정보화에 따른 프라이버시권 침해법령 조사 연구

국가인권위원회

정보화에 따른 프라이버시권 침해법령 조사 연구

국가인권위원회 2002년도 인권상황 실태조사
연구용역사업 최종 보고서를 제출합니다.

2002. 12. 27.

연구자 이은우(노동자감시근절을위한연대모임)
장여경(노동자감시근절을위한연대모임)
이지선(노동자감시근절을위한연대모임)
김승만(노동자감시근절을위한연대모임)

< 목 차 >

Ⅰ. 서론 - 프라이버시의 종말[1]과 감시[2]사회의 도래

1. 감시기술의 발달과 감시활동의 확대

가. 감시기술의 발달

오늘날 정보처리기술, 생체인식기술, 유전자정보 분석기술 등의 급속한 발달에 힘입어 감시기술은 우리의 상상을 초월할 정도로 발전하고 있다. 이로 인한 감시의 양적, 질적 증대는 우리에게 새로운 관점에서 감시문제를 바라볼 것을 요구하고 있다.

(1) CCTV 감시[3][4]

오늘날 은행, 지하철, 백화점, 편의점, 주유소, 병원, 주차장, 버스 등 공공장소이건 사적인 장소이건, 직장이건 할 것 없이 CCTV가 설치되어 실시간으로 감시가 이루어지고 있다. 최근에는 DVR(Digital Vedeo Recording) 시스템이라고 하여 디지털화된 비디오 재생시스템이 널리 쓰이고 있는데, 이것은 기존의 아날로그 방식의 CCTV보다 화질도 선명할 뿐만 아니라 저렴한 비용으로 녹화된 정보를 저장하는 것이 가능하고, 편의에 따라 검색이 가능하고 비용도 저렴하다.[5] 최근의 CCTV는 확대기능, 각도조절 및 회전기능, 야간촬영기능, 투시촬영기능, 열이나 소리나 움직임을 감지하여 자동촬영을 할 수 있는 기능, 달리는 자동차의 번호판의 번호를 식별할 수 있는 고속촬

---

1) 프라이버시의 종말이라는 표현은 렉 휘태커의 저서 The End of Privacy(1999, 우리말 번역서의 제목은 개인의 죽음, 이명균, 노명현 역, 2001, 생각의 나무 간)의 제목이기도 하고, 저명한 프라이버시 연구자인 마이클 프룸킨의 논문 'The Death of Privacy'(Stanford Law Review,)의 제목이기도 하다.

2) 감시라는 표현은 가치중립적이고 대등한 관계에서의 계약적 관계라는 의미를 내포하고 있는 개인정보의 취득이라는 표현보다 정치적이고, 권력적인 개념으로 이해된다. 이 글에서 개인정보의 취득이라는 표현 대신 감시라는 표현을 사용한 것은

3) CCTV(Closed Circuit Televsion)는 영상정보를 특정의 목적으로, 특정의 수신자에게 전달하는 시스템을 말하는데, 일반인에게 제공하는 개방형 텔레비전 방송시스템에 대응한 폐쇄형 텔레비전 시스템을 지칭하는 말이다. 최근에는 디지털 방식의 DVR(Digital Video Recorder) 시스템이 아날로그 방식의 CCTV를 대체하고 있다.

4) 프라이버시 인터내셔널의 자료에 의하면 영국의 경우 1년 동안 CCTV 감시에 소요되는 비용은 약 3000만 달러에 달한다고 하며, 런던의 경우 약 30만개의 CCTV가 설치된 것으로 추산된다고 한다(www.privacyinternational.org).

5) 디지털 방식의 DVR시스템과 아날로그 방식의 CCTV의 비교

영기능 등이 포함되어 있다[6]. 최근 경찰은 방범 목적으로 주택가에 CCTV를 설치할 계획[7]임을 밝히기도 했다.

---

6)DVR 시스템을 이용한 감시와 검색

(2) 거래기록의 저장 · 인터넷 이용기록의 저장

전자상거래나 신용카드, 전자화폐의 발달에 따라 대부분의 거래기록이 전산처리되어 저장되고 있다. 거래정보를 분석해보면 모든 활동이 추적될 수 있고, 그 사람의 습관, 사상까지도 파악할 수 있다. 그리고 인터넷의 발달로 정치, 경제, 사회, 문화적으로 다양한 활동이 인터넷을 통하여 이루어지게 되는데, 이러한 인터넷에서의 모든 활동은 로그기록, 쿠키 등의 형태로 기록으로 남게 된다. 인터넷을 통해서 수집되는 정보는 사용자의 위치를 파악할 수 있는 인터넷 프로토콜 주소(Internet Protocol Address, 흔히 IP 주소라고 부른다), 웹사이트의 접속시간, 접속한 페이지와 다운로드한 내용들과 이미지들, 사용자가 현재 페이지로 들어오기 전 머물렀던 페이지, 사용자가 입력한 데이터들), 쿠키 파일(쿠키란 웹사이트에서 사용자의 하드 드라이브에 직접 써 넣는 작은 텍스트 파일들이다. 쿠키는 원래 사용자들이 비밀번호나 아이디 등을 일일이 재입력을 하지 않고도 웹사이트를 이용할 수 있도록 비밀번호나 아이디를 저장해 두는 작은 파일인데, 쿠키를 통해서 웹사이트는 이용자의 정보를 은밀하게 수집할 수 있게 된다. 쿠키에는 사용자의 로그인 정보나 각종 등록정보, 온라인 쇼핑 구매내역을 비롯한 소비 패턴들에 관한 정보, 사용자가 최종적으로 어느 사이트를 통해서 본 사이트에 오게 되었는지에 대한 직전 웹사이트 서핑 정보 등이 저장된다) 등이 있다.[8] 이와 같은 저장성의 증대는 곧 발전한 검색기술과 데이터 마이닝 기술[9]과 결합하여 개인

---

7) 문화일보2002년 10월21일

8) http://www.cookiecentral.com/news.phtml

9) 데이터마이닝이란? (자료 : 포항공과대학 정보통신연구소; http://iislab.postech.ac.kr/)
데이터마이닝은 데이터에 잠재적으로 내재된 경향성을 파악하는 방법론으로 대표적인 활용사례를 들어보면 다음과 같다.
① BC 카드사의 카드 도용사고 방지
1,600만명의 고객과 70만명의 가맹점을 가진 BC 카드에서 매일 평균 20만건의 결제 승인 요청중에서 0.1% 가량이 카드 도용에 의한 사고이다. 이로 인한 배상액이 연간 150억원에 달하는데 이러한 사고를 미리 예측하고 조기에 분실이나 도난을 검색하는 시스템을 개발하여 상당한 효과를 보았다. 여기서는 SAS와 Enterprise Miner를 이용한 마이닝 기법으로 해결하였다.
② 마이크로소프트의 DM 발송
연간 4,000만건의 DM을 발송하는 마이크로소프트는 여기에만 약 4,000만 달러의 경비를 지출했으나 이를 고객의 구매이력 데이터를 이용하여 구매 패턴을 파악하여 구매 가능 고객에게만 발송하도록 하였다. 이로 인해 DM 매출은 현상유지 하면서 DM 발송비용은 35% 절감하였다.
③ 통신시장의 고객 이탈방지
통신 사업자들이 자기 회사 고객이 다른 사업자로 이탈하는 현상을 막기 위해 고객 데이터로부터 적절한 모델을 개발하고 데이터마이닝을 수행하여 고객 이탈의 패턴을 추출한다. 이 패턴을 바탕으로 잠재적인 이탈 가능 고객을 특별 관리하여 이탈율을 낮추었다.
④ LTV 의 결함률 조정

의 활동내역의 추적을 가능하게 한다.

(3) 생체인식 기술의 발달

지문인식, 홍채인식, 얼굴인식, 정맥인식 등 생체인식기술이 발달하면서 이러한 생체인식기술이 개인의 동일성을 확인하는 수단으로 많이 이용되고 있다.[10] 이러한 생체인식기술은 위조가 어렵고 도난가능성이 낮기 때문에 위조의 가능성과 도난당할 가능성이 있는 신분증의 대용으로 프라이버시를 보호할 수 있는 본인확인 수단으로 각광을 받고 있다. 그런데 지문이나 홍채나 정맥 등과 같은 생체정보는 각 개개인에게 고유한 정보이기 때문에 마치 주민등록번호처럼 그 개인의 고유의 식별자 역할을 하게 되므로 생체정보가 각 개개인의 정보를 담은 데이터베이스와 연동될 경우 프라이버시 침해의 가능성이 매우 높아진다는 문제점이 있다. 또한 이러한 생체정보 중에는 홍채에 관한 정보나 얼굴정보와 같이 상대방의 동의를 받지 않고, 상대방 몰래 수집할 수 있는 것들도 있어서 프라이버시가 침해될 가능성이 크다.

한편 최근에는 기술이 급속도로 발달하여 예컨대 얼굴인식(형체인식) 기술의 경우, 멀지 않아 CCTV에 촬영된 수십만명의 사람 가운데에서 순식간에 동일인을 식별해 낼 수도 있게 될 것이라고 한다. 2001. 에는 미국 FBI가 플로리다 Tempa의 Raymond James Stadium에서 있었던 2001년도 수퍼보울 결승전에 참가한 관람객들을 출입구에 설치된 카메라로 몰래 촬영한 사실이 밝혀지기도 하였다. FBI는 이 사진들을 디지털화하여 수배자들의 얼굴사진과 비교 분석을 하였다고 한다[11]. 그리고 미국의 경우 9·11 사태 이후 많은 공항들에서 테러방지라는 명목으로 얼굴인식 시스템을 도입하고 있다.

미국에서 세번째의 철강 메이커인 LTV 에서는 96년 기준으로 40억불의 매출을 올리고 있다. 이 회사는 데이터마이닝 기법을 이용해서 결함 허용도를 3~5% 이던 기존에 비해 0.03~0.05% 정도로 줄여서 제품의 질과 고객 서비스를 향상시켰고, 이로 인해 매년 1,000 만불의 비용을 절감하고 있다. 이 회사에서는 동쪽의 공장에서 생산된 코일의 색상이 잘 변색되는 문제가 있어서 서쪽 공장의 2~3% 불량률에 비해 월등히 높은 7~8% 의 불량률이 생겼는데, 이를 생산 데이터를 바탕으로 한 데이터마이닝 수행을 통해 용광로 재건설 주기와 불량률 사이의 연관성을 밝혀냈다. 이 결과로 매년 1,680만불의 비용을 절감하고 있다.

이 외에도 수많은 적용사례가 있으나 이러한 것들이 기업 경쟁력의 핵심에 해당하여 기밀처럼 다루어 지기 때문에 외부에 공개된 것들은 많지 않다고 한다.

10) 현재 지문, 홍채, 정맥 등의 생체인식기술을 활용하여 출입통제시스템 등에 활용하고 있다.

11) Feds use biometrics against Super Bowl fans. Thomas C Greene, 2001. 1. 2. The Registar

12)

(4) 위치추적 기술의 발달

GPS를 이용하거나, 휴대전화의 발신위치 추적방법을 이용하거나, 인터넷 프로토콜(IP)의 추적을 통한 방법 등 각종 위치추적기술[13]도 비약적으로 발전하고 있다.[14] 오늘날 위치추적은 배송, 물류서비스, 교통서비스, 자동항법서비스, 각종 광고서비스 등에 활발히 사용되고 있다. 교통수단의 위치, 속도 등을 확인할 수 있으며, A/S 요청이 들어올 때에도 가장 가까운 곳에 있는 A/S 요원을 GPS를 통하여 파악한 후 고객의 요구를 전달할 수 있다. 이 분야는 산업적으로 이용분야가 많기 때문에 산업계의 이해도 매우 크다[15]. 위치정보는 그 사람의 행동의 궤적이기 때문에 매우 민감한 개인정보에 해당하므로 더욱 더 가중된 보호가 필요하다.

나. 감시활동의 확대

12) Boston의 Logan 공항, Oakland 국제공항, T.F. Green 공항, Fresno Yosemite 국제공항 등이 도입을 하거나 할 예정인 것으로 알려져 있다(CNet 뉴스, Can face recognition keep airports safe? Stefanie Olsen, Robert Lemos, 2001. 11. 1. http://news.com.com/2100-1023-275313.html?legacy=cnet&tag=tp_pr)
그러나 오작동의 가능성을 들어 도입을 폐기한 공항도 있다.

13) 이동전화의 이용기록이나 교통카드의 이용기록 등을 활용하여 위치를 파악하는 것도 넓은 의미에서는 위치정보에 포함될 것이다.

14)GPS를 이용한 위치추적의 원리

15) 위치추적의 응용분야, 화물차량(화물차량의 위치, 속도, 이동경로 등을 파악), 택시(택시의 위치, 속도, 이동경로 파악), 버스(교통상황, 운행위치, 운행간격 등, 최근 서울시에서 도입예정이라고 함), 애프터 서비스 요원의 위치, 이동경로 파악, 그 외에도 최근에는 일반직원들에 대해서도 위치추적 시스템을 통해 감시하는 일이 많아지고 있다고 한다.

(1) 국가의 감시활동

국가 활동의 기초는 국민에 대한 자료의 수집으로부터 시작된다고 해도 과언이 아닐 것이다. 국가의 주요 활동인 조세의 부과 및 징수를 통한 재원의 확보, 이를 기초로 한 국방과 국가안보 유지, 사법 및 치안과 질서유지, 교육 · 문화 · 보건 · 의료 · 사회보장 등의 복지활동이 국가의 주요활동인데, 이 활동들은 국민으로부터 수집하는 각종 정보에 의존하고 있다. 최근에는 감시기술의 발달로 이러한 국가의 감시활동에도 질적 변화가 이루어지고 있다.

그 첫 번째가 국가통합전산망의 구축이다. 최근 국가는 국민들로부터 수집한 정보와 국가가 자체적으로 수집한 정보를 전산화하여 각각의 영역별로 구축해 온 전산망을 하나로 통합하고 있다. 전자정부 구현이라는 이름 아래 추진되는 이 작업은 행정의 투명성, 효율성, 국민에 대한 서비스의 강화라는 명목으로 전국민의 정보를 하나의 시스템으로 통합하여 관리하는 것을 목적으로 하고 있는데, 이러한 시스템의 통합은 국가의 국민에 대한 감시활동의 수준을 한 단계 높이게 될 것이다.

두 번째로 끊임없이 시도되는 전자주민카드와 같은 통합 신분확인 시스템의 구축시도이다. 우리나라의 경우 전자주민카드의 도입시도는 국민의 반대에 부딛혀 좌절되었지만, 전자건강보험증이니 전자공무원증이니 하는 다양한 이름으로 각 부문에서 끊임없이 도입이 시도되고 있다.

세 번째는 새로운 감시기술을 활용한 도청이나 검열, 위치추적 등의 활동의 강화이다. 국제적으로도 9 · 11 사태를 기점으로 국가의 국민에 대한 감시활동은 엄청나게 늘어나고 있으며, 이는 민주주의와 인권에 대한 중대한 위협으로 작용하고 있다.

(2) 민간기업의 소비자에 대한 감시의 확대

민간기업은 소비자나 잠재적 소비자에 대하여 상품을 판매하기 위하여 이

들을 끊임없이 감시한다. 직접 서비스를 제공하면서 소비자의 동의를 얻어 감시를 하기도 하고, 불법적으로 감시를 하기도 하고, 적법하게 또는 불법적으로 수집된 정보를 불법적으로 사기도 한다. 민간기업에게는 엄청난 이윤동기가 있고, 소비자를 감시할 수 있는 수단이 획기적으로 발달하였기 때문에(예를 들면 인터넷을 통한 소비자의 모든 활동내용의 파악, 신용카드를 통한 소비자의 모든 소비내용을 파악, 소비자의 모든 통신이용상황과 위치정보를 파악), 민간기업에 의한 소비자의 감시가 소비자의 프라이버시와 인권을 침해할 가능성이 높다.

(3) 직장에서의 노동감시

노사관계에 있어서도 감시기술의 발달은 새로운 문제를 야기하고 있다. 사용자는 저렴해지고 보다 은밀해진 노동감시기술을 활용하여 노동자에 대한 통제를 강화하려고 한다. 스마트 카드, 위치확인 시스템, CCTV, 전사적자원관리시스템, 전자우편 · 컴퓨터 사용 감시시스템 등이 최근 새롭게 도입되고 있는 감시수단이다.

다. 최근의 감시기술과 감시활동의 특징

(1) 은밀성 · 원격성 · 대량성

최근에는 감시당하는 사람이 알지 못하는 사이에 은밀하게 감시가 이루어진다. 예컨대 전자우편이나 메신저, 인터넷 이용현황에 대한 감시나 컴퓨터 이용현황 감시는 감시당하는 사람이 알아채지 못하는 사이에 은밀하게 이루어진다. 원격감시가 가능해졌다는 것도 최근의 감시기술의 발달에 따른 새로운 특징이다. 인공위성을 이용한 감시도 최근에는 정확도가 매우 높아졌다. 감시가 매우 짧은 시간에 대량적으로 이루어지게 된 것도 최근의 감시기술의 발달에 따른 새로운 양상이다. 그래서 감시의 범위에 있어서도 동시에 전세계의 거의 대다수의 통신을 감청하는 것도 가능해진 것이다.

이러한 감시기술의 발전양상은 과거처럼 감시행위에 대하여 영장주의라는

법원의 통제만으로는 실효성있게 대응할 수 없다는 것을 보여준다. 즉, 과거에는 감시행위가 눈에 보이고, 감시행위에 인적, 물적인 한계 때문에 법원의 관여가 어느 정도 효과가 있었지만, 최근에는 은밀하고, 원격적으로 동시에 대량감시가 가능하므로 얼마든지 법원의 통제를 벗어나 법원 몰래 감시를 하는 것이 가능해진 것이다. 법원의 영장을 통한 관여 외에 새로운 통제 시스템이 필요하다.

(2) 초정밀 감시

과거에는 감시를 통해 얻을 수 있는 정보의 내용이 한정되어 있었는데, 최근에는 감시를 통해 얻을 수 있는 정보가 거의 무제한적으로 늘어나고 있다. 감시의 양과 질이 과거와는 비할 수 없을 정도로 월등하게 많아지고, 높아진 것이다. 최근 발달하고 있는 데이터마이닝 기법은 감시로 수집한 정보를 수집자의 필요에 따라 다양하게 가공해 준다. 최근에는 마음만 먹으면 한 사람의 일거수 일투족은 물론 사상이나 성향까지도 알아낼 수 있게 되었다. 예컨대 한 사람에 대하여 인터넷의 로그기록, 인터넷 상에서 그가 행한 행위에 대한 분석, 위치정보의 파악에 의한 이동상황에 대한 분석, 신용카드 사용상황 분석을 할 경우 그 사람의 거의 모든 행위를 파악할 수 있다. 이와 같이 수집된 정보를 다양한 방법으로 분석하면 본인보다도 더 정확하게 본인의 생활습관이나 사고방식, 성향을 알아낼 수 있는 것이다.

이것은 감시가 단순한 프라이버시 침해의 문제에서 이제는 사상, 양심, 표현의 자유의 침해 문제로 발전하게 되었다는 것을 보여준다.

그리고 최근에는 발달한 생체인식기술과 유전자 분석기법을 동원하여 한 사람의 과거와 미래를 추측하고 있다. 한 사람의 과거와 현재의 병력이나, 유전자 검사결과를 토대로 감시자가 그 사람의 미래의 모습을 추측하는 것이다. 물론 이러한 과거와 미래의 추측이 어느 정도의 과학적 타당성을 지니고 있는지는 아직도 논란의 대상이 되고 있다. 그러나 이것은 감시가 새로운 차별의 수단으로 되고 있다는 것을 상징적으로 보여주고 있는 사례이다.

(3) 보편적인 감시사회

오늘날은 대상을 불문하고 보편적인 감시가 가능해졌고, 실제로 보편적인 감시가 행해지고 있다. 이것은 우리 인류가 처음으로 경험하는 상황이다. 보편적인 감시가 행해지게 된 이유는 여러 가지가 있겠지만, 정보의 저장성을 갖는 정보통신기술이 발달한 점, 원격거래의 증가로 인해 거래정보를 집적할 필요가 커진 점, 효율성을 추구하고 편리함을 제공하기 위해 정보를 수집할 필요가 커진 점, 통제를 위해 감시를 할 필요가 커진 점 등이 그 이유로 될 수 있다. 현대사회에서 감시는 가장 핵심적인 사회현상 중의 하나가 된 것이다. 이처럼 감시가 일상화되고, 정치화하고 강화된 현대사회를 '감시사회'라고 볼 수 있을 것이다.

2. 감시의 동기

감시기술이 발전하기 때문에 감시가 늘어나고 있는 것이기는 하지만, 감시기술의 발전을 추동하는 것은 근본적으로는 사회적 요인이다. 오늘날 감시가 비약적으로 증가하고 일상화 되고 있는 이유는 감시가 다음과 같은 효용을 갖고 있기 때문이다.

가. 감시의 경제적 효용

(1) 계획 수립의 기초

감시는 계획수립의 기초가 된다. 감시자는 자신이 추구하는 목적에 합당한 계획을 수립하기 위하여 감시를 통하여 정보를 수집한다. 감시를 통하여 획득한 정보를 이용하여 감시자는 보다 정확한 판단을 내릴 수 있는 것이다. 합리적인 판단을 위해서는 보다 많은 정보가 필요하며, 정보의 수집과정에서 합리적인 판단을 위하여 필요하다는 명분으로 감시가 정당화된다. 근래에는 감시를 통하여 획득한 정보 자체가 상품으로 판매되기도 한다.

