 등은 이러한 법률에 적용되지 않는다.

(2) 미국

미국의 사례는 미국 콜롬비아 주 MPD(Metropolitan Police Department)의 CCTV 운용에 관한 법이다. 이 법에 따르면 CCTV 및 카메라의 설치로 범죄를 예방하는데 상당한 효과가 있을 때에 한해 주거지역 및 상업지역의 CCTV 설치가 가능하다고 제시하고 있다. 비상 상황 및 법원 명령을 제외하고는 반드시 카메라 혹은 CCTV 설치 사실 및 제반 사항에 대해 경찰청장은 사전에, 비상 상황의 경우에 있어서도 그 상황이 종료되는 즉시 사후에 공지하도록 제시하고 있다.

이 법에서는 다소 모호한 성격을 띠고 있기는 하지만 CCTV 목적을 범죄 예방과 공공의 안전으로 들고 있다. CCTV를 통해 생성된 정보는 타 공공기관과 공유할 수 있으나 반드시 법률에 따라 제한적으로만 가능하다. 이렇게 녹화된 영상물은 10일 이상 보유하지 못하고 그 이후 기간에 있어서는 서면으로 허가를 받아야만 한다는 규정을 두고 있다. CCTV 시스템 장비는 제한된 직원만이 관리 할 수 있으며, 이 CCTV에 대한 보호 의무를 반드시 명시하여야 한다. CCTV 제반 사항인 일반적 성능, 대략적 위치, 운영하는 용도 등에 대해 대중에게 반드시 공지

해야 하고, 반년마다 CCTV 시스템과 사용에 대한 정보를 보고서에 포함하여야 한다. 또한 30일 내에 공지된 CCTV 설치, 특정 카메라 설치와 관련하여 경찰청장에게 의견을 제시할 수 있고, 경찰청장은 이를 반영해야할 의미 또한 가지고 있다.

CCTV 시스템의 사용에 있어 미허가 및 오용에 관여한 자에 대해 형사 소추가 가능하며, 행정적 제재도 가할 수 있다. 또한 최소 분기마다 1회씩 자체 감사를 실시하고 이를 의회에 보고해야 하는 제도적 기반을 가지고 있다.

(3) 기타 유럽연합 회원국

일부 유럽연합 회원국들은 CCTV 및 비디오 감시 관련 사례를 헌법, 법률, 여러 국가기관에서의 명령 및 판결을 바탕으로 규정짓고 있다. 일부 국가의 경우는 개인정보 처리 여부와 관련 없이 CCTV의 설치·운용은 국가 정보보호 기구로부터 사전 승인을 받도록 규정하고 있다. 비디오 감시 관련법이 존재하지 않는 국가는 정보보호 기구가 주관하여 지침, 의견서, 행동강령 등의 정보보호 규정을 바탕으로 CCTV 및 비디오 관련 사례를 평가하고 있다.

1) 덴마크

덴마크는 비디오 감시와 관련하여 민간과 공공부분에 있어 각각 금지하는 의견서를 발행하였다. 우선 민간 부분에 있어서 덴마크는 2000년 2월 Consolidation Act(비디오 감시 금지법)에서 민간단체들의 공공장소(거리, 도로, 광장 혹은 이와 유사한 지역)에서의 비디오 감시 행위를 금지하였다. 2002년 6월에는 정보보호 감독기구가 대형 슈퍼마켓의 비디오 감시 및 인터넷 출판을 통한 전송과 관련하여 의견서를 발간하였고, 2003년 7월에는 ‘민간이 운영하는 대중 교통수단에 설치된 비디오 감시 시스템은 균형성의 원칙과 덴마크 정보보호법에 포함된 규정을 준수할 것’이라는 내용의 의견서를 발견하였다. 이후 2003년 11월에는 공공 부분에 있어 공공기관이 비디오를 통해 감시하는 것에 대한 특정 제한 규정을 마련하였다.

2) 스웨덴

스웨덴의 비디오 감시에 관련된 조항은 일반 비디오 감시 관련법과 비밀 감시(범죄 조사)법을 통해 규제된다. 일반적인 비디오 감시는 보통 국가 행정 위원회의 승인이 요구되며, 비밀스러운 비디오 감시는 법원의 승인을 받아야 한다. 또한 디지털 기술을 통한 비디오 녹화는 개인정보 처리로 간주되어 일반 비디오 감시법에서 특별히 규정하지 않는 범위까지 정보조사 위원회의 감시 대상이 된다.

3) 네덜란드

네덜란드는 특정 환경에서 공익을 목적으로 비디오 감시 시스템을 공공장소에서 사용할 수 있는 명확한 권한을 시 위원 및 시장이 제공할 수 있도록 하는 지방법 변경을 제안하였다.

4) 핀란드

핀란드의 경우, 비디오 감시에 대한 특별한 규정은 없지만 다수의 다른 법률에서 비디오 감시 및 기타 기술 감시, 관측, 모니터링 관련 규정이 마련되어 있다.

3.3.6. 종합 대안

현재 우리나라는 CCTV 및 디지털 카메라 등 영상 커뮤니케이션 매체에 대한 법 혹은 제도가 미흡한 실정이다. 그리하여 각 지자체, 경찰청, 교육기관 등에서는 아무런 법적인 조치 없이 필요성에 의해 CCTV를 설치 운용하고 있는 실정이다. 뿐만 아니라 영상 커뮤니케이션 매체는 기존의 아날로그 방식에서 디지털 방식으로 급격하게 변화하고 있다. 즉 공공기관에서 사용하고 있는 비디오테이프 형식의 녹화장치에서 디지털 카메라 형식의 녹화 장치로의 이행은 한편으로는 관리 측면의 혁명을 가져올 수 있으나, 또 한편으로는 확장된 네트워크, 특정인물의 검색, 추적 기술 등과의 결합으로 인해 심각한 프라이버시 침해 가능성도 발생할 여지가 있다는 것이다.

그러므로 현재는 CCTV 관련 법·제도 마련이 시급한 시점이다. 그러나 CCTV는 공적인 공간에서 사용되는 대표적인 하나의 매체로써 CCTV 설치 및 운용에 관한 단독의 법제화가 필요하기 보다는 기존에 존재하는 유관 법률(공공기관의 개인정보보호에 관한 법률) 속에서 법적인 검토와 체계화가 필요하다. 이후 CCTV를 설치하는 주체인 지방자치단체 및 경찰청 등에 그 설치 권한을 제한적으로 부여하고 그 운영기준 및 통제 방법을 명시함으로써 조례에 위임하는 것도 한 가지 대안으로 제시될 수 있을 것이다.

그렇기 위해서는 CCTV를 설치하려고 하는 기관이 어떠한 목적으로 CCTV를 도입하고자 하는 것인지에 대한 사전 결정에 국민들의 참여가 활발하게 이루어져야 하며, 이러한 CCTV 설치 및 운용이 국민의 프라이버시에 어떠한 영향을 끼치는지 영향평가가 선행되어야 할 것이다. 또한 설치 후 운용에 있어 생성된 영상물에 대한 보존 및 공개, 공유에 대한 규정을 확실하게 제시해 주어야 할 것이다. 뿐만 아니라 CCTV를 운용하는 주체에 대한 명확한 고지와 접근에 대한 권한 설정을 명확하게 해주어야 할 것이다. 즉 CCTV 도입·설치에 관한 명확한 기준 도입 및 CCTV 운용의 목적, 데이터 수집 등에 대한 명확한 근거 및 가이드라인의 제시가 필요하다.

3.4. 도감청 및 통신제한조치의 규제

3.4.1. 도감청 및 통신제한조치에 관한 연구의 필요성

현행 통신비밀보호법은 '감청'에 대해 '전기통신에 대하여 당사자의 동의없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것'이라 규정하고 있다. 국가 주요 수사기관에 의한 이 같은 불법 도/감청은 국가기관에 의한 반민주적 행위의 전통적인 사례인 동시에 통신비밀의 보호 및 포괄적인 프라이버시 침해의 가장 대표적인 사례로 간주되고 있다.

국회 및 시민단체들의 지속적인 문제제기로 관련 법률 개정을 둘러싼 논의가 진행 중에 있음에도 불구하고 현재까지 국가기관에 의한 도/감청 사례는 줄어들지 않고 있으며 위법성 여부를 놓고 민관 사이의 공방이 계속되고 있는 실정이다.

한편 도감청과 관련한 최근의 문제는 국가기관 외에 민간에 의한 불법 도/감청 사례가 꾸준히 증가하고 있다는 사실이다. 도/감청과 관련한 각종 기술의 발달에 힘입어 민간에 의한 불법 도/감청이 광범위하게 행해지고 있으며 이를 단속할 관련 법률의 정비가 시급한 상황이다. 아울러 국가기관에 의한 통신제한조치가 개인의 통신비밀 보호를 침해한다는 비판이 꾸준히 제기되면서 보다 엄격한 법 적용과 조항의 개정이 요구되고 있다.

3.4.2. 사회적 쟁점 및 현안 사례

3.4.2.1. 최근의 주요 현안 사례

(1) 국가정보원/국군기무사, 언론기자 통화내역 불법조회 논란(2004. 1-2)

국가정보원 및 국군기무사가 국가기밀사항에 관한 조사를 이유로 K일보 및 H일보를 비롯한 수 명의 기자들의 통화내역을 조회한 사실이 드러나 인권침해 논란 및 통신정보 공개를 둘러싼 언론사외 정부, 국회와 이동통신업체간의 갈등 파문.

(2) 경찰서 통신망 도청한 견인차 기사 구속(2004. 3)

공주경찰서는 사고차량을 먼저 견인하기 위해 청계천 전자상가에서 휴대용 무전기를 구입, 이를 이용해 경찰서와 소방서 등의 통신망을 불법 도청한 견인차 기사 전모씨에 대해 통신비밀보호법 위반 혐의로 구속영장을 신청.

(3) 선거관리위원회 직원 열린우리당 모임 불법 도청 입건(2004. 3)

강원도 양구경찰서는 지역 사회단체 행사장에 녹음기를 설치해 대화내용을 몰래 녹음한 혐의로 양구군 선거관리위원회 직원 2명을 입건.

(4) 연예인 이메일 해킹, 내용 열람자 구속 (2004. 6)

서울중앙지검 컴퓨터수사부는 이메일을 이용한 해킹 프로그램으로 JYP엔터테인먼트 대표 박진영 등 연예인 수명의 포털사이트 계정 비밀번호를 알아내 이메일을 훔쳐본 혐의로 송 모씨 등 2명을 불구속 기소.

(5) 전북지방언론 기자 열리우리당사 불법 도청 녹음 입건(2004. 1) 서울 영등포경찰서는 열린우리당 김원기 의원 사무실 탁자에 특종을 목적으로 몰래 녹음기를 설치, 불법도청을 시도한 혐의로 전북지역 모 일간지 기자 김 모씨를 불구속기소.

(6) 경기 모 고등학교장 교사 85명 인터넷 사용 내역 감청 유죄 구형 (2004. 5)

인천지법 부천지원은 중학교 교사 35명과 고교교사 50명이 사용한 개인용 컴퓨터에 설치된 '넷 오피스쿨' 이라는 원격 강의 프로그램을 통해 인터넷 통신내역을 감청, 교사징계 등에 활용한 경기 T고교 교장 이모씨와 동일 재단 T중학교 교장 탄 모씨, T고 행정실장 이모씨에 대해 각각 징역 1년과 자격정지 1년, 징역 8월과 자격정지 1년을 선고하고 2년간 집행유예 선고.

3.4.2.2. 국가기관 도/감청 관련 통계

(1) 2003년 직접 도/감청수 : 1천 6백 96건(전년대비 11% 증가)
(2) 2002년 직접 도/감청수 : 1천 5백 28건

3.4.3. 현행 법률 및 제도의 현황

- 통신비밀보호법
제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
⑦ "감청"이라 함은 전기통신에 대하여 당사자의 동의없이 전자장치 · 기계장치등을 사용하여 통신의 음향 · 문언 · 부호 · 영상을 청취 · 공독하여 그 내용을 지득 또는 채록하거나 전기통

신의 송·수신을 방해하는 것을 말한다.

제7조 (국가안보를 위한 통신제한조치)

① 대통령령이 정하는 정보수사기관의 장(이하 "정보수사기관의 장"이라 한다)은 국가안전보장에 대한 상당한 위험이 예상되는 경우에 한하여 그 위해를 방지하기 위하여 이에 관한 정보수집이 특히 필요한 때에는 다음 각호의 구분에 따라 통신제한조치를 할 수 있다. <개정 2001.12.29>

1. 통신의 일방 또는 쌍방당사자가 내국인 때에는 고등법원 수석부장판사의 허가를 받아야 한다. 다만, 군용전기통신법 제2조의 규정에 의한 군용전기통신(작전수행을 위한 전기통신에 한한다)에 대하여는 그러하지 아니하다.

2. 대한민국에 적대하는 국가, 반국가활동의 혐의가 있는 외국의 기관·단체와 외국인, 대한민국의 통치권이 사실상 미치지 아니하는 한반도 내의 집단이나 외국에 소재하는 그 휘하단체의 구성원의 통신인 때 및 제1항제1호 단서의 경우에는 서면으로 대통령의 승인을 얻어야 한다.

② 제1항의 규정에 의한 통신제한조치의 기간은 4월을 초과하지 못하고, 그 기간중 통신 제한조치의 목적이 달성되었을 경우에는 즉시 종료하여야 하되, 제1항의 요건이 존속하는 경우에는 소명자료를 첨부하여 고등법원 수석부장판사의 허가 또는 대통령의 승인을 얻어 4월의 범위 이내에서 통신제한조치의 기간을 연장할 수 있다. 다만, 제1항 제1호 단서의 규정에 의한 통신제한조치는 전시·사변 또는 이에 준하는 국가비상사태에 있어서 적과 교전상태에 있는 때에는 작전이 종료될 때까지 대통령의 승인을 얻지 아니하고 기간을 연장할 수 있다. <개정 2001.12.29>

③항 및 ④항 생략

제8조 (긴급통신제한조치)

① 검사, 사법경찰관 또는 정보수사기관의 장은 국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄등 중대한 범죄의 계획이나 실행 등 긴박한 상황에 있고 제5조제1항 또는 제7조제1항제1호의 규정에 의한 요건을 구비한 자에 대하여 제6조 또는 제7조제1항 및 제3항의 규정에 의한 절차거칠 수 없는 긴급한 사유가 있는 때에는 법원의 허가 없이 통신제한 조치를 할 수 있다.

② 검사, 사법경찰관 또는 정보수사기관의 장은 제1항의 규정에 의한 통신제한조치(이하 "긴급통신제한조치"라 한다)의 집행착수후 지체없이 제6조 및 제7조제3항의 규정에 의하여 법원에 허가청구를 하여야 하며, 그 긴급통신제한조치를 한 때부터 36시간 이내에 법원의 허가를 받지 못한 때에는 즉시 이를 중지하여야 한다.

③ 사법경찰관이 긴급통신제한조치를 할 경우에는 미리 검사의 지휘를 받아야 한다. 다만, 특히 급속을 요하여 미리 지휘를 받을 수 없는 사유가 있는 경우에는 긴급통신제한조치의 집행착수후 지체없이 검사의 승인을 얻어야 한다.

④ 검사, 사법경찰관 또는 정보수사기관의 장이 긴급통신제한조치를 하고자 하는 경우에는

반드시 긴급검열서 또는 긴급감청서(이하 "긴급감청서등"이라 한다)에 의하여야 하며 소속기관에 긴급통신제한조치대장을 비치하여야 한다.

⑤ 긴급통신제한조치가 단시간내에 종료되어 법원의 허가를 받을 필요가 없는 경우에는 그 종료후 7일 이내에 관할 지방검찰청검사장(제1항의 규정에 의하여 정보수사기관의 장이 제7조제1항제1호의 규정에 의한 요건을 구비한 자에 대하여 긴급통신제한조치를 한 경우에는 관할 고등검찰청검사장)은 이에 대응하는 법원장에게 긴급통신제한조치를 한 검사, 사법경찰관 또는 정보수사기관의 장이 작성한 긴급통신제한조치통보서를 송부하여야 한다. 다만, 검찰관 또는 군사법경찰관이 제5조제1항의 규정에 의한 요건을 구비한 자에 대하여 긴급통신제한조치를 한 경우에는 관할 보통검찰부장이 이에 대응하는 보통군사법원 군판사에게 긴급통신제한조치통보서를 송부하여야 한다.

⑥ 제5항의 규정에 의한 통보서에는 긴급통신제한조치의 목적 · 대상 · 범위 · 기간 · 집행장소 · 방법 및 통신제한조치허가청구를 하지 못한 사유 등을 기재하여야 한다.

⑦ 제5항의 규정에 의하여 긴급통신제한조치통보서를 송부받은 법원 또는 보통군사법원군판사는 긴급통신제한조치통보대장을 비치하여야 한다.