(2) 평가의 기초

감시는 평가의 기초가 된다. 평가의 공정을 위해서 보다 많은 정보가 필요하고, 따라서 감시는 공정한 평가를 위해서 불가피하다는 논리로 감시를 합리화하기도 한다.

(3) 혜택의 배분 - 감시의 유인수단

감시의 강화는 감시자에게 경제적 효용을 가져다 줄 수도 있다. 감시자는 그 경제적 효용을 피감시자에게 부여하는 혜택을 통하여 피감시자와 감시자 사이에 분배하기도 한다. 흔히 감시자들은 감시를 하면서 피감시자들에게 그 감시행위의 결과 피감시자의 사회적, 개인적 효용이 늘어날 것이라고 하면서, 피감시자들에게 혜택을 주고 회유를 한다. 이것이 새롭게 감시수단을 도입할 때 사용하는 가장 전형적인 방법이다.

나. 통제수단

감시는 유용한 통제수단이 된다. 직접적으로는 감시는 피감시자의 불법행위나 일탈행위 또는 감시자가 원하지 않는 행위를 적발해 내거나, 감시를 통해 피감시자의 행위결과를 수집하여 이를 평가하여 피감시자를 통제하는 수단으로 삼는다. 나아가 감시는 피감시자에게 스스로 감시자에 대한 복종을 내면화하도록 한다.

3. 감시의 문제점

가. 기본권의 침해

감시의 가장 큰 문제점은 감시행위가 감시받는 자의 기본권을 침해한다는 데 있다. 특히 최근의 발달한 감시기술은 감시받는 사람의 일거수 일투족을 모두 감시할 수 있게 됨으로써, 프라이버시 침해를 넘어서서 그 사람의 행동과 사상까지도 파악할 수 있게 한다. 감시행위로 인하여 감시받는 사람은 프라이버시와 인격권은 물론 표현의 자유, 행동의 자유, 사상의 자유까지도 침해받게 된다. 그래서 오늘날 감시는 민주주의와 인권에 대한 가장 중대한 침

해요소로 되어 가고 있다.

나. 민주주의의 왜곡과 종속의 심화

감시행위로 인하여 감시받는 사람의 표현의 자유, 행동의 자유, 사상의 자유가 침해되고 이로 인하여 민주주의는 억압되고 왜곡된다.

또한 감시행위를 통하여 수집한 정보에 의존한 계획의 수립, 관리와 통제, 평가를 할 경우 그 과정에서 감시자의 주관에 의한 범주화가 이루어지게 되는데 이때 국민과 소비자, 노동자의 의사, 즉 민주주의가 왜곡되기 쉽다.

특히 대등한 권력관계에 있지 않은 집단 사이에서 우월한 권력관계에 있는 집단은 앞선 감시기술을 이용하여 다른 집단에 대한 지배력을 강화할 수 있다. 예를 들어 기업의 소비자에 대한 감시, 국가(관료집단이나 지배집단)의 국민에 대한 감시, 사용자의 노동자에 대한 감시 등은 우월한 집단의 지배력을 강화시켜주는 수단으로 사용될 수 있는 사례들이다.

다. 차별과 배제

감시행위로 인하여 수집한 정보를 데이터베이스화하여 이를 관리와 통제의 수단으로 삼을 경우, 국민과 소비자, 노동자는 데이터베이스에 의하여 범주화되고, 이러한 데이터베이스를 통한 관리와 통제는 정보주체를 하나의 주체로서가 아니라 고정된 객체로서 낙인을 찍는 결과를 낳는다. 이와 같이 인간이 객체화되면서 감시는 인간에 대한 차별과 배제의 도구가 된다. 수집된 데이터가 역으로 차별의 도구가 되는 것이다.

Ⅱ. 제3세대 프라이버시권으로서의 반감시권의 정립의 필요성

1. 제1세대 프라이버시권

프라이버시권은 동서고금을 막론하고 일반적으로 인정되어 오던 개인의 권리였다고 한다. 코오란[16]에도 모하메드의 말씀[17] 속에 프라이버시에 대한 언

급이 나온다고 하고, 성경[18][19]과 고대 그리스와 중국의 고대 철학에서도 프라이버시권이 인정되었다고 한다[20]. .법으로 인정된 것으로는 1361년의 영국의 평화 정의법(the Justice of Peace Act)이 있다고 한다. 이 법은 몰래 훔쳐보는 것과 몰래 엿듣는 것을 범죄화했다[21]. 영국의 국회의원인 윌리엄 피트(William Pitt)는 "가난한 자의 집은 약할 수 있다. 그의 집은 지붕이 흔들릴 수 있고, 집안으로 바람이 들이치거나, 폭풍우가 들이닥치거나, 비가 새들어올 수도 있다. 그렇지만 영국의 왕은 그의 집 안으로 들어갈 수 없다; 왕이 지닌 모든 힘들은 낡은 그의 집의 문을 감히 넘어설 수 없다"[22]고 했다.

1776년 스웨덴은 정부의 모든 정보들이 합법적인 용도로만 사용되어야 한다는 공중기록에 대한 접근에 관한 법률(Access to Public Records Act)을 제정하였다. 프랑스는 1858년에 사적인 사실의 출간을 금지했고 위반자에게는 엄한 벌금을 부과하였다.[23] 노르웨이는 1889년에 "개인 혹은 가정의 문제"와 관련된 정보의 누설을 금지하였다.[24]

1890년 미국에서는 사무엘 워렌(Samuel Warren)과 루이스 브랜다이스(Louis Brandeis)는 프라이버시를 "홀로 있을 권리"[25]로 묘사하면서, 불법행위로서의 프라이버시 권리의 침해에 관한 최초의 글을 썼다. 이 논문의 출판 이후 미국에서는 프라이버시 침해로 인한 불법행위라는 개념이 점차 확립되게 되었다.

국제적으로도 1948년의 세계 인권 선언문에서 프라이버시 보호 원칙이 천명되었고[26] 유엔에서도 인권선언에서 프라이버시를 보편적 인권으로 선언하

16) an-Noor 24:27-28 (Yusufali); al-Hujraat 49:11-12 (Yusufali).
17) Volume 1, Book 10, Number 509 (Sahih Bukhari); Book 020, Number 4277 (Sahih Muslim); Book 31, Number 4003 (Sunan Abu Dawud)
18) Richard Hixson, Privacy in a Public Society: human Rights in Conflict 3 (1987). Barrington Moore, Privacy: Studies in Social and Cultural History (1984)도 참조하시오.
19) See Jeffrey Rosen, The Unwanted Gaze (Random House 2000).
20) Id. at 5.
21) James Michael, supra n. 1, at. 15. Justices of the Peace Act, 1361 (Eng.), 34 Edw. 3, c. 1.
22) Speech on the Excise Bill, 1763.
23) The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris, 68 Tulane Law Review 1219 (May 1994).
24) Prof. Dr. Juris Jon Bing의 Data Protection in Norway, 1996(http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html)를 보시오.
25) Warren and Brandeis, supra n.4.

였고[27] 시민적 및 정치적 권리에 관한 국제규약(the International Covenant on Civil and Political Rights, ICCPR), 의 17조[28], 이주 노동자들에 관한 UN 협정(UN Convention on Migrant Workers)의 14조[29], 아동 보호에 관한 UN 협정(UN Convention on Protection of the Child) 16조[30], 인권과 기본적 자유에 대한 1950년 유럽 협약(the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950)[31]의 제8조도 이를 명시하고 있다.

애초에 이 권리는 i) 사생활 공간의 침해 금지, ii) 난처한 사적인 일의 공표 금지, iii) 오해를 낳는 표현의 금지, iv) 성명이나 초상의 영리적 사용의 금지 등을 내용으로 하는 것으로 해석되었다. 이것은 주로 개인간의 사적인 영역에서 프라이버시의 침해가 문제가 되었던 시절에 맞는 것이었다. 이때에는 이와 같이 개인의 프라이버시 침해를 보호함으로써 족했었는데, 이를 제1세대 프라이버시권이라고 부를 수 있을 것이다.

2. 제2세대 프라이버시권

(1) 1980년의 OECD 이사회 권고안

1980년 OECD(Organization for Economic Cooperation and Development)는 '프라이버시보호와 개인정보의 국제유통에 관한 가이드라인'이라는 이사

---

26) Universal Declaration of Human Rights, adopted and proclaimed by Genenral Assembly resolution 217 A (III) of December 10, 1948, <http://www.un.org/Overview/rights.html>에서 볼 수 있음.

27) See generally, Marc Rotenberg, ed., The Privacy Law Sourcebook: United States Law, International Law and Recent Develpments (EPIC 2001).

28) International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976, available at <http://www.unhchr.ch/html/menu3/b/a_ccpr.htm>

29) International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by Genenral Assembly resolution 45/158 of December 18, 1990, available at <http://www.unchr.ch/html/menu3/b/m_mwctoc.htm>

30) Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990, available at <http://www.unhchr.ch/html/menu3/b/k2crc.htm>

31) Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005) open for signature November 4, 1950, entry into force September 3, 1950, available at <http://conventions.coe.int/Treaty/EN/cadreprincipal.htm>.

회 권고안을 채택하였다. 이 가이드라인은 국가나 민간에 의하여 개인정보가 수집, 이용되고 있는 상황에서 개인정보의 수집, 이용에 따른 정보주체의 권리를 보호하기 위한 원칙들을 정식화한 것이다. 이 가이드라인은 그 후 유럽연합의 개인정보 보호에 관한 지침(1981)[32], 유럽 각국을 비롯하여 전 세계 여러 나라와 우리나라의 프라이버시 보호입법의 모델이 되어 왔다[33].

(2) 독일연방헌법재판소의 개인정보자기결정권

한편 독일에서는 1983년 독일의 연방헌법재판소에서 자신의 개인정보에 대한 결정권은 정보주체에게 있어야 한다는 '개인정보에 대한 자기결정권'을 헌법상의 권리라고 판시하여 이러한 개인정보에 대한 권리를 헌법상의 근거를 가진 권리로 자리매김하였다[34].

(3) 개인정보에 대한 정보주체의 권리의 내용

이러한 개인정보에 대한 정보주체의 권리는 이전의 프라이버시 권리가 고립된 개인의 사생활의 보호라는 소극적 측면의 권리였던 데 반해, 개인에 대한 정보의 유통이 활발해진 상황에서 자기를 보호할 수 있는 적극적인 권리라는 특징을 갖는다. 이를 제2세대의 프라이버시권으로 볼 수 있다. 그 구체적인 내용은 다소간의 차이는 있을 수 있지만 다음의 OECD의 1980년의 권고안의 내용을 기초로 하고 있다.

1) 수집제한의 원칙

모든 개인정보는 적법하고, 공정한 수단에 의해 수집되어야 하며, 정보주체에게 알리거나 동의를 얻은 후 수집되어야 한다.

2) 정보내용정확성의 원칙

---

32) The European Union Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data"
33) 우리나라의 경우 정보통신망이용촉진 및 정보보호에 관한 법률을 들 수 있다.
34) BVerfGE 65, 1

개인정보는 그 이용목적에 부합하는 것이어야 하고, 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태로 유지하여야 한다.

3) 목적 명확화의 원칙

개인정보를 수집할때는 목적이 명확해야 하고, 이를 이용할 경우에도 애초의 목적과 모순되지 않아야 한다.

4) 이용제한의 원칙

개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화된 목적 이외의 용도로 공개되거나 이용되어서는 안된다.

5) 안정성 확보의 원칙

개인정보의 분실, 불법적인 접근, 파괴, 사용, 수정, 공개위험에 대비하여 합리적인 안전보호장치를 마련해야 한다.

6) 공개의 원칙

개인정보에 관한 개발, 운용 및 정책에 관해서는 일반적인 공개정책을 취하여야 한다. 개인정보의 존재, 성질 및 주요이용목적과 함께 정보관리자의 신원, 주소를 쉽게 알 수 있는 방법이 마련되어야 한다.

7) 개인참가의 원칙

정보주체인 개인은 자신과 관련된 정보의 존재확인, 열람요구, 이의제기 및 정정·삭제·보완 청구권을 가진다.

8) 책임의 원칙

개인정보 관리자는 위에서 제시한 원칙들이 지켜지도록 필요한 제반조치를

위해야 한다.

3. 제3세대 프라이버시권으로서 반감시권의 정립 필요성

오늘날 비약적인 감시기술의 발달에 따라 국가 및 기업은 매우 저렴한 비용으로, 대규모적이고 신속하게 개인에 대하여 체계적인 정보를 수집, 관리할 수 있게 되었다. 이를 통해서 감시자는 개인의 모든 거래행위는 물론 의사소통행위와 생각까지도 분석, 감시할 수 있게 되었고, 심지어는 유전자 검사를 통하여 개인의 현재 뿐만 아니라 과거와 미래까지도 분석할 수 있게 되었다. 이에 따라 감시의 문제는 프라이버시권이나 개인정보의 자기결정권으로는 해결할 수 없는 새로운 국면의 문제가 되어가고 있다.

오늘날의 이와 같은 고도의 감시에 의하여 야기되고 있는 문제들에 대응하기 위해서 제3세대 프라이버시권이라고 부를 수 있는 보다 고양된 권리인 '반감시권'이 정립되어야 한다. 반감시권은 다음과 같은 점에서 기존의 프라이버시권이나 개인정보의 자기결정권과는 다른 내용을 가져야 한다.

가. 반감시권의 구체적인 내용과 OECD 8원칙의 수정

(가) 민주주의와 인권보장의 핵심적 권리 : 국가는 반감시권이 민주주의와 인권보장의 핵심적 권리이며, 보장의 척도임을 확인하여야 한다

반감시권은 감시가 민주주의와 인권에 대한 근본적 위협이라는 문제의식에서 출발한다. 오늘날 감시는 단순한 프라이버시 침해나 인격권의 침해와는 근본적으로 다른 양상을 보이고 있다. 오늘날 감시는 시민의 인격권, 행동의 자유, 학문사상의 자유, 양심의 자유, 종교의 자유, 언론, 출판의 자유, 표현의 자유, 정치활동의 자유와 같은 기본권의 핵심적 영역들을 위협하고, 민주주의를 위협하고 있다. 이제 현대사회에서 감시에 대한 대응은 민주주의와 인권보장의 핵심문제가 된 것이다. 반감시권은 프라이버시의 문제에서 권력통제의 문제로 문제의 초점을 이동시키고 있다.

(나) 독립기구에 의한 보호의 원칙 : 반드시 국가로부터 독립성을 가진 기구에 의하여 감시행위로부터 개인들이 보호되어야 한다

(i) 감시는 민주주의와 인권을 침해하는 행위이며, 반감시권의 문제는 권력통제의 문제이기 때문에 반감시권이 보장되기 위해서는 국가와 민간영역에서 민주주의와 인권을 위협하는 모든 감시행위에 대하여 민주주의, 권력분립, 기본권 보장의 원리에 입각하여 이를 통제할 수 있는 위상을 가지고, 효과적으로 기능을 수행할 수 있는 국가로부터 독립성을 가진 기구에 의하여 개인들을 감시로부터 보호할 수 있도록 제도적 장치를 마련하는 것이 필수적이다.

(ii) 이런 취지에서 유럽연합에서도 개인정보의 처리와 보호에 관한 지침(Directive 95/46/EC)[35]의 제28조에서 개인정보처리과정에서의 개인정보보호 감독기관에 대한 규정을 두고, 모든 국가는 국내에 개인정보 보호에 관한 유럽연합의 지침의 준수사항을 조사할 감독기관을 두어야 하며, 그 기관은 완전한 독립성을 가지고 운영될 수 있어야 한다고 하고 있다. 그리고 각국은 개인정보의 처리에 관하여 개인의 자유나 권리의 보호에 대한 새로운 행정적 수단이나 법률의 규정이 도입될 때 그러한 독립적인 개인정보 보호기관의 의견을 듣도록 해야 하며, 그 독립기관은 감독업무를 수행하는데 필요한 수사권을 가져야 하고, 개인정보 침해를 막을 수 있는 적절한 권한이 주어여야 하고. 의견을 공표할 수 있어야 하고, 개인정보 침해를 막을 수 있는 힘과 그러한 데이터의 삭제나 임시적인 중지나 제한적인 금지를 할 권한, 주의를 주거나 그 문제를 의회나 다른 정치적 기관에 제기할 권한, 소송을 제기할 권한, 정기적으로 활동에 대한 보고서를 작성, 공표할 권한을 가지고 있어야 한다고 규정하고 있다.

(iii) 감시기술의 발달은 기존의 법원에 의한 감시활동에 대한 통제제도를 무력하게 한다. 감시가 은밀하게 행해질 수 있고, 대규모적으로 행해질 수

35) DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

있고, 감시의 흔적이 남지 않고, 끊임없이 새로운 감시기술이 개발되고 있는 오늘날에 있어서는 법원의 영장에 의한 통제만으로는 부족하다. 사법부에 의한 통제 외의 또 다른 통제가 보완되어야 한다. 그 역할은 독립적인 제3기관과 국회가 담당할 수 있을 것이다.

(다) 보호대상의 개방성의 원칙 : 행동과 사상의 자유를 제약하는 모든 감시로부터 개인들을 보호하여야 한다

반감시권에 의하여 보호되는 대상은 개인의 프라이버시나 개인정보[36]로 국한되어서는 안된다. 반감시권은 개인의 프라이버시나 개인정보를 넘어, 개인과 집단의 사상과 행동의 자유를 제한하는 모든 행위를 통제의 대상으로 삼아야 한다. 과거에는 개인의 사생활의 보호나 개인정보의 보호가 문제되었으므로 보호법익이나 보호의 객체는 개인이었고, 보호의 대상도 개인이 식별되는지 여부에 맞추어져 있었다. 그러나 감시기술의 발달로 이제 감시는 개인에 대한 프라이버시의 침해나 정보 수집의 문제만이 아니라 민주적 참여를 배제하는 집단에 대한 차별과 배제의 문제로 확대되고 있다[37]. 따라서 이제 보호의 객체를 개인으로 국한시키지 말고, 보호의 대상도 개인이 식별되는지 여부에 맞추어서는 안될 것이다. 단체나 집단이나 개인의 식별여부를 불문하고 생각과 행동에 대한 통제가 가해지는 모든 행위, 계획, 제도를 감시행위로 보고 이에 대응하여 적절한 보호가 이루어져야 한다. 그리고 감시기술의 발달로 인하여 새로운 감시행위의 유형들이 끊임없이 생겨나고 있다. 따라서 감시행위의 유형에 구애받지 않고 모든 감시행위를 규제할 수 있는 개방적인 보호제도가 도입되어야 한다.

(라) 동의의 원칙에서 민주주의와 인권보장의 원칙으로 : 개인정보 수집시에 고지 또는 동의를 얻었는지 여부를 기준으로 보는 것에서 민주주의

---

36) 정보통신망 이용촉진 및 정보보호에 관한 법률 제2조 제1항 제6호
"개인정보"라 함은 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

37) 예컨대 데이터베이스를 통한 인권차별 행위의 예를 들 수 있다.

와 인권보장에 장애가 되는지 여부를 판단기준으로 삼아야 한다.

개인정보 수집시의 고지나 동의를 전제로 한 개인정보의 보호원칙은 개인이 대등한 지위에서 개인정보를 처분할 수 있다는 것을 전제로 한 것이다. 그러나 현대사회에서의 감시는 ① 고지나 동의의 과정을 거치지 않고도 얼마든지 이루어질 수 있으며, ② 끊임없는 신기술의 발달은 고지나 동의시에 의도했던 것과는 다른 새로운 감시의 효과를 낳고 있으며, ③ 오늘날 시민들은 국가나 기업의 정보수집이나 감시에 동의하지 않고는 경제활동을 할 수 없게 불평등한 구조에 편입되어 있다. 따라서 이러한 현실을 반영하여 계약적 사고에서 벗어나 침해의 효과를 기준으로 하고, 기본권 보호의 관점에서 감시에 대응할 수 있는 새로운 원칙이 모색되고 정립되어야 한다. 즉, 개인정보보호에 관한 OECD의 원칙이 새로운 상황에 맞추어 수정되어야 하는 것이다.

(마) 정책참여의 원칙 : 감시계획의 수립단계부터 참여하고 통제할 권리가 보장되어야 한다

현대사회의 감시기술의 발달에 비추어 볼 때, 감시계획의 수립은 생각과 행동에 대한 통제의 계획으로 작용한다. 예컨대 국가의 행정작용의 내용으로서 어떤 개인정보를 수집할 것인지, 개인과 집단의 행동을 어떻게 추적하고 기록할 것인지에 대한 계획(예를 들어 주민등록제도나 국가기간전산망)은 개인과 집단의 생각과 행동에 대한 통제의 청사진이 된다. 따라서 시민은 이 과정에 참여하고 통제할 수 있어야 한다. 그리고 기업이나 민간영역의 모든 감시계획의 수립에도 참여하고 개입할 수 있어야 한다(신용카드 회사의 데이터베이스, 병원이나 대학의 데이터베이스, 기업의 인사관리 데이터베이스나 ERP 등). 모든 것이 기록되고 저장되고 분류되는 데이터베이스 사회에서 민주주의와 인권에 영향을 줄 수 있는 기록, 저장, 분류에 시민과 노동자가 개입할 수 있어야 하는 것이다.

(바) 민간영역과 공공영역의 보호의 원칙 : 국가의 감시활동 이외에 민간의 감시활동에 대하여도 통제할 수 있어야 한다

최근에는 국가 뿐만 아니라 민간영역이나 고용관계 영역에서의 감시가 중요한 문제로 떠오르고 있다. 이를 효과적으로 규제할 수 있는 방안이 마련되어야 한다. 이를 위하여 민간의 감시활동에 대하여도 그것이 미치는 인권침해적인 요소를 면밀히 평가하여 적절한 규제가 이루어져야 할 것이며, 개인정보 보호원칙에서의 개인정보주체의 개인정보의 열람, 정정, 삭제청구권과 마찬가지로 기업이나 사용자에 대하여 감시활동을 당하는 자가 감시활동에 관한 정보의 공개를 청구할 수 있도록 제도적 장치가 마련되어야 한다.

나. 반감시권의 관점에서 바라본 우리 법제의 문제점

앞서 본 반감시권의 관점에서 우리나라의 현행 법제를 본다면 우리의 법제는 국가나 기업 등의 감시행위를 효과적으로 통제하여 국민의 인권침해와 민주주의의 침해를 방지하기 위한 적절한 수단을 갖고 있지 못하다고 평가할 수 있다. 즉, 국가권력이나 민간의 감시행위에 대응하는 효과적인 보호수단을 입법적으로 보장하려는 노력은 찾아볼 수 없고, 단지 소극적인 차원에서 개별적인 프라이버시의 침해에 대한 소극적인 보호와 구제만을 그 내용으로 하고 있을 뿐이다.

(1) 민주주의와 인권보장을 위하여 국가권력이나 민간의 감시행위를 통제할 수 있는 독립성을 가진 통제기구가 없다

우리 법제는 우리 국민에게 국가권력이나 민간의 감시행위를 통제할 수 있는 실질적인 권리를 부여하고 있지 않다. 무엇보다도 국가와 민간의 감시활동을 민주주의, 권력분립, 인권보호의 관점에서 통제할 기구가 있어야 한다.

우리 현행 법제상 국가와 민간의 감시활동을 통제하는 기구로 개인정보보호심의위원회와 개인정보분쟁조정위원회가 있지만 이것들은 아래에서 보다시피 반감시권을 실효성있게 보장하고, 유럽연합의 지침 95/46EC 에서 규정하고 있는 수준의 독립성을 가진 통제기구로 볼 수 없다.

(i) 개인정보보호심의위원회

개인정보보호심의위원회는 공공기관의 개인정보 보호에 관한여 정책 및 제도개선에 관한 사항, 처리정보의 이용 및 제공에 대한 공공기관간의 의견조정에 관한 사항, 개인정보보호에 관한 사항을 다루는 심의기관으로 국무총리 소속기관으로 행정자치부 차관을 위원장으로 하는 기관이다[38]. 그리고 이 위원회 말고 행정자치부장관은 공공기관의 장에 대하여 개인정보의 처리에 관한 자료의 제출을 요구할 권한을 가지고 있으며, 소속공무원으로 하여금 실태조사를 하게 할 수 있고. 공공기관의 장에게 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있는 권한을 가지고 있다. 그리고 각급 중앙행정기관의 장은 산하 공공기관에 대한 실태조사, 의견제시나 권고를 할 수 있는 권한을 가지고 있다[39]. 그러나 이들 기관은 그 스스로가 해당 개인정보

---

38) 공공기관의 개인정보보호에 관한 법률

제20조 (개인정보보호심의위원회) ①공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의하기 위하여 국무총리소속하에 개인정보보호심의위원회(이하 "위원회"라 한다)를 둔다.

② 위원회는 다음 각호의 사항을 심의한다.

1. 개인정보보호에 관한 정책 및 제도개선에 관한 사항
2. 처리정보의 이용 및 제공에 대한 공공기관간의 의견조정에 관한 사항
3. 기타 대통령령이 정하는 사항

③ 위원회의 조직 및 운영에 관하여 필요한 사항은 대통령령이 정한다.

동법 시행령

제27조 (위원회의 구성) ①법 제20조제3항의 규정에 의한 개인정보보호심의위원회(이하 "위원회"라 한다)는 위원장 1인을 포함한 10인이내의 위원으로 구성한다.

②위원장은 행정자치부차관으로 하고, 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자중에서 위원장의 추천으로 국무총리가 임명 또는 위촉한다.<개정 1999.1.29>

③위원의 임기는 2년으로 한다. 다만, 공공기관의 소속직원인 위원은 그 직에 있는 동안 재임한다.

제28조 (위원회의 기능) 법 제20조제2항제3호의 규정에서 "기타 대통령령이 정하는 사항"이라 함은 다음 각호의 사항을 말한다.

1. 법 제7조 단서의 규정에 의하여 개인정보화일에 기록되어 있는 항목의 전부 또는 일부를 관보에 게재하지 아니하려는 경우 그에 관한 사항
2. 기타 관련법령등의 정비·개선에 관하여 위원장이 부의하는 사항

39) 공공기관의 개인정보보호에 관한 법률

제18조 (자료제출의 요구등) 행정자치부장관은 이 법의 시행을 위하여 필요하다고 인정되는 경우에는 공공기관의 장에 대하여 개인정보의 처리에 관한 자료의 제출을 요구할 수 있으며, 소속공무원으로 하여금 실태조사를 하게 할 수 있다.<개정 1999.1.29>

제19조 (의견제시 및 권고) 행정자치부장관은 이 법의 목적을 달성하기 위하여 필요하다고 인정되는 경우에는 공공기관의 장에게 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다.<개정 1999.1.29>

동법 시행령

제22조 (자료제출 요구) ①법 제18조의 규정에 의하여 행정자치부장관이 요구할 수 있는 자료의 범위는 다음 각호와 같다.<개정 1999.1.29>

1. 처리정보의 열람·정정청구현황 및 그 처리실적에 관한 자료
2. 처리정보가 기록된 자기매체·주전산기·입출력장치·전산실등의 보호대책에 관한 자료
3. 처리정보의 제공실태와 제공에 따른 보호대책에 관한 자료
4. 기타 개인정보보호에 관한 제도 및 정책의 수립·개선에 필요한 자료

를 수집하는 기관이거나 해당 개인정보를 수집하는 기관의 상급기관으로서 결코 독립적인 제3기관이라고 볼 수 없다.

(ii) 개인정보분쟁조정위원회

개인정보분쟁조정위원회는 민간영역에서의 개인정보침해에 대한 분쟁조정기구로 정보통신부 장관이 임명하는 위원으로 구성된 조직이다[40]. 이 기구는 위원장 1인을 포함한 15인의 위원으로 구성하여, 개인정보 침해에 대응한 분쟁조정을 주된 역할로 하고 있다. 그런데 이 기구는 단순히 민간영역에서의 개인정보 침해에 대한 조정기구로서의 역할만을 할 뿐이고 공공영역에서의 개인정보 침해에 대해서는 전혀 아무런 조사나 대응도 할 수 없다.

(iii) 두 기구에 대한 평가

---

②공공기관의 장은 행정자치부장관으로부터 제1항의 규정에 따른 자료제출을 요구받은 때에는 정당한 사유가 있는 경우를 제외하고는 30일이내에 관련자료를 제출하여야 한다.<개정 1999.1.29>

제23조 (실태조사의 방법) 행정자치부장관은 법 제18조의 규정에 의하여 실태조사를 하고자 하는 경우에는 해당기관의 장에게 조사의 취지 및 내용, 담당공무원의 인적사항·조사일시등을 미리 통보하여야 한다.<개정 1999.1.29>

제24조 (의견제시 및 권고) ①법 제19조의 규정에 의한 행정자치부장관의 의견제시 및 권고는 권고사항, 권고사유 및 관계기관의 회신기간등을 명시한 서면으로 하여야 한다.<개정 1999.1.29>

②제1항의 규정에 의한 권고를 받은 공공기관의 장은 권고내용에 따라 필요한 조치를 취하고, 그 결과를 행정자치부장관에게 서면으로 통보하여야 한다. 다만, 공공기관의 장이 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보하여야 한다.<개정 1999.1.29>

40) 정보통신망이용촉진 및 정보보호에 관한 법률

제33조 (개인정보분쟁조정위원회의 설치 및 구성) ①개인정보에 관한 분쟁을 조정하기 위하여 개인정보분쟁조정위원회(이하 "분쟁조정위원회"라 한다)를 둔다.

②분쟁조정위원회는 위원장 1인을 포함한 15인 이내의 위원으로 구성하며, 그 중 1인은 상임으로 한다.

③위원은 다음 각호의 1의 자 중에서 대통령령이 정하는 바에 의하여 정보통신부장관이 임명 또는 위촉한다. 이 경우 다음 각호의 1의 자가 1인 이상 포함되어야 한다.

1. 대학이나 공인된 연구기관에서 부교수급 이상 또는 이에 상당하는 직에 있거나 있었던 자로서 개인정보보호관련 분야를 전공한 자
2. 4급 이상 공무원 또는 이에 상당하는 공공기관의 직에 있거나 있었던 자로서 개인정보보호 업무에 관한 경험이 있는 자
3. 판사·검사 또는 변호사의 자격이 있는 자
4. 정보통신서비스이용자단체의 임원의 직에 있거나 있었던 자
5. 정보통신서비스제공자 또는 정보통신서비스제공자단체의 임원의 직에 있거나 있었던 자
6. 비영리민간단체지원법 제2조의 규정에 의한 비영리민간단체에서 추천한 자

④위원의 임기는 3년으로 하고, 연임할 수 있다.

⑤위원장은 위원중에서 정보통신부장관이 임명한다.

⑥분쟁조정위원회의 업무를 지원하기 위하여 제52조의 규정에 의한 한국정보보호진흥원내에 사무국을 둔다.

이들 기구는 모두 행정부처로부터 독립성을 가지고 있지 못하고 있으며, 개인정보분쟁조정위원회의 경우는 국가의 국민에 대한 개인정보 침해행위나 위법한 감시행위에 대해서는 통제를 할 수 없다. 즉, 민간부문의 개인정보침해행위에 대한 조정기구인 개인정보분쟁조정위원회는 당사자들의 분쟁조정 신청이 있는 경우에만 소극적으로 활동을 개시할 수 있을 뿐이며, 다루는 업무범위도 민간영역에서의 개인정보분쟁조정에만 그치고 있을 뿐이고, 단순한 조정기구에 불과하여 각종 정책에 개입할 수 없게 되어 있다. 한편 개인정보보호심의위원회는 각종 법령과 정책에 대한 의견을 제시할 수 있기는 하지만 국가기관으로부터의 독립성이 보장되지 않으며, 프라이버시권리 침해행위에 대한 조사권도 인정되지 않아 한계가 있다. 따라서 무엇보다도 먼저 국가의 개인정보 침해행위나 감시행위에 대하여 통제하고 이를 실효성있게 규제할 수 있는 독립성을 가진 제3의 기관이 설치되어야 한다.

(2) 감시활동에 대한 영향평가 제도의 부재

어떤 감시활동이 도입될 때, 그 감시활동의 도입으로 인하여 개인의 인권이나 민주주의에 어떤 영향을 미칠지가 미리 면밀히 평가되어야 한다. 그래야만 개인의 인권과 민주주의가 지켜질 수 있다. 그러나 우리 법제에는 국가나 기업 등에 의해 구체적인 감시활동이 벌어지거나, 감시활동을 위한 법제도가 새로 도입될 때 그 법제도가 민주주의와 인권에 어떤 영향을 미칠지를 평가하고, 통제할 수 있는 기구나 수단이 존재하지 않으며, 아무런 사전 평가도 하지 않는다.

(3) 보호 및 구제범위의 협소함

현행 법제는 개인정보의 보호에 대하여 포괄적인 보호법제를 취하지 않고 개별적인 보호법제를 취하고 있는데다가, 구제수단도 매우 제한적이어서 개인에 대한 감시나 프라이버시 침해와 관련하여 보호되는 범위와 구제되는 범위가 매우 좁다. 자동처리장치로 처리되지 않는 정보에 대해서는 보호가 인정되지 않으며, 노동자의 개인정보의 보호나 직장에서의 노동감시에 대한 보호가 되지 않고 있고, 사후적인 구제가 아닌 사전적인 구제는 인정되지 않

고 있다.

Ⅲ. 반감시위원회의 설치와 프라이버시 보호를 위한 통합입법의 제정 필요성

1. 반감시위원회의 설치의 필요성

가. 독립기구의 설치

앞서 본 것처럼 국가와 민간영역의 감시활동을 효과적으로 통제하기 위해서는 행정부로부터 독립된 지위를 갖는 기구가 있어야 한다. 이하에서는 외국의 사례를 검토하고, 우리나라의 실정에 걸맞는 반감시위원회의 구성과 역할 등에 대하여 모색해 보기로 한다.

나. 외국의 사례

(1) 독일

독일은 '연방 데이터보호법'(FEDERAL DATA PROTECTION ACT)에서 프라이버시 보호를 위한 독립적인 국가 기구로서 '연방 데이터 보호위원'(이하 연방위원)을 두고 있다. 연방위원은 연방 정부의 제청에 따라 하원(Bundestag)이 선출하고 연방 대통령이 임명한다. 하원은 법정 인원의 과반수 이상의 동의를 얻어 35세 이상의 연방위원을 선출한다. 선출된 연방 위원은 5년의 임기 동안 활동하며 1회에 한하여 연임할 수 있다. 연방위원의 임무는 임기 만료나 해임에 따라 끝난다. 연방위원의 해임은 연방 대통령의 확실한 판단에 따라 합당한 근거가 있는 경우, 연방 정부의 사후 요청 또는 제안에 따라 이루어질 수 있다.

연방위원의 지위와 활동은 철저하게 보장되어 있다. 연방위원은 연방에 대하여 공법상의 공무원 자격을 가지며 직무 수행에 필요한 인적, 물적 자원을 연방 내무장관의 별도 예산서에 의해 제공받는다. 연방 위원은 직무를 수행함에 있어서 독립적인 지위를 보장받으며 오직 법률을 따른다. 보직은 연

방위원의 동의하에 충원되며 직원은 연방위원의 동의에 의해서만 전근, 파견, 재배치될 수 있다. 연방위원이 일시적으로 직무를 수행할 수 없는 경우 연방 내무장관이 대리인을 임명할 수 있지만 이러한 임명에도 연방위원의 자문을 받아야 한다.

연방위원은 본연의 직무 외에 기타 유급직을 유지하거나 수익성이 있는 활동이나 직업에 관여할 수 없으며, 이윤 형성을 목표로 하는 관리, 감독 위원회 또는 이사회에 속할 수 없고, 연방 또는 주의 정부, 입법 기관에 속할 수 없으며, 대금을 받는 조건으로 비공식적인 의견을 내놓을 수 없다. 연방위원은 직무 수행 과정에서 받는 증여에 대하여 연방 내무장관에게 알려야 하고 연방 내무장관은 이러한 증여의 사용 방법을 결정한다.

연방위원은 연방 공공기관의 연방 데이터보호법과 기타 데이터 보호 규정 준수 여부를 감시한다. 개인 데이터가 처리, 사용되는 경우, 연방위원은 데이터 주체가 이와 관련하여 자신의 권리가 침해되었음을 적절히 표시하거나, 침해의 증거를 갖고 있는 경우 데이터의 수집, 처리, 사용을 감시한다.

연방위원의 감시 활동 대상은 전문적이거나 특정한 공무상의 비밀, 특히 세무상의 비밀을 가지는 개인 데이터 주체에게까지 확대된다. 우편통신비밀은 연방위원의 감시 활동을 위해 일정하게 제한될 수 있으나 진료 정보 등 민감한 개인 정보는 제외된다. 데이터 주체가 연방위원의 데이터 감시에 대하여 이의를 제기할 경우, 공공기관은 연방위원의 감시권을 침해함이 없이 일반적인 형식으로 데이터 주체에게 이의 신청의 권리를 알려야 한다. 연방 공공기관은 감시와 관련한 모든 서류와 기록, 특히 저장 데이터와 데이터 처리 프로그램을 열람할 수 있는 기회를 제공할 뿐 아니라 연방위원의 질문에 답신하고 모든 공무 구역으로의 수시 접근을 허용함으로써 연방위원과 보좌관의 직무 수행을 지원해야 한다. 연방위원은 감시 결과를 공공기관에게 알려야 한다.

연방위원이 본 법 및 기타 데이터 보호 규정의 침해, 또는 개인 데이터의 처리, 사용에서 기타 부적합성을 발견한 경우 제소할 수 있다. 연방 행정의

경우 해당 최고 연방기관에 제소하고 독일 연방철도는 관리위원회에 제소하며, 공법상의 연방 법인, 시설, 재단 및 협회는 관리위원회 또는 해당 대표기관에 제소한다. 제소된 상대는 연방위원이 결정한 일자까지 진술서를 제출해야 하는데 진술서는 연방위원의 제소에 대해 자신의 단체가 취한 조치 내용을 담아야 한다.

연방위원은 2년마다 하원에 활동 보고서를 제출하는데 이 보고서는 민간부문에서의 데이터 보호에 관한 주요 진전 사항에 대한 내용을 포함해야 한다. 하원 또는 연방정부가 요청한 경우 연방위원은 의견서와 보고서를 작성해야 한다. 하원, 항소위원회(Petitions Committee), 내무위원회(Internal Affairs Committee), 연방정부가 요청한 경우에는 연방 공공기관에서의 데이터 보호 및 발생 사실을 조사해야 한다. 연방위원은 연방정부와 연방기관에 데이터 보호 개선에 관해 조언할 수 있으며 데이터 보호에 관한 사항을 자문할 수 있다. 또한 연방위원은 주 데이터 보호 규정의 준수를 감시할 책임이 있는 공공기관과 감독 기관과 협조해야 한다. 마지막으로 연방위원은 개인 데이터가 저장된, 자동처리되는 데이터베이스의 등록부를 관리해야 한다. 데이터 파일이 등록된 공공기관은 연방위원에게 목록을 제출해야 한다. 등록부는 모든 사람이 열람할 수 있도록 개방되어야 한다.

(2) 영국

영국은 '데이터 보호법'(DATA PROTECTION ACT)에 의해 '데이터 보호 감독관'(이하 감독관)과 '데이터 보호 재판소'(이하 재판소) 제도를 두고 있다. 데이터 보호 감독관은 여왕에 의해 임명되어 임명시 결정되는 5년을 넘지 않는 기간 동안 재직하고 재임명될 수 있다. 감독관은 65세의 정년을 채우거나 15년 동안 재직했을 때 사퇴해야 하며 상하양원의 요구에 따라 여왕의 명령으로 직위를 박탈당할 수 있다. 감독관을 그만두는 사람은 재임명 최우선자가 되지만 재임명이 공익을 위해 바람직하지 않으면 재임명되지 않는다.

감독관은 부감독관과 기타 임원 및 직원을 임명할 수 있고 이 결정들은

내무장관의 승인을 받아야 한다. 내무장관은 의회에서 제공되는 자금을 감독관에게 지급할 수 있으며 감독관의 임무 수행에 따른 수수료나 기타 금액, 즉 업무 수행과 관련한 비용을 통합기금에서 지급한다. 감독관과 임원 및 직원은 공무원은 아니다.

개인 정보의 데이터 베이스가 작성될 경우 데이터 베이스를 관리하는 데이터 관리자는 어떤 데이터 베이스가 구축되는지 감독관에게 알림으로써 국가에 등록해야 하며, 감독관은 이를 등록하고 관리하면서 데이터 주체들에게도 이를 무료로 제공한다. 감독관은 등록된 데이터 베이스가 데이터 주체에게 치명적인 피해나 고통을 초래할 가능성과 데이터 주체의 중대한 권리와 자유를 해칠 가능성을 평가한 후 28일 이내에 데이터 관리자에게 평가 내용을 통보한다. 데이터 관리자는 평가를 받기 이전에 데이터 베이스를 구축할 수 없으며 이를 어길 경우 형사처벌을 받는다.

감독관은 데이터 관리자가 데이터 보호 원칙을 위반했거나 위반하고 있는 것을 알았을 때 데이터 관리자가 일정 기간 내 특정한 조치를 취하도록 요구할 수 있다. 감독관은 이런 집행통지 업무를 할 때 이를 위반하면 어떤 사람에게 피해나 고통을 초래할지 또는 처리할 가능성이 있는지를 고려해야 한다. 이때 감독관은 부정확한 특정 데이터를 개정, 폐쇄, 삭제, 파기하도록 요구할 수 있다.

데이터 주체들은 감독관에게 자신에 대한 데이터의 처리가 데이터 보호법을 준수하고 있는지에 대해 사정할 것을 신청할 수 있다. 신청이 접수되면 감독관은 데이터 관리자에게 필요한 정보를 제공하도록 요구하고 검토하여 문제가 된 개인 데이터를 사용할 수 있는지 없는지 여부를 결정한다. 특히 개인 데이터가 특정한 목적으로만 처리되지 않고 있거나 출판을 위해 개인 데이터를 처리하고 있다는 의심이 들 경우 감독관은 데이터 관리자에게 이에 대해 확인하여 사용 가능 여부를 결정한다.

감독관의 결정을 받게 되는 데이터 관리자는 데이터 보호 재판소에 소송을 제기할 수 있다. 재판소는 소송을 유래한 감독관의 결정이 데이터 보호법에 부합하는가 등을 고려하여 감독관의 결정을 취소 또는 변경하는 판결을

내릴 수 있다. 재판소는 검찰총장과의 협의 후 대법관이 임명한 의장 · 대법관과, 이들이 임명한 부의장, 그리고 내무장관이 임명한 기타 위원으로 구성된다. 내무장관은 재판소가 그 임무를 적절히 수행하는데 필요하다고 생각되는 임원 및 직원을 두도록 할 수 있다. 재판소의 구성원은 그 임명 기간과 일치하는 기간에 따라 재직, 퇴직해야 하며, 재임용될 수 있다. 재판소 의장이나 부의장은 70세의 정년을 보장받는다. 재판소의 유지 비용은 의회에서 지급되는 자금으로 내무장관이 지출한다.