⑧ 정보수사기관의 장은 국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄등 중대한 범죄의 계획이나 실행 등 긴박한 상황에 있고 제7조제1항제2호에 해당하는 자에 대하여 대통령의 승인을 얻을 시간적 여유가 없거나 통신제한조치를 긴급히 실시하지 아니하면 국가안전보장에 대한 위해를 초래할 수 있다고 판단되는 때에는 소속 장관(국가정보원장을 포함한다)의 승인을 얻어 통신제한조치를 할 수 있다.

⑨ 제8항의 규정에 의하여 긴급통신제한조치를 한 때에는 지체없이 제7조의 규정에 의하여 대통령의 승인을 얻어야 하며, 36시간 이내에 대통령의 승인을 얻지 못한 때에는 즉시 그 긴급통신제한조치를 중지하여야 한다.

2002년에는 도/감청 관련 통신비밀 보호법이 개정되었는데 그에 대한 사항은 다음과 같은 표로 살펴볼 수 있다.

구 분	현 행	개 정 안
감청대상 범죄축소	약 130개	약 100개
감청 통지제도	별도규정 없음	수사(감청) 후 30일 내 통지
감청기간	수사목적: 3월, 안보목적: 6월	수사목적: 2월, 안보목적: 4월
통신사실확인자료 제공의 법적근거	별도규정 없음	검사장 승인으로 요청토록 강화
감청설비 신고	별도규정 없음	일반수사기관의 경우 재원과 성능을 정통부장관에게 신고

〈표 6〉 도/감청 관련 통신비밀보호법 주요 개정 내역

3.4.4. 도/감청 및 통신제한조치 관한 문제점

첫째, 국가기관에 의한 도/감청의 인권침해 사례가 여전히 빈번하게 일어나고 있다. 이와 관련하여 시민단체들은 '통신의 비밀은 정보화 시대에서 중요한 정보인권의 하나'로 보고 '통신의 비밀을 제한할 경우에는 과잉금지의 원칙이 적용되어야 한다'고 주장하고 있다. 특히 감청의 경우 그 침해가 은밀하고 계속적이라는 점에서 감청 기간을 엄격히 제한하는 등 최소한의 경우에 국한되어야 한다고 촉구하고 있으며 긴급통신제한조치의 폐지 필요성을 제기하고 있다.

둘째, 도/감청 기술의 발달에 따라 민간에 의한 불법 도/감청 행위가 범사회적으로 확산되고 있다. 특히 관련 법령의 미비로 전문 감청업체들이 생겨나면서 이를 단속할 근거 법령의 확보가 시급한 실정이다. 한편 통신비밀보호법은 송수신자를 당사자로 보고 있으며, 송수신자 모두의 동의를 받아야만 감청을 허용하고 있다. 이와 관련하여 우리 대법원은 송수신자 사이에서는 일방이 상대방의 동의없이 전기통신이나 대화를 채록하거나 녹음할 수 있지만, 제3자는 일방의 동의만을 얻어서 전기통신이나 대화를 채록하거나 녹음할 수 없다고 한다. 따라서 현재 많은 기업에서 직원들로부터 동의를 받아 전화나 이메일을 감청하거나 녹음하는 것은 통신비밀보호법 위반에 해당한다.

3.4.5. 해외 사례의 검토

최근 영국과 함께 에셜론 프로젝트를 통해 범세계적인 감청 혐의를 받고 있는 미국은 9.11 테러 이후 안보를 목적으로 한 국가기관에 의한 감청 행위가 더욱 확산되는 추세다. 이 같은 미국의 감청에 관한 중요 입법으로는 1968년 입법된 '일반범죄통제 및 도로안전법(Omnibus Crime Control and Safe Street Act)', 1978년의 '대외정보감시법(Foreign Intelligence Surveillance Act)', 1986년의 '전자통신 프라이버시법(Electronic Communications Privacy Act)', 1994년의 ' 법집행을 위한 통신지원법(Communications Assistance for Law Enforcement Act)'등이 있다.

미국의 경우 감청은 더 이상 폭력범죄와 중대범죄에 한정되어 있지 않다. 1968년 26건의 범죄를 대상으로 허용되던 감청은 1996년에는 95건의 범죄로 확대되었고 현재 감청 허용일수는 30일로 규정되고 있다. 특히 최근 미국 연방통신위원회(FCC)가 수사기관이 케이블 모뎀, 무선, 위성, 전력선 등 모든 형태의 초고속 인터넷 접속 통신을 감청할 수 있도록 규제를 강화해야 한다는 결정안을 가결한 상태다.

아울러 뉴질랜드의 경우는 감청 대상 범죄를 마약범죄와 조직범죄와 중대한 폭력범죄로 국

한하고 있으며, 오스트리아는 전화 도청의 경우에는 1년 이상의 징역에 처해질 범죄에 대해서만, 전자통신의 도청에 대해서는 조직범죄나 10년 이상의 징역에 처해질 범죄에 대해서만 허용하고 있다. 이탈리아의 경우에는 5년 이상의 징역에 처해질 범죄에 대해서만 도청을 허용하며, 룩셈부르크의 경우에는 2년 이상의 징역에 처해질 범죄에 대해서만, 일본의 경우에는 총기, 약물, 밀입국, 조직적인 살인과 관련된 조직범죄의 수사를 위해 감청이 허용되고 있다.

3.4.6. 종합대안

첫째, 통신제한조치에 있어서 '보충성'의 엄격한 적용이 필요하다. 보충성이란 수사기관이 통신제한조치 외에 다른 방법을 통해 수사를 진척시킬 수 없다는 상황을 설명하는 말이다. 현행법 역시 통신제한조치를 '범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다'고 하여, 통신제한조치가 다른 방법으로는 범죄의 수사가 불가능한 경우에 최후의 수단으로만 사용될 수 있다고 밝히고 있다.

그러나 검찰사건사무규칙에 따른 통신제한조치허가청구서(별지 제216호 서식)의 기재사항에는 이 보충성의 근거가 명확히 드러나지 않게 되어 있다. 통신제한조치허가청구서의 기재사항은 (통신제한조치를 받을 자의) 성명, 주민등록번호, 주거, 직업, 통신제한조치의 종류, 통신제한조치의 대상과 범위, 통신제한조치의 기간, 혐의사실의 요지 및 청구이유, 수통을 청구하는 경우 청구취지 및 사유, 재청구의 취지 및 이유, 기각 취지 및 이유로 구성되어 있어서 법률이 규정하는 보충성의 요건이 명확히 제시되지 않고 있다. 따라서 통신제한조치의 허가를 받으려면 다른 방법으로는 범죄의 수사가 불가능하다는 점을 법원이 판단할 수 있도록 청구서의 양식에 관련 근거가 명확히 기재되어야 하며 이를 위한 검찰사건사무규칙의 개정이 이루어져야 한다.

둘째, 통신제한조치의 적용 범위의 제한이다. 현행법은 통신제한조치의 대상범죄를 다소 포괄적으로 규정하고 있는데, 이는 수사기관의 해석에 따라 통신제한조치의 남용을 제도적으로 방조하는 결과를 낳고 있다. 따라서 통신제한조치는 수사기관에 의한 최소한의 수사방법이라는 점에서 대상범죄와 혐의의 내용을 보다 명확히 규정할 필요가 있다.

셋째, 긴급통신제한조치의 폐지를 검토해야 할 필요가 있다. 통신제한조치는 조치를 당하는 자가 모르게 진행되며, 30일 동안 모든 통신내역이 수사기관에 샅샅이 공개되는 것이므로 극히 예외적으로 인정되고 운용되어야 하며, 법원의 사전 관여는 필수적이다. 그러나 긴급통신제한조치는 법원의 관여 없이 이루어지기 때문에 수사기관에 의한 남용이나 인권침해의 위험성이 매우 큰 것으로 지적되어 왔다. 따라서 긴급한 수사가 요구될시에는 전화나 팩스를 통한 영장 청구 및 발부와 같이 법 집행 절차의 효율성을 증대하는 방향을 검토해 통신제한조치의 엄격한 영장주의를 준수해야 할 것으로 보인다.

넷째, 날로 증가하는 민간에 의한 불법 도/감청을 막기 위해 도청탐지업체의 등록제를 도입하고, 불법 도/감청 설비에 대한 사법경찰권을 확보할 필요가 있다. 아울러 국내 주요 정보보호기관을 통해 도/감청 방지기술에 대한 중장기적 계획을 수립하는 한편 불법 도/감청 행위를 근절하기 위한 대국민 인식 증진활동에도 주력해야 할 것이다.

3.5. 위치정보의 보호

3.5.1. 위치정보의 특성과 프라이버시 문제

최근 무선 인터넷과 모바일 기술이 급속히 발달하고 보편화되면서 다양한 위치기반서비스(LBS)가 제공되기 시작하였고, 이에 따라 위치정보의 활용이 중요한 사회적, 경제적 이슈로 떠오르게 되었다. 위치기반서비스는 물류, 교통, 광고와 마케팅, 생활정보, 보안, 위치기반 상거래 등 다양하게 활용될 수 있는 정보화 사회의 새로운 핵심 기반으로 자리잡고 있다. 나아가 '모바일 커머스' 등 새로운 부가가치의 원천으로서, 그리고 새로운 비즈니스 모델로 각광받으면서 차세대 성장산업이라는 중요한 역할로 평가받고 있다. 뿐만 아니라 위치기반서비스는 재난이나 사고 시 긴급구조와 같은 공공 목적으로 이용되는 등 그 활용 영역 또한 점차 확대되고 있다.

다른 한편 이러한 위치정보의 파악은 프라이버시 침해에 대한 우려를 낳고 있다. 개인의 활동영역과 활동내용이 파악됨으로써 행동의 자유가 제약될 가능성이 크기 때문이다. 특히 모바일 기술은 언제 어디서나 접속 가능하고 일상생활에서 늘 휴대하여 사용하고 있기 때문에, 지속적으로 축적되는 개인의 위치정보는 그 사람의 거의 모든 생활영역을 포괄하게 된다. 그리고 일반적인 개인정보가 도용 등을 통해 다른 용도로 쓰일 우려가 있는 것에 반해, 위치정보는 개인의 이동 궤적을 파악할 수 있게 함으로써 그 자체가 이미 직접적인 사생활 침해 요소로 작용한다. 이렇듯 위치정보는 매우 민감한 정보이며, 이에 따라 위치기반서비스의 프라이버시 침해의 심각성은 더욱 높아질 수밖에 없다.

3.5.2. 사회적 쟁점 및 현안 사례

앞에서 보았듯이, 위치정보의 활용은 긍정적 측면과 부정적 측면을 모두 담고 있다. 긴급구조나 수사 등 공공 목적으로 활용될 뿐만 아니라, 어린이와 노약자에 대한 위치정보는 개인의 안전과 보호를 위한 수단이 된다. 소비자에게는 편리함을 제공하기도 한다. 그러나 민감한 위치정보의 불법유출이나 도용의 위험이 항시 존재하며, 사생활 침해의 사례도 점차 늘어가고 있는 실정이다. 사회적 이슈가 되었던 실제 사례를 통해 이러한 이중성을 확인해 볼 수 있다.

첫째, 위치정보가 범죄수사나 긴급구조 등 긍정적인 방식으로 이용되었던 사례를 들 수 있다.

. 카드빚 갚으려 벌인 자작극 위치확인서비스로 미수(2003. 6, 한겨레)
. '명품' 여대생 납치 살해범 위치확인서비스로 검거(2003. 6, 중앙일보)
. 항공기 폭발물 허위신고 위치추적으로 덜미(2003. 5, 한겨레)
. 러시아 마피아 피살사건 휴대폰 위치추적이 일등공신(2003. 4, 한겨레)

. 삼성카드, 세계 최초 위치기반 본인확인 safe 카드 서비스(2003. 4, 매경)
. 대구 지하철 희생자 신분확인 일등공신 '위치확인서비스'(2003. 2, 한경)

둘째, 위와는 반대로 사생활 침해나 노동자 감시 등 위치정보의 오·남용 사례도 손쉽게 찾아볼 수 있다.

. 삼성SDI, 직원 휴대폰 불법복제 통한 위치정보 추적 피소(2004.7)
. 위치추적기 이용 사생활 뒷조사 심각(2003. 4, 한겨레)
. KTF 과실로 가입자 위치정보 누출 사고(2003. 1, 한겨레)
. 인터넷 심부름센터 위치추적으로 인한 사생활 침해 심각(2002. 5, 한겨레)
. 미국, 성폭력 전과자 GPS 추적 논란(2001, 12, 워싱톤포스트)

이러한 예에서 보듯이, 유비쿼터스 시대의 도래에 따라 위치기반서비스가 곧 보편화되고 급속하게 확대될 것이 예측되면서 위치정보의 악용 가능성은 매우 높은 것으로 나타나고 있으며, 이에 대한 적절한 방지 조치가 뒤따라야 할 것이다. 위치정보의 부정적인 이용 유형은 다음과 같다.

첫째, 기업에서 영리적 목적으로 악용하는 경우

기업에서 개인의 위치정보를 영리적으로 활용하기 위하여 개인의 위치정보를 수집·분석하는 경우, 이를 통해 개인의 성향을 파악할 수 있게 됨으로써 개인의 사생활을 심각하게 침해할 우려가 있다. 또한 위치정보가 제3자에게 유출되거나 불법적으로 거래되어도 확인하기도 어렵기 때문에 불법적으로 유출되거나 다른 업체에 판매될 가능성도 매우 높다. 개개인의 위치정보 분석 데이터베이스의 공유와 유통도 횡행할 가능성이 높다. 그 결과 밀착 마케팅이 개인의 평온한 생활을 깨뜨릴 가능성도 크다.

둘째, 사생활의 폭로나 명예훼손에 악용되는 경우

개인의 위치정보는 개인의 사생활을 폭로하거나 명예를 훼손하는 의도적인 불법적 행위에 이용될 수 있다. 특히 유명인사나 정치인의 경우 그 위험은 더욱 클 것이다. 그리고 이혼소송에서도 위치정보가 사생활을 폭로하는 방법으로 사용될 가능성이 높다. 위치정보는 특정 개인이 어디에 있는지를 확인할 수 있다는 점에서, 극단적인 경우 특정 개인의 신체와 생명에 위해를 끼치려는 불법적 행위를 가능하게 만들 수 있다.

셋째, 노동자 감시 및 통제의 강화에 악용되는 경우

직장에서 개인의 위치정보가 고객서비스의 강화나 서비스 품질의 개선이라는 명목으로 활용될 가능성이 높다. 특히 특정 작업장 안에서 일하지 않는 노동자의 경우 위치추적 시스템을 통해 노동통제 가능성을 높이게 된다. 또한 모니터링한 위치정보를 근무평정에 활용할 경우 노동 강도 또한 높아지게 된다. 이 경우 개인의 위치를 실시간으로 파악하게 되면 개인의 인권은 심각하게 침해될 가능성이 높고 부당한 노동통제로 이어질 수 있다.

넷째, 범죄수사 등 국가기관에서 남용되는 경우

위치정보를 범죄수사 목적이나 국가안보 명분으로 활용할 때 남용될 가능성에도 유의해야 할 것이다. 이 경우 심각한 인권침해의 문제가 발생할 수 있기 때문에, 이를 방지하기 위해서 수사에서 위치정보를 이용하고자 할 때 허용되는 요건과 절차가 명확하게 규정될 필요가 있다.

다섯째, 일상적인 사생활 노출로 프라이버시 의식의 약화 우려

위치정보로 인하여 개인의 활동이 보다 공개적으로 노출되게 될 것이다. 특히 일반 소비자들은 위치정보서비스 이용 시 자신들에 대한 위치정보가 얼마나 정확하며, 어떻게 이용되고 악용될 소지가 있는지에 대하여 잘 모르는 채 해당 서비스를 가볍게 이용할 가능성이 높다. 이는 전 사회적으로 사생활의 보호가 위축되는 것을 의미한다. 대부분 사람들이 위치정보서비스에 대한 광고와 위치정보서비스의 편리함 때문에 위치정보의 제공에 동의하게 될 경우 사회적으로 프라이버시 의식이 희박하게 될 우려가 있다.

3.5.3. 현행 법률 및 제도의 현황

모바일 기술의 활용이 점차 활성화되면서 위치정보의 보호는 중요한 과제로 떠오르게 되었다. 특히 위치정보는 개개인의 이동 상황을 추적할 수 있다는 점에서 일반 개인정보에 비해 그 중요성이 매우 높은 정보라 할 수 있으며, 따라서 일반적이고 포괄적인 개인정보 보호법에 규정되는 것을 넘어서 특수한 성격의 보호 법제가 필요하다. 그러나 현재 위치정보의 보호에 대한 별도의 법규정은 마련되어 있지 않은 상태이다. 현재 위치정보의 이용에 관한 법률 조항은 모호하거나 제대로 규정되지 않은 법률적 공백 상태라 할 수 있다. 이에 따라 기존의 경직된 법체계에 따라 운용되거나 비밀보호 등 다른 법률의 개인정보 보호 규정과 충돌을 일으키면서, 최근 긴급구조와 같은 공공 목적의 위치정보 이용이 오히려 제약되는 경우가 발생하기도 했다.