그 밖에 일반 임무로서 감독관은 데이터 관리자의 모범적 실무를 장려하고 데이터 관리자가 법의 요건을 준수할 것을 장려할 의무가 있다. 여기서 '모범적 실무'란 감독관이 보았을 때 개인 데이터의 처리 과정이 데이터 주체와 기타인들의 이익을 고려했을 때 바람직한 경우이며, 데이터 보호법의 요건을 충족시키는 내용을 포함한다. 감독관은 내무장관의 명령에 의해서나 자신이 필요하다고 생각하는 경우 조합이나 데이터 주체와 협의 후 모범적 실무를 위한 지침이 되는 실무 규정을 보급해야 한다. 또 개인 데이터 처리에 관한 모든 소송에서 국민은 감독관에게 그 소송과 관련한 조력을 요청할 수 있다. 감독관은 소원을 접수한 후 가능한 한 빠른 시기에 이를 검토하여 어느 정도까지 인정할 것인가를 통보해야 한다. 감독관은 내무장관이 명령한 그밖의 데이터 보호 기능을 수행하며, 내무장관은 프라이버시 보호에 관련된 기타 규약을 제정할 때 감독관과 상의하고 그 의견을 고려해야 한다.

(3) 캐나다

캐나다는 '프라이버시법'(Privacy Act)에 의해 '프라이버시 위원'(Privacy Commissioner) 제도를 두고 있다. 프라이버시위원은 상하원의 동의를 얻어 지명되며 7년간의 임기 동안 활동하고 연임될 수 있다. 단, 상하원의 청원이 있을 때 해임된다.

프라이버시위원은 공무원으로서 차관급 권한과 직위를 가지며 독립적인 지위를 보장받는다. 국회에 공무원 신분의 보좌관 약간 명을 추천하여 임명받을 수 있으며 자신이 필요한 공무원 및 직원들을 임명할 수 있다. 프라이

버시위원과 프라이버시위원 보좌관은 다른 직을 겸하거나 보수를 받는 다른 직업에 종사할 수 없다.

프라이버시위원 또는 위원의 위임, 지시에 따라 활동하는 자는 본 법에 따라 위원의 권한, 임무, 역할을 수행, 행사하는 과정에서 선의로 수행, 보고, 진술된 사항에 대하여 민·형사상의 책임을 지지 않는다. 프라이버시위원의 활동과 관련하여 명예 훼손 소송이 발생하면 프라이버시위원은 조사 과정에서의 진술, 제공된 정보, 서류 등에 대해 면책 특권이 적용되며 보고서, 간행물, 언론 보도 내용에 대해서도 마찬가지로 면책 특권이 적용된다. 어떤 사람도 프라이버시위원의 활동을 방해할 수 없으며 이를 위반할 경우 일천 달러 미만 벌금의 즉결 심판에 처한다.

먼저 프라이버시위원은 제소의 업무를 수행한다. 프라이버시위원은 정부기관이 보유한 개인정보가 법에서 정한 원칙을 따르지 않고 사용·공개되었을 경우, 국민이 자신의 정보에 대한 접근을 거부당하거나 지연될 경우, 자신의 정보에 대한 정정을 거부당했을 경우, 정보가 공개될 때 자신이 요청한 언어로 공개되지 않았거나 적절한 번역 및 통역을 제공받지 못했을 경우, 시청각 장애가 있는 개인에게 필요한 방식으로 제공받지 못했을 경우, 부당한 비용을 청구받았을 경우, 기타 정부기관의 개인정보 수집·유지·처분과 사용 및 공개, 그리고 자신의 접근권에 대한 제소를 접수한다. 제소 내용이 합당한 근거가 있다고 판단한 경우 프라이버시위원은 이를 본격적으로 조사하며, 조사에 착수하기 전 관련 정부기관의 장에게 이를 통보한다. 프라이버시위원의 모든 제소 조사는 은밀히 수행되어야 한다. 조사는 상급 법원과 동일한 방법으로 관련자들을 소환하여 위원 앞에 출석시켜 선서 하에 구두로 또는 서면으로 증언하는 방식으로 진행된다. 프라이버시위원이 제소에 대해 조사할 때 정부기관에 출입하거나 정부기관이 통제하고 있는 모든 형식의 정보를 검사할 수 있다. 단, 캐나다 여왕 프라이버시회의의 비밀 정보는 예외로 한다. 프라이버시법의 위반에 대한 기소, 위반에 대한 재심과 항소 과정에서 나온 개인의 증언은 법원이나 다른 소송 절차에서 그 개인에 대한 증언으로 채택될 수 없다.

결론적으로 프라이버시위원이 개인정보와 관련한 제소가 매우 타당하다고 판단한 경우, 프라이버시위원은 권고 사항과 이를 이행하기 위한 조치 내용을 포함한 보고서를 해당 개인정보를 통제하고 있는 정부기관의 장에게 제출하고 제소자에게 알린다. 조사 결과 제소자에게 여전히 정보에 대한 접근이 허용되지 않는 경우, 프라이버시위원은 재심을 법원에 청구할 권리가 있음을 알려야 한다. 제소자가 동의할 경우 프라이버시위원이 직접 법원에 재심리를 신청할 수 있으며 재심리를 신청하였던 개인을 대신하여 법원에 출석할 수 있다. 이러한 소송 절차에서, 이 정보가 공개되어야 하지 않아야 함을 입증할 책임은 관련 정부기관에 있다. 공개의 거부가 정당한 거부가 아닐 경우 법원은 정부기관의 장에게 개인정보를 공개하도록 명령한다.

또한 프라이버시위원은 수시로 정부기관이 통제하고 있는 개인정보와 관련하여 조사를 수행할 수 있다. 조사 후 정부기관이 원칙을 준수하지 않았다고 판단한 경우 프라이버시위원은 조사 결과 및 권고 사항을 포함하는 보고서를 기관의 장에게 제공해야 한다. 정부기관의 장은 특정한 개인정보 데이터베이스를 공개 면제 대상으로 지명할 수 있지만 프라이버시위원은 수시로 면제 대상으로 지정된 파일을 조사할 수 있다. 프라이버시위원이 면제 대상이 된 파일의 재심리를 법원에 신청한 경우 정당한 근거가 없었던 것으로 판결이 난다면 법원은 데이터베이스를 통제하고 있는 정부기관의 장에게 파일의 삭제를 명령한다. 정부기관이 공무를 위해 개인 정보를 공개할 경우 경우에 따라 프라이버시위원은 정부기관의 장에게 관련된 기록을 요청, 조사할 수 있으며 정부기관은 이 요청에 응해야 한다. 정부기관은 일부 경우에 정보가 사용되거나 공개된 용도를 프라이버시위원에게 즉시 통지해야 한다. 프라이버시위원은 사안에 따라 관련된 개인에게 이를 통보할 수 있다.

프라이버시위원은 법무부장관에게 수시로 보고서를 제출하고 법무부장관은 의회가 개정하면 15일 이내에 이 보고서를 의회에 제출해야 한다. 프라이버시위원은 위원의 활동에 관하여 의회에 연례 보고서를 제출하며 긴급하고 중요한 사안에 대해서는 언제든지 위원의 권한 범위, 의무, 역할 및 기능에 관한 특별 보고서를 의회에 제출할 수 있다. 프라이버시위원은 법무부장관이 요청한 프라이버시 침해 사건, 정보기관의 개인정보 수집 · 유지 · 처분 · 사

용 · 공개에 관한 연구를 수행한다.

(4) 프랑스

프랑스는 '정보처리 파일 및 자유에 관한 법률'(이하 프라이버시법)에 따라 프라이버시 보호 국가 기구로서 '국가정보처리자유위원회'(이하 위원회)를 두고 있다. 위원회는 정보처리와 관련된 자에게 그의 권리 · 의무를 알려주고, 정보처리를 기명정보처리에 적용하는 것을 통제하면서 프라이버시법의 준수에 대한 감독 업무를 담당한다.

위원회의 예산은 법무부 예산에 의해 편성되며 독립된 행정기관이다. 위원회는 국민의회와 상원, 경제사회위원회, 국참사원, 파기원, 회계검사원에서 2명씩 선출되고 국민의회의장과 상원의장이 추천한 2명과 각의에서 지명한 3명 등 총 17명의 위원으로 구성되며 임기는 5년이다. 정부의 각료나 정보처리와 관련된 업체의 직원이나 지분 소유자는 위원직을 겸직할 수 없다. 위원회는 자체적으로 위원장과 2명의 부위원장을 선출하며 직원은 위원장 또는 위임을 받은 부위원장이 이를 임명한다. 수상이 지명한 정부 위원이 위원회에 파견근무를 하며 위원회의 심의를 재심의할 수 있다. 위원회는 관할 행정항소법원장 또는 행정지방법원장에게 법관의 파견을 요구할 수 있다.

위원회는 기명정보의 공적 또는 사적인 처리를 프라이버시법의 규정에 따라 행하는지의 여부를 감시한다. 공적인 기명정보의 자동처리는 법률에 의하여 허가받아야 하는 경우를 제외하고 위원회의 의견을 청취한 후에 처리 여부를 결정한다. 위원회가 자동처리에 찬성하지 않는 경우에는 정당한 의결기관의 결정이 있지 않는 한 무시할 수 없다. 특히 보건분야의 기명정보의 처리는 위원회의 허가를 얻어야 한다. 사적인 기명정보의 자동처리는 처리 전 위원회에 신고해야 하며 신고 후에 처리할 수는 있지만 이로 일해 일어나는 법률적 책임을 져야 한다. 위원회는 기명정보에 대한 통제임무를 수행하기 위하여 그 보존을 허가하지 않거나 기간을 정하는 등 규제적인 결정을 내리고 경우에 따라 안전조치 등 규칙을 정하고 명령할 수 있으며 이해관계자에게 통고를 하고 확인된 위반행위를 검찰에 고발한다. 개인의 자기 정보에 대

항목 / 국가	독일	영국	캐나다	프랑스
명칭	연방 데이터 보호위원	데이터 보호 감독관, 데이터 보호 재판소	프라이버시 위원	국가정보처리 자유위원회(17명)
임명권	연방정부의 제청, 하원의 선출, 대통령의 임명	여왕	상하원의 동의로 지명	국민의회와 상원, 경제사회위원회, 국참사원, 파기원, 회계검사원, 국민의회의장, 상원의장, 각의
임기	5년, 연임가능	5년, 15년 이내 연임가능	7년, 연임가능	5년
임기, 정년 이외 해임권	대통령의 판단, 연방정부의 요청	상하양원의 요구, 여왕의 명령	상하원의 청원	위원회 자체
직급	공무원, 겸임 금지	공무원 아님	공무원으로서 차관급, 겸임 금지	독립된 행정기관, 겸임 금지
구성 및 권한	직원 배치 동의권	부감독관과 직원배치에 대한 임명권	공무원 보좌관 추천권(국회 임명), 직원 임명권	위원장과 부위원장 호선, 직원 임명권, 정부위원 파견, 법관 파견 요청권
임무 및 대상	연방공공기관의 프라이버시관련 법 준수 감시	- 개인정보 데이터 베이스 등록받고 평가 * 평가 후에 구축 가능 - 개인들의 사정 신청 접수, 검토 후 사용여부 결정	- 정부기관의 침해사실 조사, 제소 * 민형사상 면책특권 * 활동 방해에 대해 일천 달러 미만 벌금의 즉결 심판	- 공적인 기명정보의 자동처리 여부 결정 * 특히 보건분야 기명정보 처리에 대해 허가권 - 사적인 기명정보의 자동처리 신고 접수 * 활동 방해에 1년징역 및 1,000,000프랑의 벌금
침해사실에 대한 조치	제소대상의 최고및대표기관에 제소	- 조치 요구(개정, 폐쇄, 삭제, 파기), - 데이터 보호 재판소에 제소 및 당사자 소송 지원	- 해당 정부기관의 장에게 보고서 제출 - 제소자에 고지 - 재심은 법원에서 이루어지되 입증 책임은 정부에	- 자동처리 불허, - 보존기간제한 등 조치 및 명령 - 이해관계자에 통고 후 - 검찰에 고발

[표 1] 각국의 프라이버시 보호 관련 국가기구

한 접근성 · 수정권의 행사방법이 제한되지 않도록 감시하며 이에 대한 이

의 · 청원 및 고충사항을 접수한다. 위원회는 확보한 정보처리목록을 일반대중이 자유로이 이용하게 한다. 또한 매년 대통령 및 의회에 그의 임무수행을 보고하는 보고서를 제출하고 동보고서를 공개한다.

위원회 위원은 그의 권한을 행사하면서 어떠한 기관의 지시도 받지 아니한다. 관계 장관, 행정기관, 공사기업의 경영자, 각종 단체의 책임자 및 기명정보화일의 소지자는 위원의 활동에 반대할 수 없고, 위원회의 임무수행을 용이하게 하기 위하여 필요한 모든 조치를 취하여야 한다. 위원회의 활동을 방해하는 자는 1년의 징역 및 1,000,000프랑의 벌금에 처한다.

나. 외국의 사례의 검토

독일, 영국, 캐나다, 프랑스 등 민주주의가 진전된 다른 나라에서는 모두 프라이버시 보호를 위하여 행정부로부터 독립된 기구를 두고 있다. 독일은 '연방 데이터 보호위원'을, 영국은 '데이터 보호 감독관'과 '데이터 보호 재판소' 제도를 두고 있었으며 캐나다는 '프라이버시 위원' 제도를, 프랑스는 '국가정보처리자유위원회'를 두고 있었다.

물론 각국의 개별적인 법제도의 형태에 따라 각 기구의 구체적인 설치 · 운영 방식 역시 조금씩 다르지만 이 기구들이 국가적 수준에서 설치 · 운영되며 활동의 독립성을 보장받는다는 점에서 공통적이다. 영국을 제외하고는 겸임을 금지하여 이해 관계로부터 자유롭도록 하였으며 영국을 제외하고는 공무원 신분을 보장받거나 꽤 높은 직급을 보장받아 정부의 침해 사실에 대해 조사할 때 원활한 업무 수행을 할 수 있도록 꾀하고 있다. 캐나다와 프랑스는 프라이버시 위원의 활동 방해에 대해서도 엄격한 처벌 조항을 명시하였다.

가장 독립적으로 기구가 구성되어 있는 국가는 프랑스이다. 독일, 영국은 기구 구성이나 예산에 있어 특정한 정부 부처의 감독을 받도록 되어 있지만, 캐나다는 의회의 감독을 받도록 되어 있어 상대적으로 독립적인 편이고 프랑스는 기구 구성이나 의원 해임에 있어 위원회 자체의 결정에 따르도록 되어 있다.

임무는 나라마다 조금씩 다른데, 독일은 공공기관의 프라이버시 관련법 준수를 감시·감독하는 것으로 제한되어 있는 반면에 프랑스, 영국, 캐나다는 공공기관과 민간 모두를 통털어 프라이버시 관련법의 준수여부를 감시·감독하고 있다. 가장 중요한 일은 프라이버시 침해행위에 대한 조사와 그에 대한 조치이다. 침해행위에 대한 조사는 고발이나 신고에 의하여 개시되기도 하지만 직권으로 개시할 수도 있다. 조사결과 위법이 발견되는 경우에는 고발을 하거나 시정명령을 내릴 수 있다. 이러한 조치의 미이행에 대해 영국은 데이터 보호 재판소에 제소하고 프랑스는 검찰에 고발하도록 하였다. 마찬가지로 프라이버시 보호 국가 기구의 조치에 이의가 있을 경우 영국은 데이터 보호 재판소가, 캐나다는 법원이 재심하도록 하였는데 캐나다의 경우 입증책임은 정부에 있다.

다. 우리나라의 '반감시위원회'(가칭)의 구성

(1) 위원회제도와 감독관제도

우리도 행정부로부터 독립한 국가기구로서 반감시위원회(가칭)를 구성해야 할 것인데 그 구성은 독일이나 영국과 같은 1인의 감독관이나 위원제도 보다는 여러 명의 회의체로 구성되는 프랑스식의 위원회제도가 적합할 것으로 보인다. 우리나라의 경우 지금까지 존재해 왔던 거의 모든 규제나 견제기구가 1인제로 운영되기 보다는 위원회제도로 운영되어 왔으며, 위원회제도로 해야 좀더 공정성도 기할 수 있을 것이기 때문이다.

그리고 위원회는 독립성을 갖는 국가기구로서 구성되어야 할 것이다. 독립성을 갖는다는 의미는 인사와 예산과 활동에서의 독립성이 보장되어야 한다는 것이다. 그래서 위원회의 위원들은 대통령, 국회, 대법원에서 동수로 추천권을 갖되 대통령이 임명하고, 임기는 4-5년 정도로 보장을 하고 직위를 보장하여야 할 것이다.

(2) 포괄범위 - 공공기관만 할 것인가 민간영역까지 포함할 것인가?

위원회의 기능은 국가나 공공기관 만을 대상으로 하는 것보다는 프랑스나 캐나다처럼 민간영역에까지 포괄하는 것이 좋을 것이다. 왜냐하면 우리나라의 경우 민간영역에서의 개인정보 침해나 감시행위가 빈번하게 일어나서 큰 문제를 일으키고 있는데바, 현재의 개인정보분쟁조정위원회는 이러한 문제에 대하여 전혀 실효성있는 보호기관의 역할을 하지 못하고 있기 때문이다.

(3) 역할 범위는 어떻게 할 것인가?

(i) 수사권 - 위원회는 국가나 민간의 감시활동에 의하여 권리침해가 있는 경우 직권 또는 침해받은 자의 제소에 의하여 또는 직권으로 감시활동에 대한 조사 및 수사를 할 수 있는 권리를 가져야 한다.

(ii) 시정요구권 및 형사고발권 - 위원회는 시정요구권을 가져야 한다. 위원회가 문제가 있다고 판단할 경우 시정요구를 하면 그 시정요구는 강행성을 갖도록 해서 실효성을 담보해야 한다. 그와 함께 형사고발권을 갖도록 해야 한다.

(iii) 정책평가 및 정책제안권 - 위원회는 국가나 민간이 국민의 프라이버시권이나 기타 권리를 침해할 우려가 있는 감시활동을 내용으로 포함하는 법률이나 제도를 도입할 때 필요적으로 위원회의 의견을 청취하도록 하고, 의견제시를 할 수 있도록 해야 하고, 영향평가를 할 수 있는 영향평가권을 가져야 한다.

3. 포괄적인 프라이버시 보호입법의 제정

가. 반감시권을 보장하는 포괄적인 프라이버시 보호입법의 필요성

현재 우리는 감시와 프라이버시 침해행위를 포괄적으로 금지하는 법률을 갖고 있지 않다. 다만 영역별로 규율하고 있을 뿐이다. 이러한 방식은 영역의 특수성에 맞추어 보호의 정도를 다르게 정할 수 있다는 점에서 가중적인 보호가 필요한 민감한 분야(예컨대 의료분야나 통신분야 등)의 감시나 프라

이버시 침해에 대한 법적 규율로서는 적합하나, 법률의 보호에 공백이 생기게 되므로 법적으로 보호되지 않는 부분이 있게 되어 문제가 있다.

따라서 먼저 무엇보다도 모든 영역을 포괄하는 감시나 프라이버시 침해행위를 금지하는 법률을 제정하도록 하는 것이 급선무라 할 것이다[41]. 여기에 덧붙여 의료나 교육과 같은 특별히 가중적인 보호가 필요한 민감한 부분에 대하여는 개별법에서 가중적인 보호를 하면 될 것이다.

나. 목적과 범위

이러한 반감시권을 구체화할 수 있는 법률을 제정할 경우 그 목적은 당연히 국가와 민간영역의 감시활동에 의한 민주주의와 인권의 침해를 방지함이 될 것이다. 그리고 이 법률의 적용범위는 모든 영역을 포괄하는 것이 되어야 할 것이다.

다. 다른 법률과의 관계

이 법은 국가와 민간의 감시활동의 규제에 관한 기본법이 되어야 하며, 다른 법률에 특별한 규정이 없는 경우 감시활동에 대해서는 이 법이 기본법으로 적용되어야 한다.

라. '감시'의 정의

'감시'란 행위의 결과로서 개인이나 집단의 사상의 자유, 행동의 자유가 억압될 수 있는 행위가 포괄적으로 아울러질 수 있는 개념으로 정의되어야 한다. 감시행위를 매체별, 또는 감시의 수단별로 정의하여 이에 대해 규제하는 것은 매체의 통합, 감시기술의 발달에 비추어 부적당하다. '감시'를 그것

41) 요즘에는 많은 국가들이 개인정보의 보호 등에 관하여 포괄적인 입법주의를 취하는 방향으로 가고 있다. 포괄적인 입법주의는 유럽연합이 택하고 있는 제도이며, 유럽연합의 국가들이 많이 이를 따르고 있다. 그에 반해서 개별법주의를 취하고 있는 대표적인 나라는 미국이다. 포괄입법주의를 취하지 않을 경우 유럽연합수준으로 데이터보호가 되지 않는 지역으로의 개인정보 유통을 금지하고 있는 유럽연합의 지침에 따라 경제교류를 못하게 될 우려도 있다.

이 미치는 영향을 기준으로 하여 개인이나 집단의 사상의 자유, 행동의 자유를 억압하는 행위를 포괄적으로 아우를 수 있는 개념으로 정의해야만 기술의 발전에 뒤쳐지지 않고 감시행위를 규제할 수 있다. 이렇게 정의할 경우 감시에는 프라이버시의 침해, 개인정보의 수집 및 이용도 당연히 포함되게 될 것이다.

마 감시활동의 규제

원칙적으로 어느 누구를 막론하고 기본권을 침해할 우려가 있는 감시활동은 금지되어야 한다. 단, 당사자의 동의가 있는 경우, 법률의 규정이 있는 경우, 계약의 이행을 위하여 필요한 경우 등에는 예외적으로 감시활동이 허용되는 것으로 볼 수 있을 것이다. 단, 허용되는 경우라도 인권침해적인 방법으로 이루어져서는 안될 것이다. 감시행위로 인하여 수집된 정보에 대해서는 원칙적으로 당사자의 접근권이 보장되어야 하고, 정보에 대한 수정, 삭제요구권이 허용되어야 한다[42].

바. 감시활동의 계획단계에 대한 개입이 인정되어야 한다

국가가 감시활동에 관한 법률을 제정할 때 개입할 수 있어야 하며, 국가와 민간의 감시활동의 계획에 대하여 개입할 수 있어야 한다. 그리고 감시활동의 계획에 대하여 그것이 인권과 민주주의를 침해할 우려가 있는 경우 이를 다툴 수 있는 수단이 마련되어야 한다. 이는 반감시위원회를 통하여 이루어질 수 있다.

사. 반감시위원회의 설치

감시활동을 인권보호와 민주주의 보호의 측면에서 통제하고 규제하는 기구로서 3권분립의 원칙에 입각하여 행정부를 통제할 수 있도록 대통령, 대법원장, 국회의 추천에 의하여 이루어 구성되어야 할 것이다. 그 활동범위는

42) 따라서 개인정보의 처리시의 원칙(수집시의 당사자의 동의의 원칙, 목적범위를 특정한 고지의 원칙, 개인정보에 대한 개인의 접근권의 보장 등)은 정보통신망 사업자 뿐만 아니라 모든 범위로 확장되게 될 것이다.

앞에서 본 바대로 (i) 국가나 민간의 감시활동에 의하여 권리침해가 있는 경우 직권 또는 침해받은 자의 제소에 의하여 감시활동에 대한 조사권 (ii) 위법한 사항이 발견될 경우의 시정요구, 형사고발권, (iii) 국가가 감시활동을 내용으로 포함하는 법률이나 제도를 도입할 때 필요적으로 의견을 청취하도록 하는 정책평가, 국가나 민간의 감시활동에 대한 의견제시권 등을 내용으로 하여야 할 것이다.

Ⅳ. 국가의 감시활동과 그에 관한 개별 법제의 검토

1. 호적제도와 주민등록제도에 대한 검토

가. 국가나 지방자치단체의 국민, 주민관리체제의 개요

(1) 신분등록제도[43]

모든 국가는 사람의 권리의무관계를 정하기 위하여 민법상의 신분관계를 확인해 주는 신분등록제도를 가지고 있다.

국가나 지방자치단체는 국민이나 주민의 신분에 따른 권리관계의 확인을 해 주기 위해 신분을 등록받아 관리하고 있는데, 그 관리방식으로는 편제의 방법에 따라 출생, 사망, 혼인 등 사건별로만 편제하고 이를 따로 개인별로는 편제하지 않는 사건별 편제방식과 이를 개인별로 편제하는 개인별 편제방식이 있고, 함께 편제하는 사람의 범위에 따라 개인별로만 편제하는 개인별 편제 방식과 가족단위로만 편제하는 가족별 편제방식과 가(家)의 범위에 따라 편제하는 가(家)별 편제방식이 있다.

우리나라의 신분등록제도는 호적제도인데, 우리나라는 출생부, 사망부, 혼인부 등 사건별로 편제하는 사건별 편제방식을 따르고 있는 프랑스, 독일, 미국과 달리 각 사람의 신분변동을 하나의 기록부에 반영하는 인적 편제방

43) 출생, 혼인, 이혼, 사망을 등록하는 제도로 민법관계를 분명하게 하기 위한 가족관계 및 출생, 사망의 증명을 목적으로 하는 제도를 신분등록제도라고 한다. 김기중, '국가의 국민관리체계와 인권', "21세기의 인권 1", 한길사, 2000. 378페이지.

식을 채택하고 있다. 이것은 그 사람의 신분관계를 쉽게 파악할 수 있는 장점이 있지만, 그 사람의 신분관계가 누구에게나 쉽게 노출된다는 단점이 있다[44]. 거기에 우리나라의 호적제도는 입적과 제적에 따른 기록이동이 상호 연결되어 있는 데다가 제적부의 보존연한이 80년이기 때문에 우리나라의 호적의 경우는 사실상 거의 무한으로 혈연관계를 추적할 수 있게 된다고 한다.[45]

우리 호적제도는 인적편제방식 중에서도 '가'(家)별 편제방식을 채택하고 있다. 우리나라가 택하고 있는 가별편제방식은 가족의 범위보다 더 넓은 가(家)를 중심으로 호적을 편제하는 방식으로, 매우 독특한 것이다. 이 방식을 취하고 있는 사례로는 중국민법과 스위스민법에서 찾아볼 수 있다고 하나, 중국과 스위스법상의 가(家)는 현실에서 함께 생활하는 가족을 의미하므로 사실상 가족별편제방식으로 볼 수 있을 것이다. 우리나라의 가별편제방식은 철저하게 혈연을 중심으로 한 호적편제방식이다.

(2) 국민(주민)등록제도[46]

한편 각 나라들은 신분등록제도 외에 조세, 행정 등의 목적을 위하여 국가나 지방자치단체가 국민이나 주민을 별도로 관리하는 등록제도를 두고 있기도 하다. 특정한 행정목적을 수행하기 위하여 목적 수행에 필요한 범위 내에서 특정인으로부터 등록을 받거나 신고를 받는 것은 어느 국가나 지방자치단체에서나 보편적인 현상이지만, 특정한 행정목적 수행을 위한 것이 아니라 일반적으로 행정을 펼치는데 필요하기 때문에 국민이나 주민에게 국가나 지방자치단체에 등록을 하도록 하는 것은 나라마다 편차가 있다. 이 업무는 연방이나 국가에서 담당하기도 하고, 지방정부에서 담당하기도 하고, 어떤 나라에서는 아예 등록제도를 두지 않고 있기도 한다. 즉 이러한 등록제도가 반드시 필요한 것은 아닌 것이다. 미국, 영국, 아일랜드, 오스트레일리아, 캐나

44) 장영아, '호적제도의 개선방안에 관한 연구', 한국여성개발원, "'96 연구보고서 200-4", 1996. 10. 37페이지
45) 장영아, 앞의 책, 14페이지
46) 국민의 주거지를 등록하도록 하는 것으로 행정적 통제, 복지급부 및 통계의 목적으로 시행되고 있다. 김기중, 앞의 책, 379 페이지

다 등과 같은 나라들은 일반적인(전국민적인) 국민(주민)등록제도를 두지 않고 있는 나라들이다. 오히려 강제적인 국민(주민)등록제도를 두고 있는 나라들은 소수의 나라에 속한다.

(3) 일반 신분증 제도

각 나라들은 국가나 지방자치단체는 신분증 제도를 운영하기도 한다. 운전면허증, 여권, 건강보험증, 공무원증 등은 특수한 목적에 맞추어 발급하는 신분증인데, 그 외에 전국민을 대상으로 하는 범용성을 가진 일반목적의 신분증을 모든 국민에게 의무적으로 발급받도록 하는 나라가 있기도 하고, 원하는 사람만 발급받으면 되는 나라도 있고, 아예 그런 신분증이 없는 나라도 있다. 강제적으로 전국민을 대상으로 일반 신분증을 발급받도록 하고 있는 나라들은 극히 소수의 나라에 불과하다.

(4) 국민특정제도

신분증은 아니지만 사실 그보다 더 중요한 것은 국민이나 주민을 특정하기 위하여 부여하는 번호체계이다. 특히 전국민을 대상으로 단일한 특정번호제도(이를 전국민 식별번호제도, National ID 제도라고 부르기도 한다)를 두게 되면 개인의 모든 개인정보가 단일한 특정번호를 중심으로 통합되게 되므로 국가나 민간의 영역에서 개인정보의 통합에 따른 프라이버시 침해나, 감시를 받게 될 위험은 더욱 커지며, 신분 절도(ID Theft: 타인의 신분으로 속여서 타인행세를 하는 것)의 위험이 더욱 커지게 된다. 실로 전국민을 대상으로 하는 단일한 특정번호 제도가 있느냐, 없느냐는 그 나라의 국민의 프라이버시 상황을 단적으로 보여주는 시금석이 되기도 한다. 이러한 전국민 식별번호 제도는 편리할 수는 있지만 매우 위험한 제도이다. 이러한 전국민 식별번호제도를 의무적으로 시행하고 있는 나라도 있고, 원하는 사람에게만 부여하는 나라도 있고(이런 경우는 전국민 식별번호제도로 보기는 어렵다), 그런 종류의 번호가 아예 없는 나라도 있다. 세계 각국 중에서 전국민 식별번호제도를 가지고 있는 나라는 극히 드문 예에 속한다.

제도	목적	방식	우리나라의 경우
신분등록제도 : 주로 국가(법원)에서 취급	신분관계의 증명	*사건별 편제/인적 편제 *개인별 편제/가족별 편제/가별 편제	지방에 신청, 중앙에서 발급 편제 방식의 호적부 지방에서 발급, 번호없음
주거등록제도 : 국가나 지방자치단체에서 취급	행정처리의 목적	지방에서 발급, 번호없음	주민등록제도
국민특정제도 : 국가나 지방자치단체에서 취급	행정처리의 목적 (데이터 식별자)	법무부에서 발급, 번호없음.	기타 납세자 번호, 여권번호 등의 특수목적 특정제도
신분 또는 자격증명 제도 : 국가나 지방자치단체에서 취급	행정처리의 목적 (간편한 업무처리 또는 신분확인)	*특수목적에 따른 신분증/일반적 목적에 따른 신분증	여권, 운전면허증, 공무원증 등의 특수목적 신분증 제도
주민등록제도	일반적 목적	*단일기능/통합기능	일반적 목적의 주민등록증

표 3 국가의 신분등록과 주거등록제도, 신분증 제도와 특정번호제도

오스트리아	임의적 발급	*사건별 편제/인적 편제
벨기에	의무적 지참	*개인별 편제/가족별 편제/가별 편제
덴마크	없음	*국가 또는 지방자치단체에서 관리
핀란드	임의적 발급	*주거등록 없이 전거인 등록, 납세자 등록, 사회보장 등록
프랑스	임의적	회보장 수급자 등록 등 개별적으로만 등록됨
독일	15세 이상 의무적	경우와 일반적인 주거 등록을 요구하는 경우
그리스	14세 이상 의무적	*의무등록제, 임의등록제
네덜란드	임의적	*특수 목적에 따른 특정 납세자 번호
룩셈부르크	임의적	제도
스페인	강제적	*국가/지방자치단체 *전국민에 부여/원하는 자에게만 부여
아일랜드	카드 없음	
이탈리아	임의적	신분증
스웨덴	카드 없음	
미국	카드 없음	
오스트레일리아	카드 없음	
캐나다	카드 없음	

표 2 각국의 범용적 국가등록제도 및 신분증제도, 국민특정제도

이하에서는 우리나라의 신분등록제도와 주거등록제도 및 신분증 제도와 국민특정제도에 대해서 살펴보면서 그것이 가지고 있는 문제점과 개선방안을 알아보고자 한다.

나. 우리나라의 신분등록제도

(1) 현황

먼저 우리나라의 신분등록제도인 호적제도는 호적법이 규정하고 있는데, 인적 편제 방식이서 개인의 신분관계가 일목요연하게 드러나게 되고, 게다가 인적 편제도 개인별 편제방식이 아니라 가(家)별 편제방식으로 구성되어 있어서 다른 혈연구성원의 개인정보까지 드러나게 되고, 혈연관계와 입적과 제적에 따른 기록이 체계적으로 정리되어 있으며, 입적과 제적에 따른 기록의 이동이 연동되어 개인의 혈연관계와 혼인관계, 적출여부 등이 고스란히 드러나게 된다는 점에서 개인의 프라이버시를 심각하게 침해하는 문제가 있다[47]. 그리고 기본적으로 국가에 신고해야 하는 사항이 너무 많다. 구체적으로 살펴보면 호적법에서 규정하고 있는 신분변동의 신고는 출생신고[48], 입양신고[49], 혼인신고[50], 이혼신고[51], 사망신고[52]인데, 이를 토대로 하여 호적부[53]

47) 장영아, 앞의 글

48) 제49조 (출생신고의 기재사항) ①출생의 신고는 1월이내에 이를 하여야 한다. <개정 1975.12.31>
②신고서에는 다음 사항을 기재하여야 한다. <개정 1984.7.30, 1998.6.3>
1. 자의 성명, 본 및 성별
2. 자의 혼인중 또는 혼인외의 출생자의 구별
3. 출생의 연월일시 및 장소
4. 부모의 성명·본 및 본적(부 또는 모가 외국인인 때에는 그 성명 및 국적)
5. 자가 입적할 가의 호주의 성명 및 본적
6. 자가 일가를 창립하는 때에는 그 취지 및 그 원인과 장소
③자의 이름에는 한글 또는 통상 사용되는 한자를 사용하여야 한다. 통상 사용되는 한자의 범위는 대법원규칙으로 정한다. <신설 1990.12.31>
④출생신고서에는 의사·조산사 기타 분만에 관여한 자가 작성한 출생증명서를 첨부하여야 한다. 다만, 부득이한 사유가 있는 경우에는 그러하지 아니하다. <신설 1990.12.31>

49) 제66조 (입양신고의 기재사항) ①입양의 신고서에는 다음 사항을 기재하여야 한다. <개정 1990.12.31, 1998.6.3>
1. 당사자의 성명·본·출생년월일·본적(당사자가 외국인인 때에는 그 성명·출생년월일·국적) 및 양자의 성별
2. 양자의 친생부모의 성명 및 본적
3. 당사자가 가족인 때에는 호주의 성명, 본적 및 호주와의 관계
4. 일가창립 또는 분가로 인하여 호주로 된 자가 폐가하고 양자로 될 때에는 그 취지
5. 민법 제783조의 규정에 의하여 양가에 입적하는 자가 있는 때에는 그 성명, 본, 출생연월일, 그 부모의 성명 및 양자와의 관계
6. 삭제 <1990.12.31>
7. 삭제 <1990.12.31>
②삭제 <1990.12.31>

50) 제76조 (혼인신고의 기재사항) ①혼인의 신고서에는 다음 사항을 기재하여야 한다. <개정 1990.12.31, 1998.6.3>
1. 당사자의 성명·본·출생년월일 및 본적(당사자가 외국인인 때에는 그 성명·출생년월일 및 국적)
2. 당사자의 부모와 양친의 성명 및 본적

에 신분의 변동상황이 기재된다.

(2) 개선방안

현재 호적제도의 개선방안으로 기본가족별 호적제도, 개인별 호적제도[54],

---

3. 당사자가 가족인 때에는 그 호주의 성명, 본적 및 호주와의 관계
4. 처가에 입적할 혼인인 때에는 그 사실
5. 당사자가 초혼 아닌 때에는 직전의 혼인이 해소된 연월일
6. 당사자가 동성동본일지라도 혈족이 아닌 때에는 그 사실
7. 여호주가 폐가하고 혼인하는 경우에는 그 취지

②제19조의2제1항의 혼인신고의 경우에는 제1항의 기재사항외에 신본적을 신고서에 기재하여야 한다. <신설 1962.12.29, 1975.12.31>

③당사자의 일방이 혼가로부터 다시 혼인으로 인하여 타가에 입적하는 경우에는 친가의 호주의 성명, 호주와의 관계 및 본적을 기재하여야 한다.

51) 제79조 (리혼신고의 기재사항) ①리혼의 신고서에는 다음 사항을 기재하여야 한다.<개정 1998.6.3>

1. 당사자의 성명·본 및 본적(당사자가 외국인인 때에는 그 성명 및 국적)
2. 당사자의 부모와 양친의 성명 및 본적
3. 당사자가 가족인 때에는 호주의 성명, 호주와의 관계 및 본적
4. 혼가를 떠나는 자가 친가에 복적하는 때에는 그 가의 호주의 성명 및 본적. 그러나 친가를 부흥하는 때에는 그 취지 및 부흥의 장소
5. 혼가를 떠나는 자가 일가를 창립하는 때에는 그 취지와 창립의 원인 및 장소
6. 민법 제909조제4항의 규정에 의하여 친권을 행사할 자가 정하여진 때에는 그 취지와 내용

②재판상 리혼의 신고서에 제1항제4호 또는 제5호의 기재를 할 수 없는 경우에는 혼가를 떠나는 자가 친가에 복적하는 것으로 본다. 다만, 친가가 없거나 그 본적을 알 수 없는 때에는 리혼 당시의 본적지에 일가를 창립하는 것으로 본다.

[전문개정 1990.12.31]

52) 제87조 (사망신고와 그 기재사항) ①사망의 신고는 제88조에 규정한 자가 사망의 사실을 안 날로부터 1월이내에 진단서 또는 검안서를 첨부하여 이를 하여야 한다. <개정 1975.12.31>

②신고서에는 다음 사항을 기재하여야 한다.

1. 사망자의 성명, 성별 및 본적
2. 사망의 연월일시 및 장소
3. 사망자가 가족인 때에는 호주의 성명 및 호주와 사망자와의 관계

③불득이한 사정으로 인하여 진단서나 검안서를 얻을 수 없는 때에는 사망의 사실을 증명할만한 서면으로써 이에 갈음할 수 있다. 이 경우에는 신고서에 그 진단서 또는 검안서를 얻지 못한 사유를 기재하여야 한다.

53) 제15조 (호적의 기재사항) 호적에는 다음 사항을 기재하여야 한다.

1. 본적
2. 전호주의 성명 및 호주와의 관계
3. 호적의 편제 기타 호적변동사유의 내용과 년월일
4. 호주 및 가족의 성명·본·성별·출생년월일 및 주민등록번호
5. 호주 및 가족이 된 원인과 년월일
6. 호주 및 가족의 친생부모와 양친의 성명
7. 호주와 가족과의 관계
8. 타가에서 입적하거나 타가로 떠난 자에 대하여는 그 타가의 본적과 호주의 성명
9. 호주 또는 가족의 신분에 관한 사항
10. 기타 대법원규칙으로 정하는 사항

[전문개정 1990.12.31]

54) 좀 길지만 서울고등법원 조대현 부장판사의 글 중에서 개인별 신분등록제도에 관한 부분을 싣는다.

개인별 신분등록제도의 내용

(1) 모든 국민의 신분기록을 하나의 시스템으로 전산화하되, 개인의 성명과 주민등록번호에 의하여 그 신분기록을 검색할 수 있도록 한다. 개인별 신분등록제도를 채택하면서 모든 국민의 신분기록을 하나의 시스템으로 전산화하지 않으면, 친족관계의 파악이 어렵게 된다.

(2) 모든 국민의 신분기록사무를 하나의 신분등록청에서 지정된 신분기록관이 담당한다. 전산시스템에 의한 신분기록의 정확성과 변조가능성을 예방하기 위한 것이다. 다만, 그 열람과 등본 발급은 전국 어디서나 가능하게 한다.

(3) 개인의 신분등록표는 출생신고 · 기아발견신고 · 취적신고 · 귀화신고 등에 의하여 새로 편제하고, 일생 동안의 신분변동사유를 그 신분등록표에 모두 기재한다. 본인의 성명 · 주민등록번호 · 출생년월일 · 성별과 같은 개인의 특정을 위한 사항은 물론이고, 본인의 출생 · 사망 · 인지 · 입양 · 친자관계 변동 · 혼인 · 국적변경 · 개명 등의 신분변동사유를 모두 기록한다.

(4) 부부관계와 친자관계를 파악할 수 있도록 하기 위하여 개인별 신분등록표에 본인의 배우자 · 부모(친생부모와 양친부모를 모두 포함한다) · 자녀(혼인중의 자, 혼인외의 자, 전혼중의 자, 재혼중의 자, 양자 등을 모두 포함한다)의 성명과 주민등록번호를 기재한다. 그리고, 신분등록표에 기재된 본인의 배우자 · 부모 · 자녀의 성명과 주민등록번호에 의하여 그 사람들의 각 신분등록표를 바로 검색할 수 있도록 한다. 혼인신고에 의하여 부부의 각 신분등록표에 혼인사유를 기재함과 동시에 배우자의 성명과 주민등록번호를 기재한다. 출생신고에 의하여 출생자의 신분등록표를 편제하면서 출생사유와 부모의 성명 · 주민등록번호를 기재함과 아울러 그 부모의 각 신분등록표에 출생자의 성명 · 주민등록번호를 기재한다. 인지나 입양신고의 경우에도 마찬가지로 처리한다. 배우자 · 부모 · 자녀에 관해서는 그 신분등록표에 대한 검색부호인 성명과 주민등록번호만 기재하고, 그 밖의 개인특정사항이나 신분변동사유는 기재하지 아니한다.

(5) 신분변동에 관한 신고를 접수하거나 신분사항을 기재할 때에 검색부호인 주민등록번호의 정확성을 확보하기 위하여 당사자들의 주민등록번호의 정확성을 점검하도록 한다.

(6) 본인이 사망하거나 국적을 상실하는 경우에도 그 배우자 · 부모 · 자녀의 친족관계 검색을 위하여 검색의 필요성이 없어질 때까지 계속 검색 자료로 비치한다.