이에 독자적인 법률 제정의 필요성이 늘어남에 따라 정부에서는 ‘위치정보의 이용 및 보호에 관한 법률(안)’을 2003년 입법예고한 바 있고, 17대 국회에서 상정될 예정에 있다.

이 법안에는 이용자의 개인위치정보 보호와 위치정보의 오남용에 따른 피해보상 방안을 비롯하여 위치정보사업자의 자격 및 위치정보 수집 및 활용 상의 정당한 절차, 긴급구조나 재난방지 또는 범인체포 등 공공 목적의 위치정보 허용 근거, 그리고 위치기반서비스 관련 기술 개발 및 표준화 조항이 포함되어 있다.

(1) 위치정보 보호를 위한 독자 법률 필요성

국내 개인정보 보호와 관련된 법률 중 위치정보와 관련된 법률로는 통신비밀보호법, 전기통신사업법, 정보통신망이용촉진 및 정보보호 등에 관한 법률이 있지만, 아직까지 위치정보를 명확히 규정하고 보호하는 법률은 없는 상태이다. 본격적인 위치정보서비스를 위해서는 개인정보 보호와 함께 위치정보의 정확성, 위험성 등과 같은 위치기반서비스의 특수성을 고려한 법안이 필요하다.

우선 통신비밀보호법은 보호해야 할 통신정보를 범죄수사 등 예외적인 경우에 감청이나 발

신 기지국의 위치확인 등을 허용하기 위한 법률이다. 반면에 위치정보보호법은 정보화 사회의 새로운 인프라에 해당하는 위치정보를 철저히 보호하되, 본인 또는 동의를 얻은 제3자가 위치정보를 계약에 의해 널리 이용할 수 있도록 하기 위한 법률이라 할 수 있다.

둘째, 정보통신망이용촉진및정보보호에관한법률(이하 '정보통신망법')은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호하기 위한 법률이다. 반면에 위치정보는 비록 정보통신망법의 포괄적인 개인정보에 포함될 수 있으나, 그 성격이 위치정보 업자에 의해 획득되는 복합정보이며, 특정인의 신분을 인지하기 위한 일반 개인정보와 성격이 다르다고 볼 수 있다.

셋째, 정보통신기반보호법은 해킹이나 바이러스 등으로부터 정보통신시스템 전반에 대해 물리적, 전자적으로 보호하기 위한 법률이다. 반면에 위치정보보호법은 특정 정보시스템의 보호를 위한 법률이 아니라, 위치정보의 내용과 그 이용정보를 보호하기 위한 법률로서 별개의 법률이 필요하다.

(2) 위치정보 이용 및 보호 법률(안)의 주요내용

위치정보 이용 및 보호 법률은 유비쿼터스 시대의 본격적 개막을 앞두고 차세대 이동통신 서비스로 주목받는 위치기반서비스에 대한 법적 근거를 마련한다는 데 의의가 있다. 이 법의 기본방향은 두 가지로 이루어져 있다. 첫째, 기술발전 추세에 따라 위치기반서비스(LBS)와 관련 산업이 발전할 수 있도록 정부의 지원방안을 마련한다. 둘째, 위치기반서비스의 발전과정에서 발생되는 역기능의 방지와 이용자의 사생활 보호 등에 관한 사항을 강화한다. 즉 개인정보를 법으로 엄격히 보호하는 동시에 사회경제적으로 이용가치가 높은 개인위치정보를 IT산업과 접목시켜 다양한 관련 산업을 창출함으로써, '보호와 이용'이라는 두 가지 목적을 동시에 지향한다고 볼 수 있다.

이 법률은 크게 세 가지 내용을 담고 있다.

첫째, 위치기반서비스에 있어서 개인정보 보호를 위한 제도적 장치를 마련하고 있다. 우선 위치정보를 수집 처리 제공하는 위치정보사업자는 의무적으로 별도 시설과 설비, 인력을 갖추고 정통부 장관으로부터 허가를 받도록 명시했다. 이에 따라 위치기반서비스를 제공하는 통신사업자나 보험사, 차량운송정보업체 등은 정통부 장관의 허가를 얻어야만 사업을 할 수 있게 된다. (제5조)

또한 위치정보사업자는 개인이 동의하지 않은 정보에 대해 수집할 수 없으며, 약관에 명시하지 않은 목적 외의 용도로 위치정보를 이용하거나 제3자에게 제공할 수 없다. (제14조, 제15조) 특히 개인위치 정보주체의 권리 조항이 강화되어, 수집의 범위 및 약관 내용 중 일부에 대해 동의를 유보하거나 위치기반서비스의 일부에 대해 일시적 동의 철회가 가능하도록 규정되어 있다.(제15조 제2항, 제16조 제2항) 또한 위치정보사업자등에게 개인위치정보의 수집, 이용 및 제공 등에 대한 사항의 열람을 청구할 수 있도록 규정되어 있다.(제19조) 위치정보사업자가 개인위치정보를 제공하거나 접근한 모든 기록은 위치정보시스템에 자동으로 저장되며

정통부장관은 기록실태를 점검하도록 되어 있다.(제12조)

둘째, 위치정보가 긴급구조, 아동 및 노약자 보호 등 공공 목적으로 사용이 가능하도록 하고 있다. 우선 개인위치 정보주체가 119등을 통해 긴급구조를 요청할 경우 소방서와 경찰 등 공공구조기관은 위치정보시스템에 의해 위치정보사업자에게 해당 위치정보를 제공받게 된다. 이 밖에 천j재지변이나 비상사태가 발생할 경우 공공구조기관은 위치정보사업자가 해당 지역 내에 있는 개인들에게 위험 경보를 전달하도록 요청할 수 있다. (제22조)

셋째, 위치기반서비스의 활성화와 관련 국내 산업의 경쟁력 강화를 위한 정부의 지원방안을 담고 있다. 위치정보의 수집, 이용 및 제공 등과 관련된 기술개발을 위하여 연구개발과 관련표준을 정하여 고시할 수 있도록 되어 있다. (제25조, 제26조) 그리고 정통부장관은 위치기반서비스의 활성화를 위하여 기술 및 서비스의 활용과 보급을 촉진하기 위한 사업을 실시할 수 있다.(제28조) 이 법을 통해 통신사업자나 위치기반서비스 제공업체들은 합법적으로 개인위치정보를 수집 가공하고 부가가치를 생산할 수 있는 길이 열리게 되고 이를 통해 차세대 산업으로 주목받는 위치기반서비스 시장을 활성화하는 계기가 된다.

3.5.4. ‘위치정보의이용및보호등에관한법률(안)’의 문제점

최근 정보통신부와 시민단체 간에 벌어진 위치기반서비스 관련법 제정 논란은 위치기반서비스에 대한 기본 인식의 차이에서 기인하는 것으로 보인다. 정통부의 입장은 개인위치정보의 보호와 위치기반서비스 산업화에 대한 적절한 지원과 규제를 위해 ‘위치정보보호 및 이용등에 관한법률’의 제정을 추진하고 있는 반면, 시민단체는 이 법의 제정이 오히려 사업자에게 위치정보를 상업적으로 이용할 수 있는 근거로 작용할 가능성이 높다고 주장하면서 비판하고 있다.

(1) 진흥과 규제라는 법 목적의 혼재

정통부의 법안은 위치정보 이용을 촉진하는 입법 목적과 위치정보 보호의 입법 목적이 한 법률 안에 규정되고 있다. 따라서 위치정보를 보호하고 위한 법 조항은 유명무실해질 가능성이 높다. 더욱이 기본적으로 정보통신산업 진흥 역할을 맡고 있는 정보통신부 및 통신위원회가 주요 보호 조치를 담당하도록 되어 있는데, 위치정보서비스 산업의 이해를 고려하여 위치정보 보호의 임무를 소홀히 할 가능성이 크다.

특히 ‘위치정보의 이용기반 조성’을 규정한 이 법안의 제5장은 위치정보 이용을 촉진하기 위해서, 위치정보의 수집·이용 및 제공에 관련된 기술 및 기기의 개발에 필요한 정부의 예산 지원과 위치정보 이용 활성화를 위한 관련 기술 및 응용서비스의 효율적인 활용·보급을 촉진하기 위한 사업에 필요한 예산 지원을 할 수 있는 근거 규정까지 마련하고 있다. 이런 점에서 시

민단체들은 이 법안이 개인위치정보의 보호 보다는 이용촉진에 우선적인 목표를 두고 있다는 의구심을 감추지 못하고 있다.

(2) 위치정보의 프라이버시 영향 평가 미비

위치정보는 현재에도 제한적인 수준에서 이용되고 있지만 이를 규율할 법이 없는 법적 공백 상태이다. 따라서 이 법이 제정된다면, 위치정보의 이용이 합법화됨에 따라서 이용의 범위와 건수가 대폭 늘어날 것으로 예상되고 있다. 그러나 위치정보의 대규모 이용에 따라서 야기될 프라이버시 침해의 내용 및 정도에 대한 체계적인 평가는 부재한 상황이다.

더욱이 긴급구조와 같은 공공적 목적으로 위치정보를 이용하는 것과 다르게, 상업적 목적으로 위치정보의 이용을 무제한적으로 허용할 것인가에 대해서는 신중하게 판단해야 할 것으로 보인다. 위치정보가 다른 개인정보와 다른 민감한 정보이기 때문에, 단순히 정보주체의 동의만으로 위치정보의 이용을 제한없이 허용하는 것이 타당한 것인지 검토가 필요하다.

특히 위치정보는 서비스의 유형에 따라 어느 정도로 정확하게 위치를 파악해야 하는지가 달라진다. 따라서 위치정보서비스에서 목적 명확성의 원칙과 관련하여 중요한 것은 위치정보의 정확도, 즉 수집 범위의 문제를 포함한다. 그런데 이 문제는 다분히 기술적 측면과 연관되어 있기 때문에 이용자들로서는 목적에의 부합 여부를 정확히 알기 어렵다. 법률안은 정보통신부 장관이 고시를 통해 위치정보의 등급을 정할 수 있도록 하고 있다.(제27조) 그 등급에 따라 위치의 정확도나 응답 속도, 동의 절차 시행 여부까지 결정할 수 있게 되는 것이다. 그러나 이 문제는 행정부처에서 임의로 결정하는 것보다는 프라이버시 영향 평가제도 등을 도입하여 해결하는 것이 더욱 바람직할 것이다.

(3) 정보주체의 권리보호 조항 부족

이 법안의 위치정보의 보호 조항은 개인정보 보호에 관한 다른 법률의 규정보다 정보주체의 권리보호 조항이 강화되어 있다는 점에서 긍정적이지만, 몇 가지 점에서 보다 강화될 필요가 있다.

우선 동의는 사전에 서면으로 이루어져야 한다는 점을 명확히 할 필요가 있다. 현재 법률안은 이동통신사업자를 통해 일괄적으로 위치기반서비스에 대한 개인의 동의를 받는 방식으로 이루어져 있다. 그러나 이렇게 개인이 위치정보 수집에 동의했을 경우에도 해당 위치정보의 사용에 대해 포괄적인 동의를 했다고 말하기는 어렵다. 따라서 불편하고 비용이 드는 일부 문제에도 불구하고, 정보주체의 자기정보결정권을 강화하기 위해서는 각종 서비스의 종류에 따라 동의 여부를 별도로 물어야 할 필요가 있다.

또한 이용자가 원할 경우 위성항법장치(GPS)를 통한 정밀한 위치정보 추적 등을 원천적으로 회피할 수 있는 선택권이 보장되어야 할 것이다. 정통부는 2003년 긴급구조 등 공공부문

에서 위치기반서비스의 적극적 활용을 위해 휴대폰에 GPS 칩 장착을 의무화하겠다는 방침을 정한 바 있었다. 그러나 개인의 위치정보가 해킹 등 부정한 방법으로 유출될 가능성에 대한 우려가 높아지고, 시민단체들이 강력한 반대 의견을 표출함에 따라, 법률안에서 관련 조항을 삭제하였다. 그러나 일각에서는 여전히 LBS의 확산 및 활성화를 위하여 의무 장착 논란을 계속하고 있으며, 특히 이 법안에서의 표준화 조항에 근거하여 시행령에서 GPS칩 장착을 권고하고 있다. 따라서 GPS 칩의 의무 장착을 배제한다는 입법 취지와 다르게 시행령에서 이를 권고할 가능성을 배제하기 위해서 법률에서 이를 명시할 필요가 있다.

한편 이동전화 단말기 제조업자가 GPS 칩이 장착된 단말기만을 보급할 경우, 사실상 GPS 칩 의무화 효과가 발생하게 된다. 따라서 법률은 시장에 개입하여 기업이 GPS 칩을 장착하지 않은 단말기를 일정 비율 범위 내에서 공급하도록 하여, 이용자가 원할 경우 충분한 선택권을 행사할 수 있도록 해야 할 것이다.

(4) 공공목적의 위치정보 이용의 문제

긴급구조라는 특성상 위치정보 수집자가 직접 당사자로부터 동의를 확인하지 못하더라도 긴급구조기관에게 위치정보를 제공하는 것은 필요한 일이다. 문제는 긴급구조기관이 당사자로부터 구조요청을 받았는지를 확인하는 것이 쉽지 않다는 점이다. 공공구조기관 혹은 그 종사자가 긴급구조 요청을 받지 않았음에도 불구하고 다른 목적을 위해 개인위치정보를 요청하는 경우가 발생할 수 있다. 또한 다른 누군가가 악의적으로 긴급구조기관을 속이거나 불법매수할 경우 부작용에 대한 대처방안이 없다는 문제점을 갖고 있다. 따라서 긴급구조 관련 오남용을 차단할 구체적 대책을 규정할 필요가 있다.

이와 함께 긴급구조요청을 받아 위치정보사업자에게 개인위치정보를 제공받을 수 있는 ‘공공구조기관’을 보다 명확히 규정해야 할 필요가 있다. 예컨대 민간 경비업체 등의 영리적 목적을 가진 조직까지도 공공구조기관으로 지정할 것인지 등이 명확하지 않다.

또한 위험지역 내의 개인위치정보주체에게 위험경보를 하는 것은 당사자가 원하지 않았음에도 위치를 파악하여 경보를 발송하는 것이어서, 공익적 목적이라고 할지라도 지나치게 정보주체의 프라이버시권을 침해한다는 비판이 제기될 수 있기 때문에 보다 신중한 논의가 필요하다.

(5) 기기 소유자와 사용자가 상이한 경우의 문제

현실적으로 이동통신기기 소유자와 실사용자가 다른 경우가 많기 때문에 어느 쪽을 ‘개인위치정보주체’로 규정할 지가 문제가 된다. 대체로 위치정보 서비스 가입이나 탈퇴는 이동통신기기 소유자에 의해 이루어질 가능성이 높으며, 위치정보 제공의 동의나 동의 철회 등도 함께 이루어진다. 그러나 위치정보의 수집은 실제로는 이동통신기기의 위치를 수집하는 것이기

때문에, 실제 사용자에 대해 이루어진다고 볼 수 있다. 이에 따라 가입자의 동의 없이 실사용자가 서비스 자체를 탈퇴하는 경우가 발생할 수 있으며, 반대로 실사용자가 일시적 철회 등을 요청할 때, 서비스 가입 당사자가 아니라는 이유로 권리를 보장받지 못할 우려가 있다. 따라서 '개인위치정보주체' 와 '위치정보서비스 가입자' 를 구분할 필요가 있으며, 이러한 구분된 인식에 따라 기기 소유자와 사용자의 권리가 공히 인정될 필요가 있다.

3.5.5. 해외 사례의 검토

미국에서는 민간부문에서 활용되는 개인위치정보의 오남용을 방지하기 위해 2001년부터 '위치 프라이버시 보호법(Location Privacy Act)' 제정을 추진 중이다. 이 법안에서는 통신서비스업체가 휴대폰 사용자들의 위치정보를 수집할 경우 미리 본인에게 고지할 것을 강제하고 있다.

다만 '무선통신과 공공안전법(Wireless Communications and Public Safety Act)' 에 예외조항을 두어 긴급한 위기상황에 처한 당사자를 구제하기 위해 위치정보를 이용하는 것은 허용하고 있다. 1999년 미국 연방통신위원회(FCC)는 이동전화 사용자들이 911 사용 시 이동통신사업자가 위치정보를 공공구조기관에 의무적으로 제공하는 법안(Enhanced-911 Act)을 제정한 바 있는데, 2005년말까지 각 사업자당 전체 이용자의 95%에 대한 위치확인이 가능하도록 규정하고 있다.