(7) 경과조치로서 종전의 호적을 찾아볼 수 있도록 새로운 개인별 신분등록표에 종전 호적의 본적과 호주를 표시하여 줄 필요가 있다.

다. 개인별 신분등록제도의 장점

① 본인의 성명과 주민등록번호로 신분기록을 찾아낼 수 있기 때문에 따로 신분기록의 색출기능을 마련할 필요가 없다. 본적제도도 필요 없고, 신분기록의 명칭 또는 대표자의 명칭과 같은 것도 필요 없다.

② 현행과 같은 호적사항란도 필요 없다. 호적사항란은 호적부의 편제 · 재제 · 전적 · 제적 등의 사유를 기재하는 것이다. 개인별 신분등록표는 출생신고 · 취적신고 · 국적취득신고 등에 의하여 편제되는데, 그러한 사유를 신분사항란에 기재하면 되고 신분등록표의 편제사실을 별도로 기재할 필요가 없다. 그리고, 본적이 없으므로 전적의 문제도 생기지 아니한다. 신분기록이 모두 전산화되므로 신분기록을 재제할 필요성도 없을 것이다. 본인이 사망하거나 국적을 상실한 경우에도 본인이나 그 배우자 · 부모 · 자녀의 친족관계 검색을 위하여 계속 검색 자료로 비치할 필요가 있으므로 말소 · 제적 등의 조치를 취할 필요도 없다.

③ 가족부제도에서 자녀의 신분기록을 부모 중 누구의 가족부에 편제할 것인가에 관한 복잡한 문제가 생기지 아니한다.

④ 가족부제도에서 생기는 남녀평등의 문제가 생기지 아니한다. 개인별 신분등록제도에서는 자녀의 성명과 주민등록번호는 부의 신분등록표와 모의 신분등록표에 모두 기재된다.

⑤ 이적(移籍) · 이기(移記)의 문제가 생기지 아니한다. 신분등록표가 개인별로 편제되고 가

주민등록제도를 보완하는 호적제도[55]가 제기되고 있는데, 개인정보의 침해를 최소화한다는 측면에서 본다면 개인별 편제방식의 호적제도, 그 중에서도 사건별 편제방식의 호적제도가 가장 바람직하다.

개인별편제방식이란 개인마다 기록표를 만들어 그의 신분사항을 시간별로 기록해 가는 방식인데, 미국[56], 프랑스[57], 독일[58]에서는 이 방식을 채택하고

족단위로 함께 편제되는 것이 아니기 때문에, 분가·분적의 문제가 생기지 아니하고, 인지·입양·혼인 등의 경우에도 다른 가족부로 이적하고 신분기록을 이기하여야 하는 문제가 생기지 아니한다. 신분기록사무의 업무량이 대폭 줄어들 것이다.

⑥ 배우자·부모·자녀가 일괄 공시된다. 가족부제도에서는 부부와 자녀의 가족부가 서로 나누어지는 현상을 막을 수 없으므로, 친족관계를 확인하기 위해서는 그들의 가족부가 나누어지기 전의 가족부를 추적하여야 하는 문제가 생긴다. 그러나, 개인별 신분등록표에는 본인의 배우자·부모·자녀의 성명과 주민등록번호가 모두 기재되기 때문에 부부관계와 친자관계를 한 눈에 파악할 수 있다. 사망자의 신분등록표를 보면 그 사람의 배우자·부모·자녀가 모두 기재되어 있기 때문에 제1순위 및 제2순위 상속인까지 바로 파악할 수 있다. 다만, 그들의 사망 여부는 그들의 개인별 신분등록표를 보아야 알 수 있다.

⑦ 프라이버시 침해의 문제를 줄일 수 있다. 개인별 신분등록표에는 본인의 신분변동사유만 기재되고 그 배우자·부모·자녀의 신분변동사항은 기록되지 않기 때문에, 본인과 가족들의 신분변동사유가 한꺼번에 공시되는 가족부제도에 비하여 개인의 프라이버시를 더 보호할 수 있다.

⑧ 하나의 신분등록청에서 신분기록업무를 총괄하므로 신분변동신고서를 한 장만 제출하면 되고, 현행과 같이 여러 장 제출할 필요가 없다.

라. 개인별 신분등록제도의 문제점

㉮ 현재 전국의 호적이 단일 시스템으로 전산화되고 있지만, 그것은 현행 호적제도에 따른 것이므로, 개인별 신분등록제로 바뀌면 그 전산시스템의 내용을 변경하여야 한다.

㉯ 현재의 가족별 호적제도를 개인별 신분등록제도로 바꿀 경우에 본인의 신분사항에 관해서는 다른 바 없으므로 별 문제가 생기지 않을 것이다. 다만, 본인의 주민등록번호와 성명이 컴퓨터에 의한 검색부호이므로, 주민등록번호의 정확성을 확인하고 한자 성명의 한글 표기를 통일시켜 정비할 필요가 있다.

㉰ 본인의 배우자·부모·자녀의 성명과 주민등록번호를 새로 찾아서 기록하여야 하는 문제가 생길 것이고, 이것이 가장 큰 문제이다. 기존 호적도 부부와 그 자녀들이 하나의 호적에 편제되고, 그 호적에 배우자·자녀의 성명과 주민등록번호가 기재되어 있는 경우가 많다. 그러나, 본인과 그 배우자·부모·자녀들의 호적이 서로 다른 경우도 많고, 주민등록번호가 기재되지 않은 경우도 적지 않다. 본인의 배우자·부모·자녀들을 모두 찾아내고 그 주민등록번호를 확인하려면 본인의 신분 내력에 관련된 호적·제적을 모두 찾아서 조사하여야 한다. 그 업무량이 엄청날 것이다. 그러나, 기존 호적의 전산시스템에 호주뿐만 아니라 가족도 그 성명과 주민등록번호에 의하여 호적을 검색할 수 있는 기능을 부가하고, 주민등록 전산시스템까지 동원한다면 어려운 일은 아닐 것이다. 많은 인력과 시간과 예산이 필요할 뿐이다.

㉱ 신분기록이 개인별로 작성되기 때문에 친족들의 구체적인 신분사항을 파악하기 위해서는 관련자의 신분등록표를 모두 열람하여야 한다. 그러나, 개인별 신분등록표에 배우자·부모·자녀의 성명과 주민등록번호가 모두 기재되어 있고, 그 기재를 클릭하여 필요한 신분등록표를 바로 검색할 수 있기 때문에 별로 문제되지 않을 것이다.

55) 장영아, 앞의 글, 대통령직속 여성특별위원회, 현행가족법의 문제점과 개선방안 연구 - 호주제도 폐지를 중심으로, 1999. 12.

56) 미국은 철저한 사건별 기록제도를 가지고 있어, 출생, 혼인, 사망에 따라 각각 증명서를

있다고 한다. 그리고 나아가 그 중에서도 인적편제방식을 배제하고 사건별 편제방식을 채택한다면 개인의 프라이버시 침해를 최소화할 수 있을 것이다. 이 경우 독일이나 프랑스의 경우처럼 난외부기의 방식을 통하거나 가족 수첩 등의 보완적인 제도에 의하여 신분관계의 효율적인 파악을 도울 수 있을 것이다.

한편 이와 같이 개인별편제방식의 호적제도를 채택하면서 할 경우 호적에 기재할 내용도 대폭적으로 줄이는 것이 좋을 것이며, 입적과 제적의 기록연동도 없애도록 해야 할 것이다[59]. 또한 호적사무의 처리와 관련해서 국가에서 담당하고 단일의 시스템으로 운영되도록 연동하는 것보다는 지방에서 처리하는 사무로 분권화시키는 것이 바람직할 것이다. 또한 호적부에 대한 비

작성한다. 그리고, 이러한 증명서간에 연결은 없다. 이혼은 법원에서 하고, 그 기록은 법원에서 보관한다. 장영아, 앞의 글

57) 프랑스도 독일과 마찬가지로 개인별, 사건별 편제방식에 따라 호적부를 편제한다. 프랑스는 호적제도로서 신분증서제도를 두고 있고, 출생증서, 혼인증서, 사망증서, 인지증서 등, 다양한 증서들을 작성한다. 이러한 증서에 기록한 사항을 일람하여 파악하기 위하여, 역시 난외부기방법을 채택하며, 나아가 출생증서에 다른 증서사항을 난외에 대부분 부기하여 출생증서의 일람으로 개인정보를 파악할 수 있도록 하고 있다. 또한 가족관계를 파악하기 위하여 가족대장을 각 가정에 발급하여 보관하도록 하고 있다. 장영아, 앞의 글

58) 독일에서는 개인별, 사건별 편제방식에 따라 출생, 혼인, 사망의 각 사건마다 호적부를 작성한다. 따라서, 출생부, 혼인부, 사망부가 존재한다. 그리고, 개인의 이러한 사항을 일람하여 파악하기 위하여, 이러한 호적부간을 연결하는 난외부기방식을 채용한다. 나아가, 가족관계를 분명하게 하기 위하여 가족부도 작성한다. 가족부는 혼인으로 개설하고, 부부와 미혼자녀의 신분사항을 기록한다. 출생부, 혼인부, 사망부에서 가족부에 기록할 사항을 통지한다. 장영아, 앞의 글

59)한편 김상용 교수는 호주를 중심으로 하는 추상적인 가별편제방식의 호적제도가 실제의 가족생활관계를 반영하지 못함으로써, 주민등록제도가 신분등록제도의 역할까지 하게 되어 개인의 사생활 침해로 이어지고 있다고 한다.

"호주를 중심으로 하는 추상적인 '가'를 기본단위로 하여 편제되는 현행 호적은 실제의 가족생활관계를 반영하지 못한다. 그 결과 주민등록제도가 비정상적으로 확대되는 문제가 발생하게 되었다. 원래 안보목적으로 도입된 주민등록제도가 본래의 취지를 넘어 일반행정, 민간거래는 물론 호적제도의 기본 기능인 신분관계 확인을 위한 공부로도 이용되고 있는 것이 현실이다. 이처럼 주민등록제도가 호적의 기능까지 수행하고 있으므로, 대부분의 국민들은 일상생활에서 호적의 필요성을 거의 느끼지 못하게 되었고, 따라서 현행 호주제와 호적제도의 문제점에 대해서도 제대로 인식하지 못하게 된 것이다. 그러나 주민등록제도의 비정상적인의 팽창은 개인의 사생활 침해로 이어지는 정보유출을 비롯하여 많은 문제를 낳고 있다(주민등록표에 의해서 관리되는 개인정보는 140개 항목에 달하며, 이 가운데 78개 항목은 국가가 관리하는 데이터베이스에 수록되어 있다. 국가가 국민 개개인에 대하여 이처럼 방대한 정보를 보유·관리한다는 것은 국가에 의한 개인의 인권침해 가능성을 의미하는 것이다). 결국 현행 주민등록제도의 문제점을 해결하기 위해서도 가를 중심으로 편제하는 현행 호적제도는 개선되어야 한다. 위에서 본 바와 같이 부부를 중심으로 호적을 편제하는 방식을 따르게 되면, 현실적으로 공동생활을 하는 가족이 같은 호적에 기재될 수 있으므로, 주민등록제도의 필요성이 그만큼 감소하게 될 것이다. 나아가 호적이 주소등록제도를 겸하도록 하는 방법도 생각해 볼 수 있으며, 이와 같은 방식을 통하여 호적제도와 주민등록제도가 각각의 고유한 기능을 되찾을 수 있으리라고 생각한다."

밀보호의무를 엄격하게 부과하고, 당사자 이외의 열람을 극히 제한적으로 허용해야 할 것이다.

다. 국민(주민)등록제도의 개선방안

(1) 현황

우리나라는 주민등록법을 통하여 국가에서 직접 전국민을 대상으로 주거등록을 하도록 하는 주민등록제도를 실시하고 있다. 주민등록법에 의하여 모든 국민은 30일 이상 거주할 목적으로 주소를 둘 경우 국가에 주민등록신고를 해야 한다.[60] 주민등록신고를 하면 이를 토대로 개인별 뿐만 아니라 세대별

---

60) 제6조 (대상자) ①시장·군수 또는 구청장은 30일이상 거주할 목적으로 그 관할구역안에 주소 또는 거소(이하 "거주지"라 한다)를 가진 자(이하 "주민"이라 한다)를 이 법의 규정에 의하여 등록하여야 한다. 다만, 외국인에 대하여는 예외로 한다.<개정 1991.1.14>
②제1항의 등록에 있어 영내에 기거하는 군인에 대하여는 그가 속하는 세대의 거주지에서 본인 또는 그 세대주의 신고에 의하여 등록하여야 한다.<개정 1975.7.25>
③해외이주법 제2조의 규정에 의한 해외이주자는 대통령령이 정하는 바에 의하여 해외이주를 포기한 후가 아니면 등록할 수 없다.<신설 1991.1.14>
제7조 (주민등록표등의 작성) ①시장·군수 또는 구청장은 주민등록사항을 기재하기 위하여 개인별 및 세대별 주민등록표를 작성·비치하고, 세대별 주민등록표색인부를 비치·기록하여야 한다.<개정 1991.1.14>
②개인별 주민등록표는 개인에 관한 기록을 종합적으로 기록·관리하며 세대별 주민등록표는 그 세대에 관한 기록을 통합하여 기록·관리한다.
③시장·군수 또는 구청장은 주민에 대하여 개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다. <신설 2001.1.26>
④주민등록표와 세대별 주민등록표 색인부의 서식과 기재방법 및 주민등록번호의 부여방법은 대통령령으로 정한다.<개정 1993.12.27>
제10조 (신고사항) ①주민은 다음 각호의 사항을 그 거주지를 관할하는 시장·군수 또는 구청장에게 신고하여야 한다.<개정 1968.5.29, 1991.1.14, 1993.12.27>
1. 성명
2. 성별
3. 생년월일
4. 세대주와의 관계
5. 합숙사에 있어서는 그 관리책임자
6. 본적
7. 주소
8. 본적이 없는 자 또는 본적이 분명하지 아니한 자는 그 사유
9. 대한민국의 국적을 가지지 아니한 자는 그 국적명 또는 국적의 유무
10. 거주지를 이동하는 경우에는 전입전의 주소 또는 전입지와 그 년월일
11. 삭제<1999.5.24>
12. 대통령령으로 정하는 특수기술에 관한 사항
②누구든지 제1항의 신고를 이중으로 할 수 없다.<신설 1968.5.29, 1975.7.25>

로도 주민등록부가 체계적으로 작성되게 된다.

(2) 개선방안

주거등록제도는 국가 또는 지방자치단체가 행정처리를 목적으로 주거하는 국민이나 주민의 신상을 등록하게 하는 제도인데 앞서 본 것처럼 많은 선진국들은 아예 이러한 국민등록제도를 두지 않고 있기도 하다. 이것들은 일반적인 인식과는 달리 국민등록제도를 두지 않아도 행정목적을 실현하는데는 아무런 문제가 없다는 것을 방증하는 것이다.

따라서 우리의 경우에도 의무적인 국민등록제도를 아예 폐지하고 임의적으로 원하는 사람만 등록을 하게 국민등록제도를 임의화해도 문제가 없을 것이다. 따라서 우리나라의 경우 의무적인 국민등록제도를 임의적인 국민등록제도로 변경하는 것도 고려해 볼 수 있을 것이다. 그리고 또한 임의적인 등록제도를 둔다 하더라도 등록을 국가에서 받는 것이 아니라 각 지방별로 등록을 하도록 한다면, 개인정보 통합이 덜 가속화될 것이므로 임의적인 지방자치단체에 의한 주민등록제도가 현행의 강제적인 국가의 국민등록제도의 폐해를 줄이는데 도움이 될 것이다. 따라서 지방자치단체에서 주민등록을 받는 임의적인 주민등록제도로 변경하는 것이 가장 바람직할 것이다. 물론 이와 같이 임의적인 주민등록제도로 변경한다 하더라도 각 분야별로는 행정목적에 따라 해당 행정기관에 개인이 등록을 해야 하는 경우가 많이 있을 것이다. 예컨대 예비군이나 민방위와 같은 병무관련 등록, 차량등록, 부동산 등기, 사회보장을 위한 각종 등록, 의료보험 등록 등이 필요할 것이다. 그러나 이러한 특정한 목적에 따른 등록이나 신고는 포괄적인 주민등록제도와는 목적과 효과가 엄연히 다른 것이고, 정보의 공유도 엄격하게 제한되어야 할 것이다.

그리고 현행 주민등록법은 국민등록시에 지나치게 많은 개인정보를 국가에 등록하게 강제하고 있는데, 주민의 지위를 정하는 법률이어야 할 주민등록법이 이와 같이 목적범위를 벗어나는 과도한 정보를 등록하도록 하고 있는 것은 큰 문제가 아닐 수 없다[61]. 따라서 지방자치단체가 주민등록법에 의

해 수집할 수 있는 정보를 지방자치단체 주민의 지위를 정하는 데 필요한 최소한의 정보로 한정할 필요가 있다. 그리고 개인에게 민감한 정보일 수 있는 동거가족을 반드시 기재하도록 하고 세대주와의 관계까지 신고하도록 하는 세대별 주민등록표를 폐지해야 한다[62]. 또한 주민등록정보의 수집, 보관, 관리, 이용에 있어 정보주체가 참여할 수 있는 범위를 최대한 넓히는 방향으로 주민등록법을 개편해야 할 것이다. 특히 주민등록정보를 중앙정부 행정기관이나 다른 공공기관이 이용하도록 할 경우 반드시 필요한 경우로 한정하고, 그 이용의 목적을 분명히 하고 제공의 목적이나 일자 등 관련정보를 문서로 기록하도록 하며, 사후관리를 강화하고, 정보주체에게 주민등록정보의 이용 또는 제공에 관한 사항을 알리거나 적어도 적절한 방법으로 공지해야 할 것이다. 정보주체가 본인 정보의 열람이나 정정을 요구할 경우 즉시처리되도록 해야 하며, 정보주체가 전산화된 정보에 쉽게 접근할 수 있는 장치를 별도로 마련해야 할 것이다.[63]

라. 범용 신분증 제도

우리나라는 18세 이상의 자에게 의무적으로 범용 신분증인 주민등록증을 발급받도록 하고 있는데, 이 제도 역시 많은 프라이버시의 노출의 위험을 가지고 있다. 특히 우리나라의 경우 신분증을 발급받으면서 주민등록증 발급신청서라는 서식에 의해 강제되는 열 손가락 지문날인제도 및 주민등록법에 의해 수집한 지문정보를 법률적 근거도 없이 경찰청이 보관하며 범죄수사에 활용하고 있는데 이것은 법적 근거나 합리적 사유없이 인격권을 침해하는 제도로서 헌법이 보장하는 무죄추정권, 인격권을 침해하는 위헌의 소지가 있기 때문에 폐지되어야 할 것이다.[64]

마. 국민특정제도(National ID)

(1) 현황

---

61) 김기중, 윤현식, 한국주민등록법의 개정방향.
62) 김기중, 윤현식, 한국주민등록법의 개정방향.
63) 김기중, 윤현식, 한국주민등록법의 개정방향.
64) 김기중, 윤현식, 한국주민등록법의 개정방향.

우리나라의 경우 주민등록법에 따라 국가는 전국민에게 일률적으로 일련번호에 의한 주민등록번호를 부여한다[65]. 우리나라가 국민에게 부여하고 있는 주민등록번호는 전국민 특정제도(이른바 National ID제도)[66]로 볼 수 있다. 그런데 우리나라의 주민등록번호제도는 다음과 같은 점에서 가장 강력한 수준의 국민특정제도로 불릴 만하다.

(i) 주민등록번호를 국가에서 통괄하면서 일률적으로 부여한다. 이것은 분권화된 지방자치단체에서 부여하는 국민특정번호보다 더 강력한 전국민에 대한 특정번호제도이다.

(ii) 국가가 모든 국민에게 부여하는 주민등록번호는 외부에서 그 번호만 보아도 나이, 출신지역, 성별 등을 확인할 수 있게 되어 있으며, 한번 발급된 주민등록번호는 평생 변하지 않고 그 사람을 따라다닌다는 점에서 임의적인 번호체계로 단순한 일련번호에 불과한 번호인 경우나, 번호가 바뀔 수 있는 경우보다 훨씬 더 강력한 전국민 특정번호제도이다.

(iii) 국가는 개인별 주민등록부 뿐만 아니라 세대별 주민등록부를 전산처리하여 주민등록표 파일의 형태로 보관, 관리한다. 이로써 국가는 전국민에 대한 개인별 자료 뿐만 아니라 세대별 주민등록 전산정보자료까지 함께 구축한다.

(iv) 특히 우리나라는 그 동안 수십년의 축적된 주민등록자료가 전산화되어 있으며, 행정영역의 경우는 모든 행정영역에서 제한 없이 주민등록번호를 사용해 왔으며, 민간부문에서도 주민등록번호를 개인식별수단으로 사용해 오고 있어서 개인정보의 통합화된 정도가 전세계에서 유례를 찾아볼 수 없을 정도로 강력하다.

---

65) 제7조의2 (전산정보처리조직에 의한 주민등록표화일 작성등) ①제7조의 주민등록표 및 주민등록표색인부에 기재할 사항은 전산정보처리조직(이하 "전산조직"이라 한다)에 의하여 처리하여야 한다. 이 경우 그 주민등록표화일(자기테이프·자기디스크 기타 이와 유사한 방법에 의하여 기록·보관하는 개인별 또는 세대별 주민등록표 및 세대별 주민등록표색인부를 말한다. 이하 같다)은 제7조제1항 및 제2항의 규정에 의한 주민등록표 또는 세대별 주민등록표색인부로 본다.<개정 1997.12.17>

②제1항의 규정에 의한 주민등록표화일의 정리·관리·보관등에 필요한 사항은 대통령령으로 정한다.