유럽연합의 경우에도 2000년부터 긴급구조 E-112 서비스를 위한 시스템 규격 및 표준화를 위해 이동통신사, 의회, 구조기관, 자동차회사 등이 참여하여 LOCUS(Location Of Cellular Users for Emergency Services) 프로젝트를 추진 중이다. 2002년 3월 유럽평의회는 E-112 관련 법안을 상정했으며, 이 법안은 유럽 전역에서 서비스가 이뤄질 것과 사용자의 권한을 명시하고 있다. 또한 이동통신사업자는 응급서비스 관련기관(경찰, 소방서) 등에 112 신고자의 위치정보를 제공할 수 있어야 한다고 규정하고 있다. 또한 최근 유럽연합에서는 노약자 보호 및 의료서비스 등 복지와 관련한 위치기반 서비스에도 상당한 관심을 보이고 있다. 대표적 사례로 원격관리 서비스인 LOCOMOTION 서비스를 들 수 있는데, 2010년 이전까지 실현될 수 있도록 추진 중이다.

3.5.6. 개선방안의 제시

시민단체들은 대체로 위치정보가 다른 개인정보들보다 민감하기 때문에 특별한 보호가 필요하다는 점에서 별도의 입법에는 찬성하고 있다. 그러나 이 법안이 위치정보 이용이라는 진흥법의 성격과 위치정보 보호라는 규제법의 성격이 혼재되어 있어서 실제로는 보호조항이 사문화될 우려가 있다는 점에서 반대하는 것이다.

따라서 개선방안으로 ‘위치정보의보호및이용에관한법률(안)’의 수정을 제안, 위치정보보호법의 성격을 분명히 할 것을 주장하고 있다.

첫째, 위치정보 이용을 촉진하기 위해 연구개발 및 시범사업 등에 예산지원 근거 규정 등을 마련하고 있는 조항들을 삭제하고, 시민단체들의 제안처럼 법안의 명칭을 ‘위치정보보호및긴급구조시위치정보이용에관한법률’로 수정할 것을 검토할 필요가 있다.

둘째, 정보주체의 동의와 선택권 보장 등 권리 강화 등을 위한 관련 조항을 개정할 필요가 있다. 위치정보의 수집과 이용은 특정 부가서비스에 대한 사전 신청에 의해서, 그리고 해당 부가서비스에 필요한 범위 내에서만 이루어지도록 해야 할 것이다. 따라서 수집되는 정보의 내용과 목적이 분명하게 표시되어야 하고, 특정 서비스의 이용이 위치정보의 수집에 대한 포괄적인 동의로 간주될 수 없다는 점을 분명히 해야 한다. 즉 현행법의 포괄적 동의 방식을 개선하여, 선택적 거부권(opt-out)를 인정해야 할 것이다.

셋째, 일시적 동의 철회를 위한 기술적 조치 의무는 위치정보사업자뿐만 아니라, 이동통신기기 제조업자에게도 확대 적용되어야 할 것이다.

넷째, 긴급구조용 위치정보시스템이라 할지라도 ‘정보주체의 요청에 의해 작동된다’는 사실을 명문화할 필요가 있다.

다섯째, 위치정보기술의 상업적 이용이 야기할 프라이버시 침해 가능성을 평가하는 ‘프라이버시 영향평가’를 실시할 필요가 있다.

여섯째, 정통부 장관의 고시에 의해 위치정보 등급지정을 하도록 하는 조항을 개선하여, 독립적인 위치정보 등급심의위원회 혹은 개인정보기본법에 따라 설치될 개인정보위원회가 등급지정 권한을 갖도록 해야 할 것이다.

3.6. 생체정보의 이용 금지(제한)

3.6.1. 생체정보의 정의 및 범주

생체정보란 얼굴인식, 지문, 음성, 홍채, 망막, 손금, 서명, 정맥, 키스트록(key stroke), 걸음걸이, DNA 등 인간의 생리적 혹은 행동학적 특성을 모두 포괄한다. 인간의 생체 정보는 이름이나 주소 등의 개인정보와는 달리 소량의 정보만으로 분석이 가능하며 이를 통해 많은 정보를 얻어낼 수 있다는 특징을 가지고 있다. 즉 생체 정보는 누구나 가지고 있는 보편성, 개인의 고유성, 영속성을 그 특성으로 가지고 있다.

생체 정보는 위와 같은 특성을 가지고 있음으로 인하여 장점과 부정적인 선입견을 동시에 가지고 있다. 생체 정보를 이용하여 개인의 인증 및 보안을 한 단계 높일 수 있다는 점이 있는 반면에 범죄자의 악용, 오남용 문제가 발생할 수도 있다는 것이다. 또한 생체 정보를 획득하기 위해서 노력과 시간이 그리 많이 필요하지 않다는 점과 생체 정보가 당사자의 동의 혹은 인지 없이 수집, 이용될 수 있다는 점, 그리고 잠재적으로 상업적 이득을 위해 사용될 수 있다는 점에서 다른 정보에 비해 특별한 보호 대책 필요하다.

특히 국가 차원에서 생체 정보를 수집하는 것은 개인의 신체의 자유, 사생활의 자유 등 세계인권선언과 국제 인권 규범에서 널리 인정해 온 기본적 인권에 대한 침해일 뿐 아니라, 해당 개인을 잠재적 범죄자로 취급하여 무죄추정의 원칙을 정면으로 위배하는 행위가 될 수 있다.

그렇기 때문에 현재 지방자치단체 및 출입국관리소에서 행해지고 있는 신원확인을 위한 생체정보 인식에 관해 엄격한 이용 제한이 필요한 실정이다.

3.6.2. 사회적 쟁점 및 현안 사례

최근 생체정보 이용에 관련하여 나타나고 있는 유형은 크게 2가지로 나누어 살펴볼 수 있다. 미국, 일본 등에서 추진하고 있는 여권 발급에 있어 생체 정보 이용과 일부 지자체에서 사용하고 있는 지문 인증에 관한 것이다.

3.6.2.1. 출입국 시 생체여권 도입

(1) 일본은 입국하는 외국인의 신분 확인을 위해 지문대조를 위한 방안을 추진 중에 있다(세계일보. 2004. 7. 21).

(2) 미국은 비자 면제국에 대하여 생체여권을 1년 간 연기하기로 결정하였다(동아일보. 2004. 7. 26).

(3) 영국은 생체정보를 이용한 전자신분증을 도입하기로 하였으나, “테러 예방”이냐 “인권 침해”냐를 놓고 설전을 벌이고 있는 상태이다(동아일보. 2004. 4. 27).

(4) 우리나라도 출입국 때 홍채-지문정보를 채취하는 방안을 추진하기로 하였다(동아일

보. 2004. 4. 9).

(5) 미국은 무비자국도 입국 시 지문채취, 사진촬영을 의무화 하기로 결정하였다(문화일보. 2004. 4. 3).

(6) 인천공항과 나리타 공항에서는 생체인증 여권으로 출입국 관리를 시범적으로 실시하였다(문화일보. 2004. 1. 8)

(7) 일본은 2005년부터 생체정보를 칩으로 내장한 생체여권을 도입하기로 추진하였다(한국일보. 2003. 9. 8).

(8) 현재 우리나라는 출입국 관리 시스템이 텍스트 기반임에 따른 문제 해결을 위해 2007년부터 생체 정보를 기반으로 변경하기 위한 준비를 하고 있다(법무부 출입국정책추진단이 2004년 1월 9일 출범하였으며, 2004년 4월 2일 출입국관리 서비스체계 과학화 사업(TIPIS, The Technologic Infrastructure for Progressed Immigration Service)의 로드맵 보고회j를 개최하였다).

(9) 미국이 9.11. 테러 이후, 출입국 관리 강화 방침에 따라 지문 및 생체정보를 채취하는 것에 맞추어 외교통상부 역시 생체 여권 발급을 추진하기로 하였다.

3.6.2.2. 지문인식식별시스템 도입

(1) 충남지방경찰청이 선거법 위반사례를 수사하는 과정에서 지문을 이용하여 지목 수사하여 파문이 야기되었다(2004. 4. 30. 진보네트워크).

(2) 지방자치단체의 지문인식기 도입에 대해 인권 침해네 – 편해지잖아 파문이 확산되었다.(한겨레. 2004. 6. 15).

(3) 은행에도 지문인식기 보급 추진하기로 결정하였다(한겨레. 2004. 6. 11).

(4) 강남구청, 수원시, 경북 경주시, 영덕군 등 일부 지자체가 지문인식기를 탈법으로 운용하였다(한겨레. 2004. 6. 9).

: 수원시의 관내 동사무소에 인감증명 발급 시 신원확인을 목적으로 지문인식시스템을 도입하려다가 못한 사례가 발생하였다.

3.6.3. 현행 법률 및 제도의 현황

생체 정보 현재 나타나기 시작하는 개인정보이기 때문에 생체정보에 대한 명확한 정의와 왜 보호가 되어야 하는지, 이를 어떻게 보호해야 하는지에 대한 논의로부터 출발해야 한다. 아직까지는 생체정보와 관련된 법제 없이 이루어지고 있다.

3.6.4. 시민단체 및 정부의 입장

지문을 비롯한 생체정보는 개인정보 중에서도 매우 민감한 정보로서 함부로 채취하거나 이용되어서는 안된다. 왜냐하면 생체정보는 신원확인을 위한 가장 확실한 방법일 뿐 아니라 개인의 특성을 가장 안전하게 보여주는 정보이기 때문이다. 특히 국가 차원에서 생체정보를 수집하는 것은 개인의 신체의 자유, 사생활의 자유 등 세계인권선언과 국제 인권 규범에서 널리 인정해 온 기본적 인권에 대한 침해이고, 해당 개인을 잠재적 범죄자로 취급하여 무죄추정의 원칙에 정면으로 위배하는 행위이다.

남겨진 생체 정보의 오·남용 가능성, 집적된 데이터베이스의 확대 가능성 등의 문제를 제기할 수 있다. 그렇기 때문에, 세계 여러 나라에서 국민의 생체 정보를 수집할 때에는 다른 개인정보보다 엄격한 제한을 두고 있으며, 장기적으로 추상적인 목적으로 생체 정보를 수집하는 것을 금지하고 있다. 그러나 우리나라는 생체 정보를 도입, 사용하는데 있어서 규제할, 이용 금지할 명분적인 법률적 토대가 현재 존재하지 않는다.

현재 생체 비자를 통해 입국자를 인증하는 국가들은 단순히 인증만 할 뿐 생체 정보를 수집하지 않는다고 주장하고 있다. 그러나 이는 국내에서의 개인정보 수집과는 다르다. 왜냐하면 외국에서 정보를 수집할 경우, 개인이 보호받을 수 있는 방법이 별로 없고 실제적으로 합법적인 인증 절차를 밟는지 여부에 대해 정보 주체나 정부가 감독할 방법이 없기 때문이다.

국내에서는 생체 인식 정보를 안전하게 보호하고 관리하기 위한 구체적인 가이드라인이나 법률이 마련되지 않은 상황이다. 하지만 최근 생체정보 프라이버시 보호를 위해 한국정보보호진흥원을 중심으로 생체 정보보호를 위한 생체인식 시스템 운영 가이드라인을 마련하기 위한 작업에 나서고 있다.

3.6.5. 해외 사례

생체 정보에 있어서 캐나다는 소비자 생체인식 프라이버시 보호법(Consumer Biometric Privacy Protection Act) 제정하였고, 유럽은 Data Protection Directive 시행법, 미국은 IBIA(International Biometric Industry Association)와 IBG(International Biometric Group)에서 프라이버시 보호를 위한 원칙과 가이드라인을 제시하고 있다.

그 중 유럽연합의 Data Protection Directive 지침의 주요 내용을 살펴보면 다음과 같다. 이 지침에서는 개인정보를 생체 정보와 생체 정보로부터 추출된 템플릿(개인 고유의 생체 특징을 추출알고리즘을 이용하여 수집한 디지털 데이터) 및 이의 변형정보를 의미한다. 이 지침에서는 수집 및 이용 등에 관해 다른 개인정보보다 생체 정보를 더욱 엄격하게 다뤄야 한다고 규정하고 있다. 첫째 생체 정보를 수집할 경우 그 목적이 합법적이고 명확해야 하며, 정보 주체의 동의가 있는 경우를 제외하고 명시된 목적 외에 다른 목적으로 생체 정보를 이용하거나 제3자에게 제공해서는 안된다. 둘째 사용하는 생체 정보만의 수집 및 이용이 목적에 비교하여 과도하지 않은 방식이어야 한다. 셋째 생체 정보 수집 시 정보의 주체에게 수집 목적과 정보 관리자

를 고지하여야 한다. 특히 본인 모르게 생체 정보를 수집하는 것은 위법이다. 넷째 생체인식 시스템은 생체 정보의 파괴, 우연한 사고로 인한 손실, 변경, 파괴, 누출 등에 대한 적절한 보호방안을 지원하여야 한다. 다섯째 민감한 정보를 포함하는 생체 정보는 그렇지 않은 생체 정보보다 엄격한 개인정보보호의 기준을 적용하여야 한다. 마지막으로 중앙데이터베이스를 사용하는 경우 부당한 접근이나 다른 목적으로 사용될 가능성이 높으므로 사전 영향 평가를 받고 중앙데이터베이스를 사용하지 않는 시스템의 개발이 필요하다.

3.6.6. 종합대안

생체 정보는 그 정보가 가지고 있는 고유한 특성으로 인하여 여러 가지 장점이 존재함에도 불구하고 잘못 이용될 경우 크나큰 해악을 가지고 올 가능성이 높기 때문에 이용에 있어 엄격한 제한이 필요하다. 더더구나 현재 생체 정보에 대한 엄밀한 정의 및 범주에 대해서도 논의가 진행되지 않은 상황에서 생체 정보 인식 산업이 확장되는 것은 보다 빠른 생체 정보에 대한 숙의가 필요한 시점임을 뜻하는 것이라 할 수 있다. 이후 도입될 생체 여권 등은 세계적으로 확산될 예정이어서 생체 정보의 범국가적인 중앙 데이터베이스의 집적될 가능성에 대해 논란의 소지가 충분히 존재한다.

현재 우리나라의 경우에도 생체 정보에 관해 규제할 법·제도가 존재하지 않으므로 이에 대한 대비책이 조속히 마련되어야 할 시점이다. 또한 생체 정보에 대한 명확한 정의 규정이 필요하다. 더불어 국가에서 수집될 가능성이 있는 생체 정보에 대한 감시·감독의 의무를 개인정보보호위원회에 속하게 함으로써 생체 정보 이용 제한을 명확히 할 필요성이 존재한다. 뿐만 아니라 생체 여권에 따른 출입국 관리 시 인증 외 생체 정보를 사용하지 못하도록 규제 및 금지에 조항이 포함되어야 하며, 이러한 생체 여권 사용은 범세계적인 추세이므로 국제적인 규범화에 대한 노력이 필요하다. 또한 주민등록법 개정으로 지문 등의 생체 정보 수집을 금지하고 생체 정보보호를 위해 생체 정보 관리 시스템 운영에 관한 가이드라인이 마련되어야 한다.

3.7. 신원조사제도의 정비

3.7.1. 신원조사제도 정비 연구의 필요성

신원조사제도는 주민등록제도와 마찬가지로 매우 오랜 시간에 걸쳐 은밀한 인권침해를 낳을 수 있는 제도로 간주되어 왔다. 그럼에도 불구하고 제도의 개선에 대한 범사회적 논의는 통신비밀 침해나 주민등록제, 지문날인제 등에 비해 미미한 상황이다.

현행 법령은 공무원 및 군인, 교원 등의 임용시에 임용 예정자가 작성한 신원진술서에 대해 사실 확인을 거치는 신원조사를 관할 기관에 의뢰하고 그 결과를 회보 받을 수 있도록 하고 있다. 그러나 신원조사 의뢰 및 회보가 법령이 규정한 대상과 목적외에 불법적으로 이루어지고 있는 점, 조사와 판정이 비공개적으로 이루어져 불이익에 대한 호소가 쉽지 않다는 점 그리고 형의실효등에관한법률시행령에 따른 복권, 말소정보가 정확히 처리되지 않고 있다는 점에서 잦은 인권침해 논란을 낳고 있다.

3.7.2. 사회적 쟁점 및 현안 사례

(1) 국정원 신원조사 권한 불법 논란(2003. 8, 대통령령과 훈령 근거 기본권 제한)

(2) 인권위 국정원 및 경찰청 신원조사제 개선 권고안 발표(2003. 1, 사면·복권된 범죄경력 통보 헌법 침해 소지)

(3) 경남예고 국어과 교원 모집에 필기시험을 통과한 이 모씨가 신원조사회보서에 국가보안법 위반 혐의로 형을 받았다가 사면, 복권된 전과가 나타나자 학교장에 의해 임용 제청을 취소당함. 이에 대한 진정을 접수한 국가인권위원회는 형의 효력이 사라진 전과를 이유로 한 고용상의 차별 행위는 평등권 침해라고 지적.