③시장·군수 또는 구청장은 주민에 대하여 개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다.

66) 고유의 일련번호의 특징으로 유일성, 영속성을 들 수 있다.

우리나라의 주민등록번호는 국가가 모든 국민에게 부여하고 관리하는 번호로서 그 국민에게 유일하고, 영속적이며, 변하지 않는 번호이다. 따라서 그 번호는 국내 어디에서든 그 사람을 대표하는 유일한 번호가 되는 것이다. 그렇기 때문에 그 번호는 그에 관한 모든 개인정보의 통합자와 식별자 역할을 하게 된다. 우리나라의 경우 이렇게 전국민을 대상으로 부여된 식별번호를 바탕으로 전국민에게 의무적으로 신분증을 발급받도록 하고 있는 것이다. 따라서 주민등록증이라는 플라스틱 카드는 전국민에 대한 고유번호 데이터베이스 체계의 외화된 일부에 불과할 뿐, 진정 중요하고 위험한 역할을 하는 것은 전국민에 대한 고유번호 체계인 주민등록번호인 것이다.

오늘날 이 주민등록번호는 각급 공공기관에서 보유하고 있는 개인정보화일(중앙행정기관 99종, 지방자치단체 126종, 각급학교 22종, 정부투자기관 기타 204종 : 2000. 12. 행정자치부 공고)과 민간영역에서 보유하고 있는 모든 개인정보의 식별자 역할을 하고 있다. 그 뿐만 아니라 최근에는 대부분의 인터넷 웹사이트에서 주민등록번호를 개인의 신분확인용으로 사용하고 있으며, 심지어는 국가에서 민간기업들에게 전국민의 주민등록번호를 개인신분확인용으로 사용하도록 데이터베이스를 제공하고 있기도 하다.

(2) 문제점

국가가 전국민에 대하여 고유번호를 부여하는 제도는 (i) 국가기관이나 민간영역에서의 개인정보에 대한 데이터의 통합을 손쉽게 함으로써, 심각한 프라이버시의 침해위험을 가져오고, (ii) 이를 통하여 국민에 대한 감시가 손쉽게 이루어질 수 있게 되며, 국가기관이나 경찰권의 힘을 강화시키고, (iii) 전국민에 대한 고유번호가 신분확인의 수단으로 사용되면서 손쉽게 신분도용(ID theft)의 문제가 생기게 되며, (iv) 개인정보 데이터베이스에 대한 침해를 용이하게 한다는 점에서 국가기관에게 전국민을 감시할 수 있는 우월한 감시능력을 부여하는 제도로서 문제가 있다.

현재 비교법적으로 보더라도 독일[67], 프랑스[68], 영국[69], 미국[70], 호주[71]를

67) 독일의 경우는 국가에서 사건별 편제방식의 신분등록제도를 기본으로 하면서, 가족부와 혼인부를

비롯한 대다수의 많은 국가들이 전국민에 대한 고유 식별번호(National ID)를 도입하지 않거나 최소한 의무적인 국민등록제와 결합된 전국민 고유 식별번호제도를 도입하지 않고 있으며, 전국민에 대한 고유 식별번호로 될 가능성이 있는 번호(예를 들어 미국의 경우는 Social Security Number, 호주의

보충적으로 운영하고 있다. 한편 주거등록제도는 각 주별로 주법에 의하여 주소와 본인확인정보를 신고하도록 하고 있는 것으로 알려져 있다. 그런데 각주에서 관리하는 이 주거정보는 연방정부나 각 지방정부 사이에 상호 통보되거나 상호 전산망으로 연동되어 있지 않다고 한다. 한편 독일의 경우 연방차원에서 신분증제도를 가지고 있으나, 이 신분증에는 일련번호가 부여되지만 이 일련번호는 단순히 그 신분증에 부여되는 일련번호일 뿐 그 사람에 대한 일련번호는 아니라고 한다. 그래서 새 신분증을 발급할 때마다 새 번호가 부여된다고 한다. 또한 이 일련번호에는 생년월일이나 성별 등의 인적사항 등을 추정할 수 있는 내용을 담을 수 없도록 하고 있으며, 공적기관은 물론 사적기관도 일련번호를 데이터베이스에서 인적사항을 추출하는 것(프로파일링)이나 여러 데이터베이스 자료의 결합(머징)하기 위하여 사용할 수 없도록 명시적으로 규정하고 있다고 한다. 즉, 독일의 경우 연방차원에서 신분증제도를 가지고 있기는 하지만, 전국민을 대상으로 하는 고유식별번호는 부여하지 않고 있으며, 연방의 신분등록정보와 각 지방의 주거정보와 연방의 신분증 정보가 서로 엄격하게 분리되도록 철저한 법적 장치를 마련해 두고 있다고 한다(이상 김기중, 국가의 국민관리체계와 인권).

68) 프랑스의 경우 모든 국민에게 개인식별번호를 부여하고 있으나 강제적인 주거등록제도는 없다고 한다(이상 김기중 앞의 책)

69) 영국에서는 최근 전국민을 대상으로 하는 고유식별번호부여 및 전자신분증 도입을 추진하고 있으나 강력한 반대에 부딛혀 실현되기 어려운 상황이라고 한다.(프라이버시 인터내셔널의 사이트 참조 : www.privacyinternational.org)

70) 미국에서는 사회보장번호는 사회보장국에서 운영된다. 사회보장번호는 사업이나 교육에서도 상당히 사용되고 있다고 한다. 사회보장번호는 인구의 대다수가 부여받고 있으나 완전성은 매우 낮다고 한다.(FACFI 1976, CG 1980, OTA 1981).미국의 경우 최초의 사회보장법(Social Security Act of 1935)이 제정되었고, 피용자와 고용주에게 세금을 부과하는 고유번호가 1936년에 성립되었다고 한다. 피용자는 그 번호를 고용주에게 제출해야 했다. 발행된 사회보장카드에는 '신분증명용이 아님'이라는 설명이 들어 있었다고 한다.(HEW, 1973, pp.114-122). 1943년 사회보장번호를 모든 연방정부의 근로자에게 확대하여 사용하는 결정이 취해졌다(루즈벨트의 행정명령[9937]). 많은 비용 부담이 되는 중복업무를 피하기 위하여 모든 연방기관은 사회보장번호를 이용한 개인 식별시스템을 확립할 것을 명령한 이 명령은 지금도 유효하다고 한다(Westin & Baker, 1972, p.41).그러나 1961년 재무성 산하의 소득세 담당부서인 Internal Revenue Service(IRS)가 납세자를 확인하기 위하여 사회보장번호를 사용하기 시작하기 전(P.L. 87-397 : 1961. 10. 5.)까지는 사회보장번호의 사용범위에는 큰 영향이 없었다고 한다. IRS는 개인에게 이자를 지급하는 기업에게 해당 개인의 사회보장번호를 수집하여 보고하도록 임무를 부여했다. 사회보장번호는 통합성이 낮다고 한다. 이것은 외견상 유효해 보이는 번호가 사회보장청으로부터 발행된 것인지 여부를 확인해 줄 수 있는 능력을 갖춘 조직이 별로 없기 때문이라고 한다. 현재 9개의 번호로 구성된 사회보장번호의 약 40%가 배당되었다고 한다. 현재 남아 있는 번호 중에도 외견상 유효한 번호는 많이 있다고 한다. 가장 대표적인 거짓번호는 078-05-1120이라고 하는데, 이 번호는 1940년대와 1950년대에 지갑에 샘플로 넣어져서 판매된 번호라고 한다. 이런 심각한 약점이 있음에도 많은 연방정부 기관들은 신분확인용으로 사회보장번호를 사용하고 있다고 한다. 기업들은 사업을 하는데 법적인 근거가 없음에도 그 번호를 사용한다고 한다(Hibbert 1992). 소비자의 정보를 판매하는 The Lotus Marketplace service도 사회보장번호를 사용한다고 한다.(이상 Roger Clarke, Human Identification in Information Systems: Management Challenges and Public Policy Issues)

71) 호주에서도 최근 전국민 특정번호를 도입하려고 하였다가 강력한 반대로 무산되었다. (프라이버시 인터내셔널 웹사이트 참조 : www.privacyinternational.org)

경우는 Tax Payer's Number)에 대하여 특별한 법적 보호를 하고 있다. 그래서 전국민에 대한 고유 식별번호로 기능하지 않도록 최선의 노력을 기울이고 있다.

실제로 독일과 헝가리, 필리핀에서는 전국민에 대한 고유 식별번호의 부여에 대하여 위헌이라고 판시한 사례가 있기도 하다.[72] 이런 점에서 볼 때 전국민에 대하여 고유의 일련번호를 부여하는 현재의 고정불변의 주민등록제도는 국가와 민간에 의한 과도한 국민감시를 허용함으로써 헌법상 보장되는 인격권을 침해하는 제도로 판단될 가능성이 높은 제도이다.

(3) 개선방안

(i) 주민등록번호제도의 폐지

중앙과 지방, 행정 각부처와 사법부 등에 산재되어 있는 국민이나 주민들의 개인정보화일의 통합을 막기 위해서는 가장 우선적으로 전국민에 대한 국가의 주민등록번호의 부여제도가 폐지되어야 한다.

국가의 전국민에 대한 의무적인 등록제에 기초한 주민등록번호제도를 폐지하는 방법으로는 (i) 국가에 의한 의무적인 국민등록제를 완전히 폐지하고 주민등록번호 자체를 폐지하는 방안과 (ii) 전국적인 의무적 국민등록제를 폐지하고, 지방자치 차원에서 임의적인 주민등록제를 운영하면서 주민등록번호를 폐지하고 임의적인 일련번호를 부여하는 방안, (iii) 전국민에 대한 의무적인 등록제를 두되, 국민식별번호제도를 없애고, 국민식별번호를 통한 개인정보의 통합을 억제하는 방안 등을 생각해 볼 수 있는데, (i)의 방안이 가장 바람직하겠지만 오랫동안 국민식별번호제를 운용해오고 있었으므로 갑작스런 행정의 공백이 우려된다면 현실적으로 (ii)의 방안을 택하여 점진적으로 국민식별제도를 없애 나가는 방법을 택할 수도 있을 것이다.[73]

---

72) 프라이버시 인터내셔널(www.privacyinternational.org), 전자프라이버시정보센터(www.epic.org)

73) 김기중, 윤현식, 한국주민등록법의 개정방향

즉, 두 번째 방안을 택한다면 전국민에게 고유번호를 부여하는 국가의 전국민에 대한 통합관리체제인 주민등록제도를, 지방자치단체별 주민에 대한 등록체제로 주민등록법을 지방자치단체 주민의 지위를 정하는 법률로서 위치짓고, 전국민에 대한 일련번호의 부여제도를 폐지하고, 지방자치단체에서 자발적으로 원하는 사람들에게 필요한 경우에만 필요한 범위 내에서 통용되는 임시적인 신분등록번호를 부여하는 것으로 하면 될 것이다. 이것은 예컨대 운전면허증의 고유번호, 여권의 고유번호, 납세자 번호 등과 같이 필요한 범위 내에서만 통용되는 것으로 해야 할 것이다. 따라서 주민등록제도의 경우 지방자치단체에서 주민의 등록정보로서만 활용하여야 할 것이다[74]. 그리고 이 경우 주민등록시 부여되는 신분등록번호는 중앙정부와 통합을 시도해서는 안될 것이며, 지방자치단체에서도 다른 주민의 개인정보와 통합되지 않도록 해야 한다. 또한 이 경우 주민등록제도는 개인별 고유번호가 아니라 신분증발급번호가 되어야 하며, 따라서 다른 목적으로 그 번호를 개인을 특정하기 위한 번호로 사용하는 것을 엄격하게 금지하고 이를 법정해야 한다.

(ii) 주민등록번호의 보호

주민등록을 임의적인 제도로 변경을 하는 경우에도 주민등록번호가 사라지지 않는다면 주민등록번호는 여전히 개인의 정보에 대한 식별자 역할을 하게 될 것이다. 실제로 미국의 경우나 오스트레일리아의 경우 사회보장번호나 납세자 번호가 개인정보에 대한 식별자 역할을 하게 되어 사실상 전국민 고유번호제도로 운용되고 있다는 비판이 제기되고 있는 상황이다. 따라서 이 경우 주민등록번호에 대해서는 특별한 보호가 취해져야 한다. 즉, 주민등록번호를 함부로 사용하지 못하게 하고, 특별히 법적으로 요구되는 꼭 필요한 경우가 아니라면 주민등록번호를 요구하지 못하도록 하고, 주민등록번호가 꼭 필요한 경우가 아니라면 주민등록번호의 제공을 거부했다는 이유로 서비스 제공을 거부해서는 안된다는 규정을 두어야 할 것이다.

실제로 미국의 경우 법으로 사회보장번호의 공개를 금지하고 있으며, 법령이 정하고 있는 경우를 제외하고는 사회보장번호를 요구하는 것을 금하고

74) 김기중, 윤현식, 한국주민등록법의 개정방향.

있으며, 사회보장번호를 제공하지 않았다는 이유로 서비스 제공을 거부해서는 안된다는 규정을 두고 있다(the Privacy Act of 1974. 5 U.S.C. Sec. 552a). 그리고 미국의 법원은 선거인명부의 등록시에 사회보장번호를 요구하는 것은 프라이버시권을 침해하는 것이라고 판시하였고{Greidingerv. DavisGreidingerv. Davis, 988 F.2d 1344 (4th Cir. 1993)}, 국가는 개인의 사회보장번호를 정보공개시에도 공개해서는 안된다고 하였으며{Painting and Drywall Work Preservation Fund, Inc. v. Department of Housing and Urban Development, 936 F.2d 1300 (D.C. Cir. 1991) 등}, 연방직원의 사회보장번호는 공적기록에 해당하지 않는다고도 하고, 일단 사회보장번호가 공개되는 경우에는 그 피해가 막대하다고 보고 사회보장번호는 매우 중대한 프라이버시로서 엄격하게 보호되어야 한다고 판시하였다.{American Federation of Gov't Employees v. United States, 712 F.2d 931, 932 (4th Cir. 1983) 등}.

캐나다에서도 사회보장번호가 널리 개인의 식별자로 사용되는 문제가 지적되어 연방직원들에 대하여 사회보장번호 대신 새로운 피용자 번호를 도입하기도 하였다[75]. 그리고 오스트레일리아의 경우는 프라이버시 보호법(Privacy Act of 1988)에서 납세자 번호를 국가식별번호로 사용하는 것을 무조건 금지하고 있으며, 그리스의 경우는 국민 식별번호를 도입하였는데, 이것을 어떤 경우에도 데이터 파일의 식별번호로 사용하는 것을 금지하고 있다고 한다[76]. 그 외에 독일의 경우에도 신분증의 번호가 오용되는 것을 방지하기 위한 법률을 둠으로써 개인정보의 침해를 막기 위하여 특별한 보호조치를 규정해 놓고 있다[77].

한편 주민등록제도를 임의적 주민등록제도로 바꾸는 것이 현실적으로 어렵다고 할 때도 최소한 주민등록번호의 용도를 제한하는 규정을 두고, 주민등록번호를 정보의 통합자나 식별자로 사용하는 것을 금지하고, 주민등록번호의 제공을 거부한다고 하여 서비스의 제공이 거부되어서는 안된다는 원칙을

75) Privacy Laws & Business, February 1989, at 4, quoted in M. Spencer, 1992 And All That: Civil Liberties in the Balance 60 (1990). Access Reports, July 11, 1990, at 6.
76) M. Spencer, 1992 And All That: Civil Liberties in the Balance 60 (1990)
77) 김기중, 앞의 책.

법률에 반영할 필요가 있다.[78] 이런 점에서 볼 때 현재 국가에서 주민등록번호를 거의 모든 행정민원서류에서 본인확인을 위한 수단으로 사용하고 있는 것과, 법적 근거도 없이 국가나 신용조사기관들이 개인들의 주민등록번호 데이터베이스를 민간업체들에게 본인확인을 위한 수단으로 유료로 제공하고 있는 것은 중대한 프라이버시권 침해행위로서 중단되어야 할 것이다. 그리고 민간의 영역에서도 모든 거래에서 주민등록번호를 요구하는 관행과, 본인확인수단으로 주민등록번호를 요구하는 관행과 하다못해 무료 웹사이트에 회원가입시에도 무분별하게 주민등록번호를 요구하는 관행은 중대한 프라이버시 침해행위이므로 중단되어야 할 것이다.

요컨대 현재 우리사회에 광범위하게 퍼져있는 '주민등록번호 = 본인확인수단'이라는 생각, '주민등록번호 = 개인정보의 식별자'라는 생각은 근본적으로 잘못된 것이므로 고쳐져야 한다. 이러한 관행을 고치는 것이 자발적인 사고의 전환을 통해 이루어질 수 있을 것이라고 기대하는 것은 난망한 일이므로 다른 모든 제도가 점진적으로 개선될 수 밖에 없는 경우라도 우선적으로 주민등록번호의 보호에 관한 법률을 제정하여 먼저 이것부터 고쳐나가고 국민의 인식을 바꾸어 나가야 할 것이다. 또한 검찰과 법원에서도 주민등록번호의 누출에 대하여 중대한 프라이버시의 침해로 인식하여 강력한 처벌과 손해배상책임을 부과해야 할 것이다.

법률의 제정과 더불어 공공기관부터 무분별하게 주민등록번호를 요구하는 관행을 바로잡고 민원서류에서 불요불급한 경우를 제외하고는 주민등록번호를 사용하지 말도록 하고, 각종 데이터베이스에서도 성질에 따라 적절한 개인정보 식별자를 설정하여 주민등록번호를 개인정보식별자에서 제외시켜 나가는 작업을 추진해야 할 것이다. 그리고 민간영역에 대해서도 공정거래위원회나 통신위원회를 비롯해서 각급 기관에서 적절한 계도를 통해서 민간거래에서 주민등록번호를 사용하고 있는 실태를 파악하여 앞으로 주민등록번호를 사용하는 것을 억제, 금지시켜 나가야 할 것이다. 이를 위하여 먼저 민간부문과 공공기관에서 주민등록번호의 사용실태에 대한 조사를 벌여, 불필요

78) 김기중, 윤현식, 한국주민등록법의 개정방향

한 주민등록번호의 이용을 억제하는 작업을 시작해야 한다.

2. 전자정부[79] 추진의 문제점과 행정정보 공동이용과 전산망 통합의 문제점

가. 전자정부의 추진과 행정정보의 공동이용

김대중 정부는 전자정부 구현을 적극 추진하면서 11대 중점추진 과제[80]를

---

79) 우리 나라는 1, 2차 행정전산화사업계획(1978~1986)과, 1,2차 행정전산망사업계획(1987~1996), 제1차 정보화촉진기본계획(1996~2000)과 제2차 정보화촉진기본계획인 Cyber-Korea 21(1999~2002)과 제3차 정보화촉진기본계획인 e-KOREA VISION 2006[1](2002~2006)에 이르기까지 지속적으로 행정전산화를 포함한 '전자정부'를 추진해 왔다. 그러다가 최근 행정자치부와 정보통신부의 힘겨루기 끝에 전자정부법이 통과됨으로 인해 통일적인 법적 근거를 가진 '전자정부'가 추진되기에 이르렀다.

9) 전자정부 11대 중점추진과제

1. 정보화를 통한 민원서비스 혁신
-5대 국가주요 DB 공동활용으로 기관방문 회수 감소(5회?2회)
-전자정부 통합웹사이트 단계적 확대: 통합서비스 28종?400종
-무인증명 발급기 확대 보급: 발급대상 증명 32종
2. 전자조달(G2B)활성화
-모든 조달관련 절차를 온라인으로 단일창구에서 처리
-BPR, ISP 후 8월까지 전자조달 시스템 구축 완료
-조달절차 25% 감축, 조달품목 분류체계 세분화?표준화
3. 4대 사회보험 정보연계서비스
-4대 보험공단 정보시스템을 연계하여 one-stop 서비스 구현
-공통정보를 한 곳에서 공동관리
-7월부터 서비스 제공 추진
4. 인터넷을 통한 종합국세서비스
-국세관련 민원업무를 모두 안방에서 처리
-4월부터 부분서비스, 10월부터 본격 서비스
5. 국가 재정정보시스템 구축
-모든 재정업무를 정보시스템에 의해 자동으로 연결 처리
-전자고지(e-mail), 전자납부(인터넷 뱅킹), 전자이체 기반
-복식부기, 발생주의 회계 도입 및 9개 결산서 통합
6. 시/군/구 행정 종합정보화
-2단계 11개 업무 개발착수(2001.11)
-2단계 시범서비스 실시: 서울 양천구 등 5개 시군구(2002.10)
7. 전국단위 교육행정 정보시스템 구축
-16개 시도 교육청을 중심으로 10대 교육행정업무 연계 처리
-학부모 등 교육수요자에게 인터넷으로 정보 제공
-전국 어디서나 교육관련 증명서 발급
8. 표준인사관리 시스템 구축

발표하였다. 이를 보면 조만간 5대 국가주요 데이터베이스망(주민전산망, 부동산 전산망, 자동차 전산망, 기업전산망, 세금전산망)을 공동활용하는 시스템이 구축될 전망이고, 4대 사회보험 정보시스템이 연계될 전망이다. 그리고 전국적인 교육행정 정보시스템을 구축하여 교육행정업무를 전산처리할 방침이라고 한다. 나아가 이 모든 것들을 아우르는 범정부 통합전산센터를 운영하겠다고 한다.