(4) 교원 임용시 신원진술서 항목 논란(2002. 1, 본인 및 친인척의 좌익단체, 공산당 접촉 여부 기재)

3.7.3. 신원조사에 관한 현행 유관 법령 현황

1) 경찰공무원임용령시행규칙[일부개정 2002.3.11 해양수산부령 제00218호]

2) 경찰청과그소속기관등직제[일부개정 2004.5.24 대통령령 제18399호]

3) 경찰청과그소속기관등직제시행규칙[일부개정 2004.5.29 행정자치부령 제00231호]

4) 공무원인사기록및인사사무처리규칙[일부개정 1993.11.15 총리령 제439호]

5) 육공무원인사기록및인사사무처리규칙[일부개정2003.12.5교육인적자원부령제00821호]

6) 국회법[일부개정 2003.7.18 법률 제06930호]

7) 군무원인사법시행규칙[일부개정 2004.4.29 국방부령 제00562호]

8) 군종장교요원선발규칙[일부개정 1995.8.5 국방부령 제458호]

9) 대통령경호안전대책위원회규정[일부개정 2001.6.30 대통령령 제17270호]

10) 법원별정직공무원규칙[일부개정 2001.11.22 대법원규칙 제1724호]

11) 법원인사사무규칙[일부개정 2000.11.7 대법원규칙 제1675호]

12) 별정우체국직원인사규칙[일부개정 2002.2.25 정보통신부령 제00124호]

13) 보안업무규정[일부개정 2002.2.9 대통령령 제17517호]

14) 비밀보호규칙[일부개정 1997.12.30 대법원규칙 제01497호]

15) 선거관리위원회공무원규칙[일부개정 2004.3.13 선거관리위원회규칙 제00207호]

16) 선거관리위원회공무원인사기록및인사사무처리규칙[제정1995.2.4선거관리위원회규칙 제117호]

17) 선거관리위원회별정직공무원규칙[일부개정 1999.1.30 선거관리위원회규칙 제00160호]

18) 선원법시행규칙[일부개정 2002.6.11 해양수산부령 제00222호]

19) 소방공무원임용령시행규칙[일부개정 2004.5.29 행정자치부령 제00230호]

20) 정보및보안업무기획·조정규정[일부개정 1999.3.31 대통령령 제16211호]

21) 학생군사교육단무관후보생규칙[일부개정 2001.5.19 국방부령 제527호]

22) 행형법시행령[일부개정 2000.3.28 대통령령 제16759호]

23) 헌법재판소인사사무규칙[제정 1999.12.17 헌법재판소규칙 제107호]

24) 형의실효등에관한법률시행령[일부개정 2003.9.29 법무부령 제18104호]

3.7.4. 신원조사제도의 문제점

첫째, 국가기관에 의한 신원조사의 수행 권한과 대상, 항목에 대한 명확한 기준이 결여되어 있다. 정부기관은 물론 주요 금융기관을 비롯한 일반 민간업체들에서도 광범위한 신원조사가 음성적으로 이루어져 개인 프라이버시의 침해 여지가 매우 높다는 지적이다. 특히 이 같은 신원조사는 조사 과정이 비공개적으로 이루어짐으로써 불이익에 대한 당사자의 확인과 호소가 쉽지 않다는 점에서 더욱 은밀한 인권침해 행위로 간주되고 있다.

둘째, 신원조사시 수사자료표 정보가 말소 기간 이후에도 누락되지 않아 개인의 피해를 낳는 사례가 빈번하게 발생하고 있다. 혐의없음이나 공소권 없음, 죄가 안됨 등의 불기소처분을 받고도 수사기록이 5년간 보존되어 다양한 유형의 피해를 낳는 한편, 기소유예, 불기소처분, 무죄, 면소, 공소기각 등 경미한 범죄 기록도 5년간 지속되어 많은 민원을 낳고 있다.

3.7.5. 종합 대안

첫째, 현재 대통령령으로 범죄경력 및 수사경력 조회와 회보가 이루어지게 되어 있어 실제로는 정부기관은 물론 민간에서도 광범위한 신원조사 의뢰 및 회보가 이루어지고 있다. 따라서 조회와 회보가 가능한 경우를 법률로서 보다 명확히 규정함으로써 신원조사 행위를 엄격히 규제할 필요가 있다. 특히 현행 ’ 국가의 안정보장이나 공공의 안녕, 질서 유지 또는 공무수행을 위해 불가피하다고 인정해 대통령령으로 정한 경우 ‘의 조항은 지나치게 포괄적으로 해석되어 시급히 개정이 필요할 것으로 보인다.

둘째, 현재 신원조사를 위해 작성되는 신원진술서가 시대에 걸맞지 않는 신상정보의 기재를 요구하고 있다는 문제 제기를 수용해 통용되고 있는 관련 서식에 대한 일괄적인 검토 작업이 요구되며, 이후 시대에 걸맞지 않는 신원정보나 개인 프라이버시를 침해하는 항목 등에 대한 진술 요구를 제도적으로 막을 수 있는 서식 표준화 작업이 필요하다. 이와 함께 신원조사 의뢰 및 회보의 과정을 의뢰기관과 함께 당사자에게 공개하고 그 결과를 통보하여 오류에 의한 불이익을 적극적으로 해소할 수 있는 방법을 강구해야 한다.

셋째, 신원정보의 말소 기간에 대한 법제 정비가 필요하다. 현재 여당에서 논의 중인 ‘형의 실효등에관한법률’ 의 개정을 시급히 추진함으로써 5년간 존치되어온 불기소처분의 경미한 수사기록은 처분 후 즉시 삭제하는 방안을 검토해야 하며 신원조사 회보기관이 관련 법령이 담고 있는 말소 규정 집행을 위반할 경우 이를 법령에 의해 제재토록 함으로써 복권, 말소 대상 정보에 의한 개인의 불이익이 없도록 해야 할 것이다.

4. 주민등록 제도의 개선

4.1. 주민등록제도의 폐지 내지 개선

4.1.1. 주민등록제도의 현황

현행 주민등록제도는 1962년 5월 주민등록법을 제정하면서 시작되었다. 주민등록제도는 전 국민에게 강제되는 거주지등록제도, 전 국민에게 고유하고 불변하는 번호를 부여하는 주민등록번호 제도(고유번호제도), 모든 성인에게 강제 발급하는 주민등록증 제도(국가신분증제도)를 모두 포함하고 있다는 점을 특징으로 한다.

주민등록제도는 주민의 인적사항과 거주 이동의 실태를 파악하여 국방·조세·선거·교육·복지·주택 등 국가 행정사무의 효율적 활용 및 국민들의 인적사항 공증을 통해 국민의 편의를 도모하는데 그 목적이 있다. 이러한 목적에 따라 주민등록제도에서 다루고 있는 주요내용은 주민의 기본인적사항 및 가족사항, 주소 등을 기록·관리, 만 17세 이상 국민에 대한 주민등록증 발급, 주민등록 등·초본 형태의 공적 증명에 관한 것이다.

4.1.2. 제도의 폐지 내지 개선의 필요성 (시민단체 등의 문제제기)

주민등록제도의 폐지 내지 개선의 필요성은 다음과 같이 크게 3가지 문제점으로부터 도출될 수 있다.

첫째, 국가가 자원을 효율적으로 관리한다는 측면에서 합리성을 부여받을 수 있지만, 실제적으로 국민을 관리·통제하기 위한 수단으로 활용되고 있는 경향이 많이 보이고 있다. 즉 정부의 주민등록정보는 필요 이상의 정보를 축적하고 있다는 비판이 존재하며, 특히 전산화 과정에서 안정성이나 오용 가능성이 고조되고 있다.

둘째, 주민등록제도의 문제점은 보다 원칙적인 부분에서 제기될 수 있는 프라이버시 침해 가능성이 존재한다는 것이다. 일상생활에서의 거래 관계에 있어서 존재하는 계좌번호, 카드번호, 운전면허 번호 등은 각자 다른 목적을 위해 생성된 것이고, 각기 다르게 분리되어 사용되기 때문에 자동적인 방화벽으로 작동될 수 있다. 그러나 전 국민에게 표준 개인 식별자로서의 주민등록번호가 강제적으로 부여되고 있고, 일상생활 혹은 사이버 공간에서의 거래에 있어서 주민등록번호의 제출을 요구받고 있기 때문에, 이것은 개인정보통합의 형성 가능성을 발생시킬 수 있고, 그 무엇보다도 유출의 문제가 발생할 경우 개인에게는 크나큰 해악을 입힐 수 있다. 또한 타인의 카드를 대신 수령할 때까지도 주민등록번호를 기재토록 하는 등 주민등록번호의 사용이 일반화되어 있어 자신의 나이 또는 성별을 누구나 알 수 있게 됨에 따른 프라이버시 침해 문제도 심각하다. 특히 성전환자들에게는 주민번호를 통한 자신의 성별이 노출되는 것에 대

해 특히 민감한 문제로 인식 될 것이다.

셋째, 현재 우리나라에서 사용하고 있는 주민등록번호의 조합에 있어서의 차별을 들 수 있다. 앞의 6자리에서 개인의 생년월일을 파악할 수 있으며, 뒤의 7자리에서 성별 및 지역을 파악할 수 있음으로 해서 사회적인 차별이 발생할 수 있다는 것이다. 또한 뒤의 7자리 중 첫 번째 번호를 남성에게 1, 3을 여성에게는 2, 4를 부여하는 등 남성에게 우선번호를 부여함에 따른 성적인 차별 문제도 제기 되고 있다.

게다가 이러한 큰 문제 이외에도 소송 및 채권·채무 등 이해관계자에게 주민등록표 초본 열람 및 교부 시 당사자와 관계없는 세대주의 개인정보(성명, 주민등록번호)가 함께 열람되고 교부된다는 것을 들 수 있다. 또한 최근에 나타난 문제점은 위·변조한 주민등록증을 이용하여 여권의 부정발급, 사기 금융대출 등의 범죄가 발생하고 있고, 위조 기술의 고도화로 육안으로는 주민등록증 진위 여부 판단에 어려움이 발생하고 있다는 것이다.

4.1.3. 현행 법률 및 제도의 현황

현행 주민등록제도와 관련한 법률은 주민등록법, 동법시행령 및 동법시행규칙이 있다. 이러한 법률의 내용은 다음과 같이 요약해 볼 수 있다.

주민등록법은 행정사무의 원활한 처리를 위해 주민의 거주관계를 파악하고 인구동태를 명확히 하고자 제정된 법률이다. 특히 시 · 군 또는 구의 주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태를 상시로 명확히 파악하여 주민생활의 편익을 증진시키고 행정사무의 적정한 처리를 도모함을 목적으로 하는 법률이라 칭할 수 있다.

주민등록 사무의 관장은 시장, 군수, 구청장, 조례에 의하여 구청장, 읍·면·동장 또는 출장소장이 담당하며, 사무의 감독은 행정자치부 장관, 대통령령에 의하여 특별시장, 광역시장, 도지사에게 위임할 수 있다. 주민등록은 개인별 주민등록표와 세대별 주민등록표로 편제되어 있고, 각 기준은 세대주와 주소지이다. 주민등록제도 중 주민등록표의 내용은 별지서식으로 관리되며, 구체적인 내용이 법률의 규정으로 명시되어 있지 않는다. 그리고 주민등록증에는 성명, 사진, 주민등록번호, 주소, 주민등록증발급기관, 발급일자, 지문이 포함되어 있다. 주민등록 신고 시 포함되는 내용은 성명, 성별, 생년월일, 세대주와의 관계, 합숙사에 있어서는 그 관리 책임자, 본적, 주소, 본적이 없는 자 또는 본적이 분명하지 아니한 자는 그 사유, 대한민국 국적을 가지지 아니한 자는 그 국적명 또는 국적의 유무, 기타 대통령령으로 정하는 특수기술사항이 포함된다.

4.1.4. 해외 사례의 검토

거의 대부분의 국가에서는 각 나라의 고유한 신분증 제도를 운영하고 있으며 일본, 독일의

경우는 주민등록제도, 운전면허증, 복지카드를, 프랑스, 스페인은 국가신분증, 운전면허증, 사회보장·의료카드를, 미국의 경우는 운전면허증, 출생증명서, 사회보장카드(social security, 신분증으로 활용)를 신분증 제도로 사용하고 있다. 그러나 이러한 신분증 제도는 우리나라의 주민등록번호와 의미가 다르며, 신분증명을 위해 일련번호를 사용하고 있다. 예를 들어, 미국의 사회보장카드는 주정부에서 발급하며, 일련번호가 있어 이를 주민등록번호와 같은 기능으로 활용되고 있다.

이러한 외국의 국민(주민)등록제도 및 국가신분증제도의 내용을 구체적으로 살펴보면 다음과 같다.

(1) 독일

독일은 신분 등록은 신분법, 주거등록은 주법, 국가신분증은 신분증명법에 의해 규율되며, 각 제도는 서로 연계되어 있지 않다. 1971년 연방 차원에서 전 국민의 개인식별번호와 연방주거등록청의 설립 및 연방과 지방 사이의 주거등록전산망을 서로 연계하는 것을 목적으로 하는 법률안이 상정되었으나, 헌법상 기본권과 프라이버시 침해를 이유로 비판을 받아 처리되지 않았다.

독일의 신분등록제도는 출생 공증을 위한 출생부, 혼인 공증을 위한 혼인부, 사망을 공증하기 위한 사망부, 친족관계를 증명하기 위한 가족부로 구성되어 있다. 즉 독일의 신분제도는 사건별 편제 방식과 가족별 편제 방식을 혼용하여 사용하고 있다. 그리고 독일의 주거등록에 있어 각 주민은 주법에 따라 주소를 변경할 경우, 변경 사실 및 주소를 주정부에 신고해야 한다. 그러나 연방 정부가 관리하는 신분등록부와 지방정부가 관리하는 거주등록부는 별도로 관리되기 때문에 상호 연결되어 있지 않으며, 각 지방정부 사이에도 거주등록부의 정보를 상호 통보하지 않고 거주민등록전산망도 서로 연결되어 있지 않다.

독일 기본법 제116조 제1항을 보면 각 국민은 16세가 되면 신분증을 소지하고 조사할 권한이 있는 행정청의 요구가 있을 경우 제시할 의무가 있다고 제시되어 있다. 신분증에는 성과 이름, 학위, 예명, 출생일과 출생지, 신장, 눈의 색깔, 주소, 국적 등을 기재하고 일련번호를 부여하며, 이 중 성과 이름, 학위, 출생일, 일련번호, 유효기간에 대한 사항은 OCR로 판독이 가능하다. 이러한 내용은 심각하게 프라이버시 침해하는 것처럼 보이지만 침해적인 요소를 배제하도록 하는 여러 제도를 두어 신분증은 자신의 동일성 증명을 위해 그 소지자만 사용할 수 있는 그 목적만을 위하여 발생된 고유한 의미를 가진 것이 될 수 있는 것이다.

즉 독일은 연방 차원의 신분등록제도, 국가신분증제도와 지방정부 차원의 주거등록제도를 두고 있으나, 각 제도는 서로 분리되어 있으며, 특히 국가신분증은 엄격하게 독립되어 있다.

(2) 프랑스

프랑스는 모든 국민에게 개인식별번호를 부여하고 선거인 명부의 기능을 겸하는 국민의 신분기록을 중앙정부가 보유하고 있으나, 강제적인 주거등록제도를 두고 있지는 않다. 프랑스는 1973년 개인식별번호를 바탕으로 각 행정부처가 보유하고 있는 개인정보를 서로 연결하려고 하였으나, 취소되었다. 이후 1979년 컴퓨터로 판독이 가능한 개인신분확인카드의 발급을 계획하였으나, 이 역시 중도에 취소되었다. 결국 프랑스의 국민등록제도는 신분등록제도만으로 구성되어 있다고 할 수 있다.

프랑스의 신분등록제도는 민법 중 민적증명편에 의해 규율되며, 독일과 마찬가지로 사건을 중심으로 편제하는 사건별 편제 방식을 취하고 있다.

(3) 일본

일본은 신분등록제도로 호적제도, 주거등록제도로 주민기본대장제를 두고 있으나, 국민에 대한 개인식별번호제와 국가신분증제도는 채택하지 않고 있다.

일본의 호적제도는 인적편성주의에 기초하여 일본 국적을 가진 자에 대해서만 편제하며 부부 중심의 가족별 편성주의를 채택하고 있다. 또한 일본의 주거등록제도는 주민기본대장법에 기초하여 주민에게 지방자치단체에 대한 주소 및 주소이동의 신고의무를 부과하고 있다. 이 법에 있어서 특이한 점은 호적에 부표를 붙여 주소와 주소이동사항을 기재하도록 되어 있어, 개인의 거주관계변천은 호적에 의해서도 확인할 수 있고, 위와 같은 주민기본대장은 자기테이프나 유사한 형태의 매체에 기록할 수 있다.

(4) 미국

미국은 아주 느슨한 형태의 신분등록제도를 가지고 있으면서도 주거등록제도, 개인식별번호, 국가신분증제도가 존재하지 않는다. 미국에서는 출생기록이 국적기록이 되며, 출생, 사망, 혼인의 사건별로 편재가 되고, 가족관계는 기록되지 않으므로 사건별, 개인별 기록제도만 유지된다.

그러나 미국의 사회보장제도와 사회보장번호는 미국에서 생활하기 위해 반드시 필수적이므로 결과적으로는 강제적인 주민등록과 개인식별번호를 부여하는 것과 거의 동일한 효과를 주게 된다.

(5) 기타 나라들

영국, 캐나다, 뉴질랜드, 호주 등 영미법계 국가들의 대부분은 주거등록제도, 국가신분증제도와 개인식별번호를 두지 않는다. 특히 호주와 뉴질랜드에서는 1985년경에 도입하고자 했던 국가신분증제도가 시민운동으로 포기되었다.

스웨덴, 노르웨이, 핀란드는 신분등록제도에 주거등록제도를 결합하고 개인식별번호를 이용하여 동일성을 구분하는 제도를 도입하였다. 스웨덴의 경우, 1947년부터 전 국민에게 개인식별번호를 부여하고, 교회에서 관리하고 있는 거주민등록부를 국가적 차원에서 관리, 이를 1967년부터는 전산처리 하고 있다. 노르웨이의 경우는 1963년부터 국가단위의 주민등록제도를 도입하였으나, 이는 주로 통계의 목적으로 사용되므로 중앙통계국에서 관리한다. 덴마크와 벨기에는 1968년, 핀란드는 1972년부터 주민등록제를 도입하였다. 이들은 모두 개인식별번호를 부여하나 국가신분증 제도는 도입하지 않고 있고, 이것은 개인의 의무적인 신고가 아니다. 그럼에도 불구하고 이러한 국가들의 주민관리체계가 정확하게 이루어지는 것은 사회보장과 관련하여 개인에게 다양한 이익을 제공함을 목적으로 하기 때문이다.

특히 이러한 나라들에서 위와 같은 제도들이 갈등 없이 유지되는 까닭은 국민들이 정부의 활동으로부터 개인정보를 보호하기 위한 법률 및 제도적 장치를 가지고 있다는 점과 정부가 개인의 정보를 과도하게 요구하지 않는다는 것에 대해 시민들의 신뢰로 분석되고 있다.

<참고 3> 유럽연합국가 내의 주민등록제도

- 각국의 신분등록

신분등록 및 발급 강제 유무	**강제**	**자발**
국가	벨기에, 그리스, 독일, 스페인	네덜란드, 포르투갈, 오스트리아, 핀란드, 이탈리아, 룩셈부르크, 프랑스

- 발급주체

발급주체	**중앙정부**	**지방정부**
국가	오스트리아, 핀란드, 그리스, 포르투갈, 스페인, 네덜란드	벨기에, 이탈리아, 룩셈부르크, 프랑스, 독일

- 등록증에 들어가는 내용 중 일련번호

일련번호 유무	**유**	**무**
국가	핀란드, 프랑스, 독일, 스페인, 이탈리아, 룩셈부르크, 네덜란드	오스트리아, 벨기에, 그리스, 포르투갈

- 지문의 유무

지문 유무	유	무
국가	포르투갈, 이탈리아, 그리스	오스트리아, 벨기에, 핀란드, 룩셈부르크, 프랑스, 독일, 스페인, 네덜란드

4.1.5. 종합 대안

현재 정부는 현행 주민등록 제도를 유지하는 것을 전제로 주민등록법시행령 등의 개정을 통한 개인정보 유출을 차단할 수 있는 방안 마련, 그리고 위·변조된 주민등록증의 이용방지 및 주민등록증의 진위 확인을 위한 주민등록증 진위 확인 시스템이 개발·보급 등의 대안을 마련하고 있으나 앞에서 제기한 문제점을 해소하기에는 한계가 있어 아래와 같은 개선방안을 제시하고자 한다.

첫째 현행 주민등록번호는 유지하되 사용을 엄격히 제한하여 개인정보 유출을 근본적으로 차단할 수 있는 방안을 마련해야 한다.

먼저 민간부문에 대해서는 주민등록번호의 사용을 엄격히 규제할 필요가 있다. 주민등록번호가 모든 사람을 구분할 수 있는 고유번호이므로 데이터베이스 구축시 프라이머리 키(Primary key)로 주민등록번호를 사용하는 경우가 많다. 이렇게 되면 앞에서 지적한 대로 다른 사람의 주민등록번호를 이용해 그 사람의 프라이버시는 물론 경제적 불이익 등 심각한 문제를 야기하게 된다. 따라서 이에 주민등록번호의 사용에 대한 엄격한 규제방안을 만들어야 할 것이다. 즉 각 사업자들이 사업상 필요한 고객관리에 있어 주민등록번호가 아닌 별도의 번호체계를 사용토록 하여 주민등록번호의 오·남용이 발생하지 않도록 해야 할 것이다. 또한 정보통신사업자들의 경우에 회원모집 시 주민등록번호를 수집하는 관행이 주민등록번호의 오·남용을 초래하게 되므로 정보통신사업자들에게 주민등록번호 대신 전자서명인증의 활용을 권장하고, 쇼핑몰, 게임사이트 등 전자상거래가 이루어지는 사이트에 대해서는 전자서명제도의 이용을 의무화하는 방안을 마련해야 할 것이다.

다음으로 주민을 관리하는 기관에서는 현행 주민등록번호를 관리하되 개인에게는 별도의 개인식별번호를 부여하여 개인의 나이, 성별 등에 대한 정보 타인이 알 수 없도록 하는 방안을 마련해야 할 필요가 있다. 필요시에는 Mapping을 통해 개인식별번호와 기존 주민등록번호를 확인하도록 하는 방안을 마련하면 주민등록번호를 유지하면서 개인의 프라이버시를 보호할 수 있는 대안이 될 것이다.

둘째, 장기적으로 나이, 성별 등을 쉽게 알 수 있는 현행의 번호체계를 근본적으로 개선 할 필요가 있다. 앞에서 제기된 바와 같이 남자에게 우선번호를 부여함에 따른 성차별 문제, 그리고 성별과 나이를 누구나 알 수 있게 되어 있는 현행 번호체계로 인해 발생하는 문제를 근원적으로 해소하기 위해 기존 번호체계를 없애고 새로운 번호체계를 마련 할 필요가 있다.

셋째, 주민등록증의 강제발급 제도는 폐지하고 대신 대체 신분증명을 할 수 있는 방안을 마련해야 한다.

앞에서 언급한 바와 같이 주민등록증이 통제 수단으로 강제 발급하게 되었으므로 이는 모든 국민을 잠재적 범죄자로 취급하는 것으로 인식될 수 있다. 따라서 현재 본인확인, 거주확인 등을 위해 발급된 주민등록증을 없애고 운전면허증, 주민등록등본 등으로 본인확인 등을 대체하는 방안을 마련 할 필요가 있다. 필요시 현재의 운전면허증을 보다 위조하기 어렵게 만들어 운전면허증으로 신분확인을 기피하는 문제를 해소하고, 또한 얼굴, 지문 등을 이용해 본인확인을 하는 것도 대안이 될 수 있을 것이다. 거주 확인의 경우에는 미국과 같이 유틸리티(가스, 전기, 전화 등) 신청·설치 및 요금청구서 등을 위해 해당 회사에서 거주자에게 발송한 편지, 아파트전세(매매)계약서, 은행에서 발송된 편지와 같은 본인 거주를 분명히 할 수 있는 서류를 통해 확인하는 방안을 도입할 필요가 있을 것이다. 이 방법을 활용하면 실재 거주를 보다 명확히 할 수 있어 현재 문제가 되고 있는 위장전입 등의 문제도 동시해 해소할 수 있는 장점이 있다.

4.2. 지문날인제도의 폐지

4.2.1. 지문날인제도의 현황 및 개선 필요성

주민등록증의 지문 수록은 주민등록증을 최초로 발급한 1968년부터 이루어졌다. 주민등록증의 지문 수록은 지문이라는 정보가 국민 개개인 모두 상이하고 불변하는 특성이 있기 때문에 각종 범죄자 검거를 위한 수사 자료로의 활용, 과학적인 신원확인 등의 용도와 각종 사고, 행려병사자 및 신원 불명확자의 신원 확인을 위한 제도로써 활용되었다.

또한 주민등록증을 발급하면서 10 지문을 채취하는 것은 국민을 예비 범죄자로 취급하고, 사생활과 인권침해 등 헌법이 보장한 기본권 침해로 이어진다는 것으로 사회 쟁점화 되었고, 현재 헌법재판소에 계류 중이다.

최근 사회적 쟁점으로 제기되었던 사례는 다음과 같다.

(1) 행정자치부는 2004년 8월까지 전국 읍·면·동사무소와 은행 등에 총 1만 여개의 지문인식기를 보급하고, 신원확인과정에서 행정자치부가 관리하는 전 국민 지문정보를 제공하기로 결정함(주민등록증 위변조 식별시스템)

(2) 충남지방경찰청은 선거법 위반 사례를 수사하는 가운데 포스터에서 나온 지문을 바탕으로 표적수사함

(3) 법원에서 묵비하는 피의자의 신원조사를 위해 피의자의 지문을 날인하는 것은 위헌 소지가 있다는 판결을 함

(4) 국가인권위원회는 2003. 2월, 현행범으로 체포된 피의자라도 본인이 거부한 지문채취를 영장 없이 집행한 것은 인권침해라고 밝히고, 해당 경찰관에게 인권 교육을 실시할 것을 권고함

4.2.2. 시민단체 등의 문제제기

시민단체의 단체에서 위와 관련된 내용에 대해 현행 법률상의 문제점을 다음과 같이 제기하였다. 첫째, 주민등록법 상 10 지문날인의 근거 규정이 제대로 갖춰지지 못하였고, 단지 지문에 관한 언급은 단지 주민등록증에 수록할 내용으로서 별지서식에서 다루어지고 있을 뿐이다. 둘째, 10 지문의 경찰청 이첩의 근거 규정 또한 갖추지 못하고 있다. 즉 주민등록법에는 사법 경찰 관리의 신분증 제시 요구에 관한 규정(제17조의 10)을 제외하고는 10 지문정보를 경찰청에 이첩하는 것과 관련된 규정이 존재하지 않는다. 이와 더불어 주민등록법 시행령에 있어서도 경찰과 관련된 조항은 령38조의 규정뿐으로 이 규정은 단지 주민등록증 재발급 받을 때에 관할지서나 파출소에 재발급 신청자 명단을 통보하는 것만을 제시하고 있다. 셋째, 주민등록법 상에서는 왜 전 국민에 대해서 10 지문을 날인해야 하는지에 대한 근거를 제시하지 않고

있다는 점을 문제점으로 들 수 있다. 마지막으로 주민등록법은 정보주체인 본인이 주민등록정보에 대해서 자기정보통제권을 행사할 수 있는 방법을 제한하고 있는데, 법률상 이의 신청을 하는 경우가 극히 제한적이라고 할 수 있다.

4.2.3. 현행 법률 및 제도의 현황

지문날인제도와 관련된 현행 법률은 다음과 같다. 그것은 주민등록법 제17조의 8항과 동법 시행령 제33조이다.

- 주민등록법 제17조 8항

제17조의8 (주민등록증의 발급 등) ①시장·군수 또는 구청장은 관할구역 안에 주민등록이 된 자중 17세 이상의 자에 대하여 주민등록증을 발급한다. [개정 99·5·24]

②주민등록증에는 성명·사진·주민등록번호·주소·지문·발행일·주민등록기관을 수록한다. 다만, 혈액형에 대하여는 주민의 신청이 있는 경우 대통령령이 정하는 바에 따라 추가로 이를 수록할 수 있다. [개정 99·5·24][7)]

③제1항의 규정에 의하여 주민등록증을 발급받을 연령에 달한 자는 대통령령이 정하는 바에 의하여 시장·군수 또는 구청장에게 주민등록증의 발급을 신청하여야 한다. 이 경우 시장·군수 또는 구청장은 대통령령이 정하는 기간 내에 발급신청을 하지 아니한 자에 대하여 발급신청을 할 것을 최고할 수 있다. [개정 99·5·24]

④행정자치부장관은 필요하다고 인정될 때에는 시장·군수 또는 구청장으로 하여금 주민등록증을 일제히 갱신하거나 검인하게 할 수 있다. [개정 99·5·24]

⑤주민등록증 및 그 발급신청서의 서식과 그 발급절차는 대통령령으로 정한다. [개정 99·5·24]

⑥주민등록증의 발급에 있어서는 제17조의11의 규정에 의한 경우를 제외하고는 수수료를 징수하지 못하며, 주민등록증의 발급을 이유로 조세 기타 어떠한 명목의 공과금도 징수하여서는 아니된다. [개정 99·5·24] [전문개정 97·12·17]

- 주민등록법시행령 제33조

: 제33조 (주민등록증의 발급절차) ①시장·군수 또는 구청장은 법 제17조의8제1항의 규정에 의하여 주민등록증을 발급하고자 하는 때에는 그 발급대상자에게 6월 이상의 신청기간을 정하여 별지 제29호 서식에 의하여 통지하되, 그 발급대상자가 무단전출 등으로 인하여 통지

7) 최초의 지문날인의 법적 근거는 1970년 4월 10일 제정된 주민등록법시행령(대통령령 제4914호) 제33조 제2항이다. 이후 법률적 근거 없이 지문날인제도가 유지되어 오다가 1997년 12월 17일 법률 제5459호로 개정된 주민등록법 제17조 8 제2항에서 주민카드에 수록할 사항으로 지문을 명시함으로써 비로소 법률적 근거를 가지게 되었다.

서를 교부할 수 없는 때에는 이를 읍 · 면 또는 동사무소의 게시판에 공고하여야 하며, 통지 또는 공고한 사실을 개인별 주민등록표에 표기하여야한다.

②제1항의 규정에 의하여 주민등록증 발급통지를 받은 자 또는 공고된 자는 그 통지서 또는 공고문에 기재된 발급신청기간 내에 본인이 직접 주민등록이 되어 있는 시 · 군 · 자치구(이하 "주민등록지의 시 · 군 · 구"라 한다)의 관계공무원에게 사진(6월 이내에 촬영한 가로 3센티미터 세로 4센티미터의 탈모상반신의 사진을 말한다. 이하 같다) 1매를 제출하거나 그 사무소에서 직접 사진을 촬영하고, 본인임을 소명한 후, 그 공무원 앞에서 별지 제30호 서식에 의한 주민등록증발급신청서에 지문을 날인하여 신청하여야 한다.

③제2항의 규정에 의한 소명은 국가 · 지방자치단체 또는 공공기관에서 발급한 증명서(사진이 첩부된 것에 한한다)를 제시하거나 주민등록지의 이장이 확인하는 방법으로 한다. 이 경우 관계공무원은 본인여부가 심히 의심스러울 때에는 그 확인에 필요한 사항에 한하여 물어볼 수 있다.

④시장 · 군수 또는 구청장이 주민등록증을 발급하고자 하는 때에는 제42조의 규정에 의하여 행정자치부장관에게 해당자의 주민등록증발급을 요청하고, 발급된 주민등록증을 송부 받은 때에는 별지 제31호 서식에 의한 주민등록증발급대장을 작성하여 보관하여야 한다.

4.2.4. 종합 대안

현재 주민등록증 발급 시 10지문 날인제도에 대해 헌법 소원이 진행 중인 사안으로 헌법소원 결과에 따라 개선 방안이 검토되어야 할 것이나 현재 운영중인 10지문 날인제도는 그 목적이 명확하지 않고, 관련규정에도 10지문을 날인해야 된다는 명시적인 조항도 없는 상태에서 인권침해의 소지가 많은 이 제도를 계속 유지한다면 누구도 납득하기 어려울 것이다. 따라서 헌법 소원 결과와 상관없이 어떤 형태로든 현재 운영 중인 10지문 날인제도를 폐지하는 방향으로 추진되어야 할 것이다.

향후에도 국민의 인권침해 우려 등의 문제가 제기될 수 있는 제도를 시행할 때는 반드시 관련 이해관계자들과 그 타당성에 대한 검증이 이루진 후 관련 규정에 그 목적을 명확히 하고 운영상에 있어서도 인권침해가 발생하지 않도록 하는 장치를 마련해야 할 것이다.

참고문헌

강장묵·유의상·이정훈. 2003.「스팸메일 방지를 위한 제도적 기술적 해결방안에 관한 연구」. 『한국SI학회지』. 2(1): 25-33.

강준모, 2002,「직장내 모니터링 행위에 관한 법률문제와 제도 개선방안」,『정보통신정책』 제14권16호.

고영삼, 2001,「작업장 감시와 개인정보 프라이버시 보호대책」, 2001.08.

고웅렬. 「생체인식기술의 적용확산에 따른 EU의 개인정보보호지침」. KISA 국외동향보고서. 2003

금융감독원, 2004,「주요국의 신용정보 관리제도」

김남우, 2003,「온라인상의 소비자보호법제에 관한 연구」

김왕배·이경용, 2003,「인터넷 사용과 직무감시」,『경제와 사회』봄호(통권 제57호)

노동자감시근절을위한 연대모임, 2004,『노동자는 감시를 거부할 권리가 있다』, 노동자감시대응지침서 2004

문화연대 외. 2004.『정보인권 보장을 위한 35대 정책과제』, 인권시민단체가 꼽은 17대 국회 정보인권 과제, 2004.07.

민주사회를위한변호사모임 외. 2004.「US-VISIT과 화상인식기술」. 생체정보와 프라이버시 토론회 자료집.

변순정. 2004.「CCTV 사용으로 인한 프라이버시 침해와 영국의 규제현황」

안준모. 2003.「카메라폰과 개인정보침해」.『KISA 국외동향 보고서』

워릭, 케빈(정은영 역). 2004. 나는 왜 사이보그가 되었는가. 김영사.

이민영 주지홍, 2003,「전자정부시대의 개인정보보호: 법안분석 및 법제검토』, KISDI 이슈

리포트, 2003.11.

이민영. 「방법용 CCTV 운용사례에 대한 법적 검토」. 정보통신정책 16(16). 2004

이상헌. 「외국 스팸법 분석 및 국내법과의 비교」. KISA 국외동향보고서. 2003

이은우, 2003,「위치정보, 어떻게 보호할 것인가」, 진보네트워크센터 외,『정보인권과 위치정보의 보호』토론회 자료집, 2003.06.

이인호, 2003,「한국의 개인정보보호법제의 문제점과 정비방안」, 한국정보보호진흥원,『각국 개인정보보보 법제도의 비교법적 접근』, 제2회 개인정보보호 심포지엄.

전국정보운동포럼. 2004. 2004년 정보인권, 프라이버시를 논하자.

정영화, 2001,「정보사회에서 개인정보보호의 기준」, 정보운동강좌,『감시와 프라이버시』

정영화, 2003,「정보사회에서 프라이버시 보호를 위한 정책과제」, 함께하는 시민행동 '정보사회의제만들기' 제4차토론회

조동기 김성우, 2003,「인터넷의 일상화와 개인정보보호」, KISIDI 이슈리포트, 2003.08.

진보네트워크. 2002.「2002 정기국회 관련 정보통신 정책 제안」.

진보네트워크센터, 2003,「2003 정보인권 사업백서」

진보네트워크센터 외, 2003,『정보인권과 위치정보 보호』, 2003.6. 토론회 자료집

한국정보보호진흥원(KISA), 2003,「각국 개인정보보호 법제도의 비교론적 접근」, 개인정보보호심포지엄

한재각, 2004,「위치기반서비스의 프라이버시 문제」, 진보네트워크센터 외,『정보인권, 프라이버시를 논하자』, 전국정보운동포럼 자료집 2004.04.

함께하는 시민행동, 2001,「프라이버시 보호 가이드라인」, 2001.12.

함께하는 시민행동, 2003,「금융기관과 인터넷에서의 개인정보 공유현황 실태조사」, 2003년도 인권상황 실태조사 연구보고서

황윤경, 2002,「신용정보체계의 이해 및 현황」, 한국정보법학회 세미나

Clarke, Roger. 1999. "Introduction to Datasurveillance and Information Privacy, and Definitions of Terms."
URL: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Laurant, Cedric and Privacy International(PI). 2003. "Privacy and Human Rights 2003." URL: http://pi.gn.apc.org/survey/phr2003/index.htm

Rushkoff, Douglas. 2004. "The Networked Individual," TheFeature.
URL:http://www.thefeature.com/article?articleid=100802&sh=rushkoff&ref=3267310

Sholtz, Paul. 2001. "The Changing Definition of Privacy," ZDNet News.
URL: http://news.zdnet.com/2100-9595-530818.html

Waters, Gregory J. 2001. "Privacy and Security: An Ethical Analysis," Computers and Society, June. 8-23.

Waters, Nigel. 2000. "Rethinking Information Privacy - A Third Way in Data Protection?" Privacy Law and Policy Reporter vol.6, no.8.
URL: http://www.austlii.edu.au/au/journals/PLPR/2000/6.html

<부록 1> 국가인권정책기본계획(안)

1.1. 개인정보 수집 및 이용의 제한 원칙의 강화

◎ 필요성

-최근 개인정보침해 사례는 2000년 2,000건에서 2003년에는 2만 여건으로 급증하고 있다.

-개인정보의 보호 관련 일반법률로서 현재 공공부문의 '공공기관의개인정보보호에관한법률'과 민간부문의 '정보통신망이용촉진및정보호호등에관한법률'에는 개인정보의 수집 및 이용제한의 원칙이 비교적 잘 마련되어 있지만, 실질적인 면에서 많은 문제점을 안고 있다.

-현행법은 일괄동의 방식을 채택하고 있어서 수집 및 이용 제한원칙이 제대로 적용되지 않을 가능성이 높다.

-정보기술의 발달과 현대사회의 방대한 조직 등으로 인해 국가기구만으로 개인정보의 보호 및 관리를 위한 모든 역할을 다 하기에는 한계가 있으며, 개인정보 보호의 실효성이 떨어지는 문제가 발생하고 있다.

◎ 추진전략

1. 정보주체의 선택적 동의거부 및 적극적 동의 절차 마련 등 개인정보결정권 강화 방안
2. 공공기관 개인정보처리 현황보고의 인터넷 공개 통해 공공기관의 민감성 강화
3. 민간부문의 공동기구 설치, 공동의 기준 설정 및 자체 규제 강화
4. 개인정보 보호 및 감독을 위한 독립기구의 추진

◎ 근거 및 외국사례

-OECD의 '프라이버시보호 가이드라인' 8원칙 규정이 선례로서 유용한 지침이 되고 있음

-프랑스의 정보처리에관한법률, 독일의 연방정보보호법, 영국의 데이터보호법, 미국의 프라이버시법 등은 프라이버시 기본 원칙을 규정함. 정보수집자에게는 민간한 정보수집 금지, 목적외 사용금지, 안정성 확보의 의무를 규정하고, 한편 정보주체의 권리로서 동의권, 고지받을 권리, 열람 정정 삭제 청구권, 피해를 보상받을 권리 등을 규정하고 있음

-프랑스는 국가정보자유위원회, 영국은 데이터보호등록관, 스웨덴은 데이터감독위원회, 독일은 연방데이터담당관 등 감독기구를 두고 있으며, 미국은 행정감시기구를 설치하지 않고 업계의 자율규제를 허용하거나 개인에게 사법적 구제수단을 부여하고 있음

◎ 주관부서: 행정자치부, 정보통신부

1.2. 행정정보 공동이용에 대한 가이드라인 수립

◎ 필요성

- 정보기술의 발달로 국민편익 증진과 공공부문의 생산성 향상을 위한 정보공동이용의 필요성 제고
- 행정정보공동이용이 활성화됨에 따라 개인정보의 유출 등 프라이버시 침해 가능성 증대

◎ 추진전략

1. 정보공동이용 주관기관에서 관리해야 하는 권한과 의무에 대해 보다 명확히 규정
2. 정보 보유현황 및 활용현황, 공동이용 방안과 절차, 그리고 이용 가능한 기관의 권한과 의무 등을 국민에게 공개
3. 본인(개인)이 승인한 범위 내에서 정보공동이용이 가능하도록 하며, 주관기관 및 시민단체 등에 의한 주기적 점검
4. 개인에게 기본정보를 제외한 기타 정보의 공동이용 여부에 대한 선택권 부여
5. 제공된 정보는 각 기관의 업무에 따라 최소한으로 사용

◎ 근거 및 외국사례

- 미국에서는 인적정보 활용에 있어 프라이버시 보호를 위한 기준으로 개인의 동의, 유출금지, 정확도의 유지, 보안유지, 최소 정보의 사용, 기술적 신뢰성의 유지, 프라이버시 효과 평가 등을 제시
- 영국에서는 특히 정보공동이용의 운영상에 있어 규정제정과 운영기관의 선정, 투명성 강화, 관리·감독 강화, 개인정보의 최소화 사용 등을 중요시 함.

◎ 관련기관: 대법원, 각 행정기관 및 공공기관

1.3. 신용정보의 이용 및 보호에 관한 법률 제정

◎ 필요성

-최근 공공기관 및 신용정보업자등에 의하여 소비자의 신용정보가 정보주체의 동의 없이 무분별하게 수집·이용·제공됨에 따라, 신용정보의 유출과 남용 같은 사회적 문제가 발생하고 있다.

-현재 '신용정보의이용및보호에관한법률 '은 신용정보의 효율적이고 체계적인 이용을 도모하는 한편, 개인신용정보의 보호와 관련하여 신용정보의 수집 및 이용 제한, 공개원칙, 정보열람 및 정정청구권, 손해배상청구권 등을 규정하고 있지만, 정보주체의 권리가 보다 강화될 필요가 있다.

-현행법은 신용정보처리의 상당 부분을 시행령이 아닌 '금융감독위원회가 정하는 바'에 따라 처리하도록 규정하고 있어, 매우 자의적인 법 적용이 발생할 수 있다.

-신용정보의 수집 및 제공 시 형식적이고 일괄적인 동의 방식이어서 정보주체의 선택적 동의권이 인정되지 않고 있다.

◎ 추진전략

1. 신용정보의 수집 시 정보주체의 사전동의 원칙, 불가피한 경우 사후동의 절차 규정
2. 신용정보의 제공 동의 여부를 금융서비스 제공의 전제조건 행위 금지 조항 명시
3. 각 정보제공 대상기관들 및 제공항목들에 대해 동의 여부 선택권 부여
4. 금융감독위원회등의 자의적 지침에 따른 개인신용정보 처리 규정 정비, 법률로써 명시
5. 향후 '개인정보위원회'(가칭)등 외부기관에 신용정보 보호 및 감독 역할 부여 방안 고려

◎ 근거 및 외국사례

-미국: 공정신용거래법과 소비자신용보고개혁법(1996), 금융프라이버시법 등 별도 법률로써 신용정보 보호

-유럽: 개인정보에 대한 일반법률로써 신용정보 규율 체계

-일본: 일반 상거래 법령 및 행정부서의 통달 등에 의한 신용정보의 간접적 규제.

◎ 주관부서: 재정경제부 관련부서: 금융감독위원회, 금융감독원

1.4. 노동 감시에 대한 규제 법률 제정

◎ 필요성

-최근 통신이용에 대한 감시, 감시카메라(CCTV), 스마트카드, 통합정보시스템의 도입, 생체정보기술, 위치추적시스템 등을 이용한 노동자감시 및 노동통제 사례가 증가하고 있다.

-현재 노동자의 개인정보처리나 작업장 감시시스템과 관련하여 이를 특별히 규정하고 있는 포괄적인 법률은 아직 없고, 다만 노동관계법과 다른 법률에서 부분적으로 규정되고 있을 뿐이다. 다양한 노동감시시스템은 그 수단의 다양성과 다른 법률과의 관계로 인하여 현행 법체계로는 노동자의 효과적인 프라이버시 보호를 기대할 수 없는 실정이다.

-직장 내 감시기술의 도입과 운영에서 정보 주체인 노동자의 참여가 배제되고, 이에 따라 자신에 대한 정보가 어떻게 수집, 처리, 관리, 재가공되는지를 명확하게 알 수 없는 상태이다.

-개인정보의 수집 및 노동감시 장비의 도입 시 단체협약 등 명시적인 집단적 협의 조항이 없다.

◎ 추진전략

1. 노동자의 개인정보 보호를 위한 규정의 명문화
2. 노동감시 기술 도입을 단체협약의 필수협의사항으로 명문화
3. 노동감시 기술 도입 시 프라이버시 영향평가 제도의 도입
4. 정보주체인 노동자의 개인정보통제권 및 집단적 참가의 보장
5. 노동관계법률의 개정 및 노동감시의 규제 입법화 추진

◎ 근거 및 외국사례

-프랑스: 공공부문 사업장 감시시스템 도입 시 '국립정보자유위원회'에서 사전승인, 그 외 사업장은 '노동자위원회'와의 협의

-독일: 노동자평의회와의 공동 결정

-영국: 조사권한규제법(2000), 데이터보호법(1998)에서 작업장 프라이버시 보호 규정

-핀란드 노사관계 프라이버시 보호 특별입법, 네덜란드, 스웨덴, 노르웨이 등 감시시스템 도입 단체협약 규정

◎ 주관부서: 노동부 관련부서: 노사정위원회, 행정자치부, 산업자원부

2.1. 스팸메일의 규제

◎ 필요성

- 현재 수신자의 동의 없는 무차별적인 스팸 메일의 증가 추세

- 발신자가 동의 없이 일방적으로 수신자에게 원치 않는 메시지를 보낸다는 의미에서 스팸 메일은 프라이버시 침해 등의 법적 문제가 발생하는 것임

- 정보통신의 급속한 발전으로 인해 이러한 스팸 메일 외에도 휴대폰 문자 메시지, 팝업창, 전화, 팩스 등에서도 스팸이 발생

- 국내 뿐 아니라 국외의 외국어 스팸 및 p2p, 게시판 등 새로운 매체를 통한 스팸 역시 증가 추세

- 2004년 4월 기준으로 스팸대응연구팀에 접수된 상담 및 접수가 3만 5,982건으로 1, 2월의 기준보다 50%가 증가, 스팸 메일로 인한 경제적 손실도 수조에 다다르는 것으로 조사

- 뿐만 아니라 휴대폰 스팸 메시지의 발송 및 삭제로 인한 비용이 연간 3,000억에서 4,000억에 이르는 것으로 파악

- 이에 따라 스팸에 대한 적극적인 규제가 필요한 시점

◎ 추진전략

1. 정보통신망이용촉진및정보보호등에관한법률 50조의 개정

2. 스팸 메일의 경우 기존 옵트 아웃(선택적 거부) 방식에서 옵트 인(선택적 수용) 방식으로 전환

3. 위반 시 과태료 부과 및 처벌 사항 강화

4. 무단 이메일 추출 및 판매 유통에 대한 처벌 강화

5. 현재 휴대폰 스핌의 경우, 옵트 인(선택적 수용) 방식으로 결정, 그 외 매체 관련 사업자에 있어서도 옵트 인(선택적 수용) 방식으로 전환 필요

◎ 근거 및 외국 사례

- 정보통신망이용촉진및정보보호등에관한법률 50조

- 미국: 주 단위 및 연방 단위에서 스팸 메일 방지 관련 법안 시행(텍사스, 아리조나 주)

- 호주: 인터넷 사업자 연합회에게 자율권을 부여

- 호주, 미국, 영국: 호주 통신청(ACA)과 호주 경쟁소비자위원회(ACCC), 미 연방 거래위원회(FTC), 영 통상산업부(DTI), 영 정보 커미셔너, 영 공정거래청(OFT)과 협력하여 국경을 넘은 스팸 메일 대책 마련

- 유럽 연합: 메일 발송자가 메일링 리스트에 수신자 주소를 포함시키기 전 미리 허가를 받게 하는 옵트 인 방식의 규정 법제화

- 스페인. 라벨링 및 옵트 인 방식 도입

- 포르투갈. 자동송신장치나 팩스를 이용하여 보내는 스팸 메일은 수신자의 사전 동의 필요

◎ 관련기관: 정보통신부, 공정거래위원회

2.2. 통신비밀의 보호 개선방안

◎ 필요성

- 통신비밀 보호와 관련한 가장 큰 문제점은 국가기관을 통한 공익 명분의 통신정보수집 행위에 대해 제도적 보호대책이 미흡하다는 것으로 특히 주요 수사기관을 중심으로 행해지는 불법 통신정보수집 행위는 인권 침해의 주요 사례로 거론되고 있음.

- 민간에 의해 이루어지는 광범위한 불법 통신정보수집 행위에 대해 단속이 미비하며 기술적인 보호대책이 전무함. 현재 통신비밀보호법 위반 사례에 있어서 국가기관에 의한 위반 사례보다는 개인 또는 기업에 의한 사례의 증가추세가 더욱 높게 나타나고 있음.

- 현행 통신비밀보호법을 둘러싸고 정부와 민간에 있어서 포괄적인 인식의 차가 있음. 이 같은 인식의 차는 현행 통신비밀보호법이 국가 주요 수사기관의 통신비밀 보호 침해를 제도적으로 막지 못한다는 점과 동시에 정당한 수사 행위에 대해 민간이 법적으로 규정된 협조를 거부하는 사례들을 낳고 있음.

◎ 추진전략

1. 현재 통신정보 수집의 조건을 '수사 또는 형의 집행을 위해 필요한 경우'로 규정한 법적 조항을 '충분한 범죄혐의가 인정되는 경우'로 개정, 제한해 법리의 확대 해석을 막는 한편 엄격한 영장주의의 집행을 강화.

2. 현행법이 규정하는 '통신의 비밀'에 대해 통신의 내용뿐만 아니라 통신 상대의 인적 사항, 통신의 시간, 장소 등도 포함시켜 이 같은 자료의 공개를 청구할 경우에도 원칙적으로 영장주의를 적용.

3. 통신사실확인자료 요청의 요건에 통신 비밀 열람 외에 다른 방법을 통해서는 수사가 불가능하다는 '보충성'의 근거를 수사기관에 명확히 요구함.

4. 경찰청 사이버수사대, 개인정보보호위원회 등을 통해 민간에 의한 통신인권 침해 감시 활동을 강화함.

5. 정보보호진흥원 등 국내 정보보호 유관 기관들을 통해 정보보호 및 통신 프라이버시에 대한 대국민 인식을 증진시킬 수 있는 프로그램들을 시행함.

6. 통신비밀보호법에 대한 정부와 민간간 인식의 차로 인해 정당한 수사가 이루어지지 않는 사례를 막기 위해 유관 법률의 모호한 조항들을 보다 구체적으로 규정, 개정함.

◎ 관련기관 : 법무부, 정보통신부, 국가정보원, 검찰청, 경찰청.

2.3. CCTV 사용 규제

◎ 필요성

- 현재 강력한 범죄 예방의 수단 혹은 편리함, 효율성을 바탕으로 지자체 중심의 CCTV 도입 및 설치가 이루어짐
- 그러나 CCTV의 문제는 범죄와 무관한 사람들의 사생활 침해에 있음
- 이러한 CCTV 도입, 설치, 운영은 아무런 법적 근거 없이 지자체 및 경찰의 재량에 따라 이루어지고 있는 것이 현실임
- 또한 이러한 CCTV의 설치, 운영은 본래의 목적을 벗어나 감시의 체제로 사용될 가능성이 높기 때문에 조속히 법령 및 제도의 설치가 요구
- 그러므로 CCTV와 같은 영상 커뮤니케이션 매체 사용 규제에 대한 법 및 제도의 마련이 필요한 시점

◎ ·추진전략

- CCTV 관련 유관 법률(공공기관의개인정보보호에관한법률) 내의 법적인 검토 및 체계화 필요
- CCTV 도입·설치에 관한 명확한 기준 도입
- CCTV 운용의 목적, 데이터 수집 등에 대한 명확한 근거 및 가이드라인 제시

◎ ·근거 및 외국 사례

- 헌법 제10조, 시민적 및 정치적 권리에 관한 국제 규약, 공공기관의개인정보보호에관한법률, 공공기관의기록물관리에관한법률시행규칙, 정보통신망이용촉진및정보보호등에관한법률, 성폭력범죄의 처벌 및 피해자보호 등에 관한 법률,
- OECD 8원칙
- 영국: CCTV와 관련 데이터 보호법 시행령
- 미국: 컬럼비아 주법에 포함되어 있는 MPD(Metropolitan Police Department)의 CCTV 운용에 관한 법
- CCTV 관련 법제: 영국 개인정보보호법에 근거하여 CCTV 카메라 단속운영에 관한 시행기준, 미국 공공안전을 위한 CCTV와 지역사회경찰활동 가이드라인, 호주 사우스웨일즈주 공공장소에서의 CCTV 설치 및 운영에 관한 정책과 기준
- EU. CCTV 및 비디오 감시 관련 사례를 헌법, 법률, 여러 국가기관에서의 명령 및 판결을 바탕으로 규정

◎ 관련기관: 행정자치부, 경찰청, 정보통신부

2.4. 도감청 및 통신제한조치의 규제

◎ 필요성

- 국가기관에 의한 도/감청의 인권침해 사례가 여전히 빈번하게 일어나고 있음. 특히 감청의 경우 그 침해가 은밀하고 계속적이라는 점에서 감청 기간을 엄격히 제한하는 등 최소한의 경우에 국한되어야 한다는 범사회적인 요구가 증대하고 있음.

- 영장주의의 예외 조항인 긴급통신제한조치는 포괄적인 해석이 가능해 제도적으로 남용될 수 있다는 문제가 제기됨.

- 도/감청 기술의 발달에 따라 민간에 의한 불법 도/감청 행위가 범사회적으로 확산되고 있고 전문 감청업체들을 단속할 근거 법령의 확보가 시급한 실정임.

- 현재 대법원은 송수신자 사이에서는 일방이 상대방의 동의없이 전기통신이나 대화를 채록하거나 녹음할 수 있지만, 제3자는 일방의 동의만을 얻어서는 전기통신이나 대화를 채록하거나 녹음할 수 없다고 판결하고 있음. 따라서 현재 많은 기업에서 직원들만의 동의를 통해 전화나 이메일을 감청하거나 녹음하는 것은 통신 상대방의 동의를 얻지 않은 불법 도감청에 해당함.

◎ 추진전략

1. 통신제한조치에 있어서 '보충성'의 엄격한 적용을 강화함. 통신제한조치의 허가를 받으려면 다른 방법으로는 범죄의 수사가 불가능하다는 점을 법원이 판단할 수 있도록 검/경 청구서의 양식에 관련 근거가 명확히 기재되어야 하며 이를 위한 검찰사건사무규칙의 개정이 요구됨.

2. 통신제한조치 적용 범위를 제한함. 통신제한조치의 대상과 목적에 대해 다소 포괄적으로 해석이 가능한 문제 조항들을 보다 명확히 개정함.

3. 긴급통신제한조치를 폐지하고 긴급 수사시 전화나 팩스를 통한 영장 집행 절차의 효율성을 증대시켜 엄격한 영장주의를 구현함.

4. 도청탐지업체 등록제를 도입하고, 불법 도/감청 설비에 대한 사법경찰권을 확보함.

◎ 관련부처 : 법무부, 정보통신부, 국가정보원, 검찰청, 경찰청

2.5. 위치정보의 보호

◎ 필요성

-위치기반서비스의 보편화 및 급속 확대 추세 속에서 위치정보의 악용 가능성이 매우 높고, 최근 사생활 침해나 노동자감시 등 위치정보의 오·남용 사례가 늘어나고 있다.

-그러나 현재 위치정보의 보호 관련 법률은 모호하거나 명확한 규정이 없는 법률적 공백 상태로, 기존의 경직된 법체계에 따라 운용되는 실정이다. 이에 독자적 법률 제정의 필요성이 늘어남에 따라 '위치정보의 이용 및 보호에 관한 법률(안)'이 2003년 입법예고, 17대 국회에서 상정될 예정에 있다.

-정통부의 법안은 위치정보산업의 진흥과 위치정보 보호 규정이 한 법률 안에 존재하고 있어서 위치정보의 이용 촉진 동시에 규제라는 입법 목적의 혼란이 야기되고 있다.

-특히 정보통신산업 진흥 역할을 맡는 정보통신부가 위치정보의 보호 조치를 담당하도록 되어 있어 소홀히 다루어질 가능성이 높다.

-위치정보의 상업적 이용이 대규모로 늘어나고 있지만, 이에 따라 야기될 프라이버시 침해의 내용 및 정도에 대한 체계적인 평가는 부재한 상황이다.

-현재 법률안은 위치기반서비스에 대해 일괄적으로 개인의 동의를 받는 방식으로 이루어져 있어, 서비스의 종류에 따른 선택적 동의 여부가 보장되지 않고 있다.

- '공공구조기관'의 명확한 규정과 같은 긴급구조 관련 오남용을 차단할 구체적 대책이 규정되지 않고 있다.

-이동통신기기 소유자와 사용자가 상이한 경우, '위치정보서비스 가입자'와 '개인위치정보주체'의 명확한 구분이 없어 각각의 권리에 대한 규정이 명확하지 않은 상태이다.

◎ 추진전략

1. '위치정보의보호및이용에관한법률(안)'의 수정, 위치정보 보호법의 성격 강화
2. 현행법률안의 일괄적 동의 방식 개선, 선택적 거부권(opt-out) 인정
3. 긴급구조 목적 이용 시 '정보주체의 요청' 조항 명시
4. 위치정보기술의 프라이버시 영향평가 실시
5. 독립적인 '개인정보위원회'(가칭) 등에 등급지정 및 위치정보 보호 감독 권한 부여

◎ 근거 및 외국사례

- 미국: '위치 프라이버시 보호법' 제정 추진, '무선통신과 공공안전법'에 긴급구조 목적의 위치정보를 이용 허용 및 촉진.

- 유럽연합: 긴급구조 E-112 서비스 관련 법안 추진

◎ 주관부서: 정보통신부 관련부서: 산업자원부, 행정자치부, 노동부

2.6. 생체정보의 이용 금지(제한)

◎ 필요성

- 생체 정보란 얼굴인식, 지문, 음성, 홍채, 망막, 손금, 서명, 정맥, 키스트록(key stroke), 걸음걸이, DNA 등 인간의 생리적 혹은 행동학적 특성 포괄
- 인간의 생체 정보는 이름이나 주소 등의 개인정보와 달리 소량의 정보만으로 분석 가능
- 또한 생체 정보의 습득에 있어 다른 정보와 달리 노력과 비용 면에서 유리
- 특히 국가 차원에서 생체 정보를 습득하는 것은 개인의 신체의 자유, 사생활의 자유 등의 세계인권선언에서 널리 인정해온 기본적 인권에 대한 침해
- 해당 개인을 잠재적 범죄자로 취급하여 무죄 추정의 원칙을 위배하는 행위
- 그러므로 생체 정보는 당사자의 동의 혹은 인지 없이 수집, 이용될 수 있으므로 다른 정보보다 특별한 관리 필요

◎ 추진전략

- 생체 정보 수집, 이용 제한에 대한 법 제정 필요
- 생체 정보에 대한 감시·감독의 의무를 개인정보보호위원회에 속하게 함으로써 생체 정보 이용 제한을 명확히 할 필요성
- 여권법 개정을 통해 출입국 관리 시 인증 외 다른 목적 사용 규제 및 금지
- 국가의 출입국 관리 시스템에 대한 관리 감독 필요, 국제 규범화에 대한 노력 필요
- 주민등록법 개정으로 지문 등 생체 정보 수집 금지
- 생체 정보보호를 위한 관리 시스템 운영 가이드라인 마련

◎ 근거 및 외국 사례

- 현재 국내에서 생체 정보의 수집, 이용에 대한 법적 근거 미비
- 캐나다: 소비자 생체인식 프라이버시 보호법(Consumer Biometric Privacy Protection Act) 제정
- 유럽: Data Protection Directive 시행법
- 미국: IBIA(International Biometric Industry Association)와 IBG(International Biometric Group)에서 프라이버시 보호를 위한 원칙과 가이드라인 제시
- 유럽 연합. Data Protection Directive. 이 지침에서는 수집 및 이용 등에 관해 다른 개인정보보다 생체정보를 더욱 엄격하게 다뤄야 한다고 규정

◎ 관련기관: 행정자치부, 외교통상부, 법무부, 출입국관리소, 경찰청

2.7. 신원조사제도의 정비

◎ 필요성

- 현행 법령이 규정하는 신원조사의 대상 및 목적 외에 불법, 음성적인 신원조사 의뢰, 회보가 범사회적으로 만연함.

- 신원조사의 과정과 결과가 공개되지 않아 불이익에 대한 당사자의 확인과 호소가 어려움.

- 신원조사시 수사자료표 정보가 말소 기간 이후에도 누락되지 않아 불이익을 낳는 사례가 빈번함.

◎ 추진전략

1. 대통령령으로 이루어지는 신원조회와 회보를 법률로서 보다 명확히 규정함으로써 불법 신원조사 행위를 근절함.

2. 신원조사를 위해 작성되는 신원진술서에 시대에 걸맞지 않는 신원정보 부문과 개인 프라이버시를 침해하는 항목 등을 삭제함.

3. 신원조사 의뢰 및 회보의 과정을 의뢰기관과 함께 당사자에게 공개하고 그 결과를 통보하여 오류에 의한 불이익을 적극적으로 해소할 수 있도록 함.

4. '형의실효등에관한법률' 개정을 시급히 추진해 불기소 처분의 경미한 수사기록은 처분 후 즉시 삭제케 하고 신원조사 회보기관이 관련 법령이 담고 있는 말소 규정 집행을 위반할 경우 이를 법령에 의해 제재토록 함.

◎ 관련부처 : 법무부, 경찰청.

3.1. 주민등록제도의 폐지 내지 개선

◎ 필요성:

– 주민등록증의 강제발급 등은 국민을 관리·통제하기 위한 수단으로 활용되고 있는 경향이 많으며, 주민등록정보에 필요 이상의 정보를 축적하고 있음.

– 일상생활은 물론 사이버 공간의 거래까지 주민등록번호를 과다하게 사용함에 따라 유출 시의 개인의 프라이버시 침해 우려, 특히 전산화 과정에서 안정성이나 오용 가능성이 고조

– 번호체계상에서는 앞의 6자리에서 개인의 생년월일을 파악할 수 있으며, 뒤의 7자리에서 성별 및 지역을 파악할 수 있음으로 해서 사회적인 차별이 발생할 우려와 남성에 우선번호를 부여함에 따른 성적 차별 문제 등이 제기됨

◎ 추진전략

1. 현행 주민등록번호는 유지하되 번호의 사용을 엄격히 제한
2. 민간부분 사업자들의 고객관리 등에 주민등록번호가 아닌 별도의 번호체계를 사용
3. 개인의 나이, 성별 등의 정보가 아닌 별도의 개인식별번호를 부여
4. 장기적으로는 주민등록 번호체계를 근본적으로 개선
5. 주민등록증의 강제발급 제도는 폐지

◎ 근거 및 외국사례:

– 일본, 독일: 주민등록제도, 운전면허증, 복지카드 사용

– 프랑스, 스페인: 국가신분증, 운전면허증, 사회보장·의료카드 사용

– 미국: 운전면허증, 출생증명서, 사회보장카드(social security, 신분증으로 활용) 사용

– 그러나 이러한 신분증 제도는 우리나라의 주민등록번호와 의미가 다르며, 신분증명을 위해 일련번호 사용

◎ 관련기관: 대법원, 정보통신부 등 각 행정기관

3.2. 지문날인제도의 폐지

◎ 필요성

- 주민등록법 상 10 지문날인의 근거 규정 미비
- 10지문 날인제도의 목적이 불명확
- 10지문 날인제도는 모든 국민을 잠재적 범죄자로 본다는 의미 함축
- 경찰청 등 타 행정기관에 지문관련 정보제공에 대한 근거 규정 미비

◎ 추진전략

1. 주민등록법의 개정
2. 주민등록법시행령 개선
3. 10지문 날인제도 폐지

◎ 근거 및 외국사례: -

- 유럽연합 국가 중에서 지문 날인을 하는 국가와 하지 않는 국가로 나누어 살펴보면
- 포르투갈, 이탈리아, 그리스는 지문 날인
- 오스트리아, 벨기에, 핀란드, 룩셈부르크, 프랑스, 독일, 스페인, 네덜란드는 지문 날인을 하지 않았음
- 그러나 이러한 나라들에서 갈등을 야기하지 않고 제도들이 유지되는 까닭은 국민이 정부의 활동으로부터 개인정보를 보호하기 위한 법적인 장치 및 제도를 가지고 있기 때문

◎ 관련기관: 경찰청 등 각 행정기관

<부록 2> 국가인권정책기본계획(안) 정리표

과제명	주관부처	관련부처	비고
1. 개인정보보호를 위한 법률 및 제도			
1.1. 개인정보 수집 및 이용의 제한 원칙의 강화	행정자치부 정보통신부		
1.2. 행정정보 공동이용에 대한 가이드라인 수립	행정자치부 정부혁신·지방분권위원회	대법원 각 행정기관	
1.3. 신용정보의 이용 및 보호에 관한 법률 제정	재정경제부	금융감독위원회 금융감독원	
1.4. 노동 감시에 대한 규제 법률 제정	노동부	노사정위원회 행정자치부 산업자원부	
2. 프라이버시 보호를 위한 현안 문제			
2.1. 스팸메일의 규제	정보통신부	공정거래위원회	
2.2. 통신비밀의 보호 개선방안	법무부	정보통신부 국가정보원 검찰청 경찰청	
2.3. CCTV 사용 규제	행정자치부	경찰청 지방자치단체	
2.4. 도감청 및 통신제한조치의 규제	법무부	정보통신부 국가정보원 검찰청, 경찰청	
2.5. 위치정보의 보호	정보통신부	산업자원부 행정자치부 노동부	
2.6. 생체정보의 이용 금지(제한)	행정자치부, 외교통상부	출입국관리소 법무부, 경찰청	
2.7. 신원조사제도의 정비	법무부	경찰청	
3. 주민등록 제도의 개선			
3.1. 주민등록제도의 폐지 내지 개선	행정자치부 정부혁신·지방분권위원회	대법원 각 행정기관	
3.2. 지문날인제도의 폐지	행정자치부 정부혁신·지방분권위원회	경찰청 등 각 행정기관	