정부는 이러한 통합전산망을 구축하기 위하여 2001. 3. 28. '전자정부구현을 위한 행정업무 등의 전자화 촉진에 관한 법률'(이하 '전자정부법'이라고 줄여서 부름)을 통과시켜 전자정부 실현을 위한 법적 근거 및 행정정보의 공동이용에 관한 법적 근거를 마련하고 있다.

그런데 현재 진행되고 있는 전자정부는 매우 위험스러운 이념에 기초하고 있으며, 국민의 프라이버시 보호와 민주주의와 인권보호의 측면에서 많은 문제를 안고 있기에 시급한 방향전환이 필요하다.

나. 전자정부의 이념에 대한 비판

(1) 전자정부의 이념[81]

-전체 공무원의 인사 DB 구축, 활용
-인사관리시스템의 행정기관간 중복투자 방지
9. 전자결재 및 전자문서유통
-문서관리업무 전반을 전자화
-전자조달, 인사 등 다른 전자정부 서비스와 호환: 연계표준안 마련(2002.4)
10. 전자 서명,전자 관인 시스템 구축
-2002년까지 1,000만명의 국민이 전자서명 이용
-무선 전자 서명 인증서비스 제공
-모든 시중은행과 증권사에서 공인 전자 서명 사용토록 유도
11. 범정부 통합전산 환경 구축
-정보통신부, 행정자치부, 기획예산처 3개 기관 공동 주관
-BPR -> ISP -> 통합전산센터 구축으로 단계적 추진

81) 정부가 펴낸 전자정부에 대한 해설자료에서는 전자정부의 미래상으로 ① '문서의 생산에서 보존까지 전자화를 통한 종이없는 행정, 전자화된 행정정보가 물 흐르듯 유통되는 신속한 행정, 행정정보의 축적 활용을 통한 지식행정'등에 의한 '생산성 있는 행정', ② '국민욕구를 충족시키는 공무원의 정보기술 이용 일상화'와 '주민들의 인터넷 활용 등 정보생활화를 지원'을 통한 '세계에서 컴퓨터를 가장 잘 활용하는 정부', ③ '국민의 안방으로 찾아가는 전자민원서비스, 구비서류 없이 한번만 신청하면 되는 간편한 서비스, 빠르고, 편리하며, 투명한 서비스를

전자정부법에 의하면 다음과 같은 7가지의 전자정부의 운영 및 구현원칙을 전자정부의 이념으로 제시하고 있다.

① 국민편익중심의 원칙(법 제6조) : 행정기관의 업무처리과정은 민원인이 부담하여야 할 시간과 노력이 최소화되도록 설계되어야 한다.

② 업무혁신 선행의 원칙(법 제7조) : 행정기관은 업무를 전자화하고자 하는 경우에는 미리 업무처리과정 전반을 전자적 처리에 적합하도록 혁신하여야 한다.

③ 전자적 처리의 원칙(법 제8조) : 행정기관의 주요 업무는 전자화되어야 하며, 전자적 처리가 가능한 업무는 특별한 사유가 있는 경우를 제외하고는 전자적으로 처리되어야만 한다.

④ 행정정보공개의 원칙(법 제9조) : 행정기관이 보유·관리하고 있는 행정정보로서 국민생활에 이익이 되는 행정정보는 법령의 규정에 의하여 공개가 제한되는 경우를 제외하고는 인터넷을 통하여 적극적으로 공개되어야 한다.

⑤ 행정기관 확인의 원칙(법 제10조) : 행정기관은 특별한 경우를 제외하고는 행정기관간에 전자적으로 확인할 수 있는 사항을 민원인에게 확인하여 제출하도록 요구하여서는 안된다.

⑥ 행정정보공동이용의 원칙(법 제11조) : 행정기관은 자신이 수집·보유하고 있는 행정정보를 이를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 안된다.

⑦ 개인정보보호의 원칙(법 제12조) : 행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용하지 못한다.

즉, 전자정부법에 의하면 전자정부가 추구하는 바는 업무의 혁신과 전자적 처리, 행정정보의 공동이용을 통해 행정의 효율성을 강화하고, 국민편익을 우선하고, 필요한 정보는 행정기관이 확인함으로써 국민의 편의를 도모하고, 행정정보의 공개를 통하여 민주적인 정부를 지향하겠다는 것이다. 얼핏 보면

피부로 느끼는 행정'을 통한 '언제, 어디서, 누구에게나 한번에 서비스하는 정부', ④ '누구나 쉽게 정부로부터 풍부한 행정·생활정보 획득, 국민과 공무원이 언제나 대화하는 빠른 네트워크'를 통한 '국민과 하나가 되는 민주적인 정부'를 제시하고 있다(행정자치부가 펴낸 '전자정부법의 이해와 해설', 2001).

전자정부의 목표는 타당해 보이나 아래에서 보는 바와 같이 매우 심각한 문제를 안고 있다.

(2) 전자정부의 이념인 효율성에 대한 비판

전자정부가 궁극적으로 지향하는 바는 '문서의 생산에서 보존까지 전자화를 통한 종이없는 행정, 전자화된 행정정보가 물 흐르듯 유통되는 신속한 행정, 행정정보의 축적 활용을 통한 지식행정'을 통한 '생산성 있는 행정'이라고 한다.

전자정부법에서도 이를 구체화하여 '행정기관은 업무를 전자화하고자 하는 경우에는 미리 업무처리과정 전반을 전자적 처리에 적합하도록 혁신하여야 한다'는 업무혁신 선행의 원칙(법 제7조)과, 행정기관의 주요 업무는 전자화되어야 하며, 전자적 처리가 가능한 업무는 특별한 사유가 있는 경우를 제외하고는 전자적으로 처리되어야만 한다는 전자적 처리의 원칙(법 제8조)과, 행정기관은 자신이 수집·보유하고 있는 행정정보를 이를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 안된다는 행정정보공동이용의 원칙(법 제11조)을 규정하고 있다.

즉, 되도록 문서를 없애고 문서대신 전자적 정보처리(digital 정보처리)를 하여야 하며, 되도록 정보처리는 자동화할 것이며, 이러한 효율성의 증대를 위하여 그리고 민원인의 편의를 위하여 되도록 행정정보를 공유하고, 행정기관이 직접 정보를 확인하겠다는 것이다.

얼핏보면 이는 문서의 감축(paperless)을 통한 물자절약과 처리과정의 전자화를 통한 효율성의 증대, 자의적이고 인위적인 인적요소의 개입을 배제함으로써 처리과정의 객관화와 공정성의 확보, 행정정보의 공동이용을 통한 민원인의 불편의 해소라는 긍정적 효과를 지향하고 있는 것으로 보인다. 그러나 이를 뒤집어 보면 여기에는 다음과 같은 위험이 도사리고 있다.

첫째, 문서의 감축과 업무처리의 전산화는 수집되는 정보의 디지털화를 의미한다. 이러한 정보의 디지털화는 기존의 개인정보의 수집과는 다른 차원의 위험을 내포하고 있다. 예컨대 기존에는 사회보장과 관련하여 개인의 정보를 사회보장 수급자 대장이라는 종이문서에 수록했었는데, 이것이 문서의 감축에 의하여 디지털화될 경우 전자와 후자는 똑 같은 개인정보의 수집이라 할지라도 질적인 차이가 있는 것이다.

둘째, 업무처리의 전산화는 자동화된 판단을 의미하는데, 자동화된 판단은 오류의 가능성이 많으며, 개인의 항변이 봉쇄되며, 객관화된 수치나 범주(자의적인 구별범주로 예컨대 소득수준, 나이, 출신지역, 인종, 전과자 여부 등)에 의한 판단은 인간을 대상화시키고 차별과 배제를 영속화하는 등 많은 문제를 야기한다.

셋째 행정정보의 공동이용은 정보의 통합을 통하여 국민에 대한 국가권력의 우월적인 정보축적으로 인한 국가의 국민감시와 인권침해의 위험을 가중시키고, 수집된 정보가 맥락을 떠나 이해됨으로써 왜곡될 가능성이 높다.

(3) 전자정부의 이념인 편리성에 대한 비판

한편 전자정부는 국민에 대한 편리한 전자민원 서비스, 원스탑 서비스를 지향한다고 한다. 전자정부법에서도 행정기관은 특별한 경우를 제외하고는 행정기관간에 전자적으로 확인할 수 있는 사항을 민원인에게 확인하여 제출하도록 요구하여서는 안된다는 행정기관 확인의 원칙(법 제10조)이나, 행정기관의 주요 업무는 전자화되어야 하며, 전자적 처리가 가능한 업무는 특별한 사유가 있는 경우를 제외하고는 전자적으로 처리되어야만 한다는 전자적 처리의 원칙(법 제8조)이나, 행정기관은 자신이 수집·보유하고 있는 행정정보를 이를 필요로 하는 다른 행정기관과 공동이용하여야 한다는 행정정보의 공동이용의 원칙을 두고 있다.

그러나 앞서 효율성에 대한 비판에서도 언급한바 있지만, 민원인에 대한 편리한 서비스의 제공이라는 원칙 속에는 많은 위험이 도사리고 있다.

첫째, 편리한 전자민원 서비스의 제공은 그 과정에서의 개인정보의 침해 위험을 가져온다.

둘째, 원스탑 서비스의 지향은 개인정보의 통합을 전제하는바 이는 편리함을 넘어서는 민주주의와 인권침해의 위험을 초래할 수 있다.

셋째, 앞서 본 것처럼 행정정보의 공동이용은 국가의 국민감시와 인권침해의 위험을 가중시킨다.

넷째, 행정기관 확인의 원칙도 행정기관간의 개인정보의 공동활용과 이로 인한 개인정보의 통합을 가속화시킴으로서 국민감시와 인권침해의 위험을 가중시키게 된다.

다. 바람직한 전자정부의 이념

전자정부는 분명 행정정보화를 통한 비용의 절감, 투명한 행정을 통한 부패의 방지, 국민에 대한 편리한 서비스의 제공, 정보의 공개와 국민의 행정참여를 촉진함으로써 민주주의의 실현에 도움이 될 수 있다. 그러나 한편 행정의 효율성이나 국민에 대한 편리한 서비스의 제공만을 강조할 경우에는 민주주의와 인권에 대한 침해요소가 될 수도 있다. 따라서 전자정부를 추진할 때에는 이러한 양자를 적절히 조화시켜 나갈 필요가 있다. 그렇기 때문에 전자정부를 추진함에 있어 견지해야 할 원칙을 분명히 하고 적절한 법적 제도적 장치를 마련하는 것이 중요하다. 그렇다면 전자정부를 추진할 때 지켜야 할 바람직한 원칙은 무엇일까? 그것은 다음과 같은 것이 되어야 할 것이다.

(1) 민주주의와 인권의 최우선 원칙

민주주의와 인권의 보호는 국가의 존립기반이기 때문에 무엇보다도 우선되어야 할 원칙이다. 따라서 국가의 국민에 대한 정보의 수집은 민주주의와 인권의 보호라는 측면에서 적정한 수준을 유지해야 하고, 전자정부의 추진도 이러한 민주주의와 인권보호라는 최우선의 원칙에 종속하는 것이어야 한다. 특히 정보통신기술과 바이오테크놀로지 등의 발달로 인한 국가의 정보수집과 분석, 감시능력의 확장으로 국가의 국민에 대한 정보수집에 따른 민주주

의와 인권침해의 가능성이 그 어느 때보다도 커진 오늘날에는 국가의 국민에 대한 정보수집이 국민의 인권과 민주주의에 미치는 영향을 면밀히 분석할 필요성이 크다 할 것이다.

(2) 국가권력으로부터 독립성을 가진 기구에 의한 제어의 원칙

오늘날 국가의 국민에 대한 정보의 수집이나 전자정부의 추진은 단순히 개인정보의 침해나 프라이버시의 침해의 문제를 넘어서서 인권과 민주주의에 대한 위협요소로 될 수 있는 잠재적인 가능성이 있다. 이와 같이 국가의 국민에 대한 정보의 수집이나 전자정부의 추진이 인권과 민주주의에 대한 위협요소로 되어 가고 있기 때문에 이러한 국가의 활동에 대한 제어는 행정부의 일개부처가 아닌 국가권력으로부터 독립성을 가진 기구에 의하여 이루어질 필요가 있는 것이다. 이는 인권의 문제이기 때문에 국가권력으로부터 독립성을 가진 기구에 의하여 다루어져야 하며, 민주주의의 문제이기 때문에 민주주의의 원리에 입각하여 권력분립에 따른 독립성을 가진 기구에 의하여 이루어져야 하는 것이다.

(3) 잠재적 영향평가의 원칙

국가의 개인정보의 수집이나 처리를 포함하여 전자정부를 추진함에 있어서 그러한 개인정보의 수집이나 처리, 전자정부의 추진이 가져올 수 있는 인권과 민주주의에 대한 영향, 프라이버시 침해의 가능성에 대한 영향을 평가하는 것이 필수적이다. 이러한 영향평가는 해당 부처에 의해서도 이루어져야 하겠지만, 국가권력으로부터 독립성을 가진 기구에 의하여 이루어져야 할 것이다.

이러한 영향평가를 할 때는 다음의 점을 고려해야 한다. 첫째, 행정의 효율성이나 편의성보다는 국민의 편의성이 우선되어야 하고, 국민의 편의성보다는 민주주의와 인권, 프라이버시의 보호가 우선되어야 한다. 둘째, 영향평가는 현재적인 영향평가 뿐만이 아니라 기술의 발전에 따른 잠재적인 영향까지도 평가되어야 하며, 기술의 발전에 따른 잠재적인 위험을 방지하기 위

한 방안이 마련되어야 한다.

(4) 자동처리과정을 통한 평가시의 고려사항

자동처리과정을 통하여 평가를 할 경우에는 해당 정보가 오류일 가능성, 해당 정보주체의 항변권의 보장을 위한 방안, 해당 정보에 대한 정확성의 확보를 위한 방안, 자동처리과정이 갖는 비민주적인 요소에 대한 고려가 충분히 이루어져야 한다. 이는 정보의 자동처리가 안고 있는 근본적인 위험요소에 대한 최소한의 안전보장책이라고 할 수 있다.

(5) 정보의 디지털화와 생체정보의 처리 등과 같은 민감한 정보의 처리

정보를 디지털화할 경우는 정보체계의 개방성, 다른 시스템과의 연결가능성, 오용가능성에 의하여 정보의 주체는 새로운 위험에 처하게 된다. 따라서 이러한 점을 충분히 감안하여 그에 대한 대비책이 확실하게 마련된 경우에만 영향평가를 통하여 정보의 디지털화는 허용될 수 있을 것이다. 생체정보의 처리 역시 마찬가지이다.

(6) 정보의 통합

정보의 통합이나 공동이용은 원칙적으로 허용되어서는 안될 것이다. 정보의 통합이나 공동이용은 정보의 축적을 가속화하여 국가에게 국민에 대한 지나친 감시능력을 부여하게 되며, 맥락을 떠난 정보의 이용은 인권의 침해뿐만 아니라 민주주의의 왜곡을 가져올 수도 있다. 따라서 정보의 공동이용이나 통합은 명백한 필요성이 인정되며, 그로 인하여 파생되는 민주주의와 인권침해의 가능성이 희박하고, 맥락을 떠난 정보의 오용가능성이 없는 경우에만 제한적으로 허용되어야 할 것이다.

(7) 문서의 감축은 정보수집의 축소로 이해되어야 한다

문서의 감축은 작은 정부의 실현, 국가의 과다한 정보수집의 억제로 이해되어야 한다. 문서의 감축이 정보의 디지털화와 정보의 자동처리화로 이해되

어서는 안될 것이다. 현재의 국가의 정보수집에 대하여 문서감축의 측면에서 필요성 여부와 민주주의와 인권침해의 가능성 여부 등을 심사하여 업무를 재설계하여야 할 것이다. 이를 전제할 때에만 전자정부는 성공가능성이 높아질 것이다.

라. 전자정부법의 개정방향

이상의 원칙에 입각하여 볼 때 현재 추진 중인 전자정부와 전자정부법은 근본적인 관점의 수정이 불가피하다. 구체적인 개정방향을 검토해 본다.

(1) 기본원칙의 재정비

이상에서 보다시피 현재의 전자정부법의 전자정부의 추진원칙은 민주주의와 인권보호, 프라이버시의 보호의 측면에서 많은 문제점을 안고 있다. 전자정부의 추진원칙으로 (i) 민주주의와 인권의 최우선의 원칙, (ii) 잠재적인 영향평가의 원칙, (iii) 정보수집 축소의 원칙, (iv) 자동처리와 관련된 정보주체의 보호의 원칙, (v) 민감한 정보처리에 대한 원칙 등이 명시되도록 하는 것이 좋을 것이다.

(2) 국가권력으로부터 독립한 기구에 의한 제어장치의 확립

전자정부법에 국가의 정보수집과, 분석, 이용, 전자정부의 추진과 관련하여 국가권력으로부터 독립한 기구가 이를 제어할 수 있도록 규정을 두는 것이 필요하다. 이를 위하여 전자정부법에서 반감시위원회를 독립한 기구로서 규정하고, 여기에서 국가의 정보수집, 분석, 이용, 전자정부의 추진과 관련하여 잠재적인 영향의 평가, 침해의 구제, 의견의 제시 등을 할 수 있도록 할 필요가 있다.

반감시위원회는 국가권력으로부터 독립한 기구이므로 대통령, 국회, 대법원장이 약간 명씩을 임명하도록 하고, 지위를 보장하며, 영향평가와 침해구제를 위한 조사권과 시정요구권, 의견제시권 등을 갖도록 하는 것이 좋을 것이다. 프라이버시 위원회의 모델은 유럽의 여러 나라나 캐나다, 오스트레일

리아 등에 설치된 프라이버시 위원회가 될 수 있을 것이다.

(3) 잠재적인 영향평가제의 도입

국가의 정보수집, 전자정부의 추진과 관련하여 그것이 민주주의, 인권, 프라이버시에 미치는 잠재적인 영향을 평가하는 제도를 도입할 필요가 있다. 잠재적인 영향평가제는 현재적인 영향만을 평가하는 것이 아니라 잠재적인 영향까지도 평가하는 제도이다. 잠재적인 영향평가의 결과가 문제가 있는 것으로 나올 경우에는 그 제도는 시행을 해서는 안될 것이다.

(4) 자동처리에 의한 평가에 관한 규정의 신설

자동처리과정을 통한 평가가 허용되는 경우는 그것이 미치는 영향이 미미한 경우로서 자동처리과정을 통하지 않은 다른 평가에 대하여 보조적으로 이루어지는 경우로 제한되어야 한다. 이 경우에도 해당 정보가 오류일 가능성, 해당 정보주체의 항변권의 보장을 위한 방안, 해당 정보에 대한 정확성의 확보를 위한 방안이 보장되어야 한다. 이러한 원칙이 전자정부법에 규정되어야 한다.

(5) 정보의 디지털화와 생체정보의 처리 등과 같은 민감한 정보의 처리에 관해서는 당사자의 특별한 동의를 받도록 하거나, 정보의 확장가능성을 차단할 수 있는 안전장치의 보장이 선행되어야 한다는 점이 분명하게 규정되어야 한다

정보의 디지털화가 허용되는 경우를 제한적으로 인정하되, 충분한 영향평가가 이루어져야 할 것이다. 그리고 정보의 디지털화가 허용되는 경우에는 정보체계의 개방이나 다른 시스템과의 연결, 오용가능성 등에 대한 대비 방안이 마련되도록 해야 한다. 생체정보의 처리 역시 마찬가지이다. 이 점에 대해서는 전자정부법에 특별한 규정을 두어야 할 것이다. 그리고 이러한 정보에 대해서는 원칙적으로 정보주체의 거절권을 인정해야 할 것이다.

(6) 행정정보의 공동이용 및 행정정보의 통합의 제한

그런데 앞서 본 것처럼 원칙적으로 정보의 통합이나 공동이용은 허용되어서는 안되며, 다만 정보의 공동이용이나 통합은 명백한 필요성이 인정되며, 그로 인하여 파생되는 민주주의와 인권침해의 가능성이 희박하고, 맥락을 떠난 정보의 오용가능성이 없는 경우로만 제한적으로 허용되어야 할 것이다.

그런데 전자정부법은 행정기관은 1) 민원사항의 처리를 위하여 필요한 행정정보, 2) 통계정보 · 문헌정보 등 행정업무의 수행에 참고가 되는 행정정보, 3) 공공기관의 개인정보보호에 관한 법률 제10조제2항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보, 4) 정보화촉진기본법 제8조의 규정에 의한 정보화추진위원회가 행정기관간 공동이용이 필요하다고 인정하는 행정정보는 이를 공동이용[82]하여야 한다고 규정하고 있어서 많은 문제점을 안고 있다. 이 규정들을 약간 자세히 검토해 본다.

우선 민원사항의 처리를 위하여 필요한 행정정보는 공동이용하여야 한다는 규정은 너무나도 문제가 많은 규정이다. 행정정보의 공동이용은 어떤 행정기관이 수집한 개인정보를 다른 행정기관에서 이용하는 것으로서 이는 개인정보를 수집한 목적범위 외로 이용하는 것이며, 이를 통하여 개인정보가 통합되게 되는 것이다. 따라서 이는 원칙적으로 허용되어서는 안되는 것이다. 그런데 '민원사항의 처리를 위하여 필요한 행정정보'를 공동이용하도록 허용하고 있는 것은 원칙의 포기와 다름없다.

다음으로 공공기관의 개인정보보호에 관한 법률 제10조 제2항의 규정에 의하여 다른 기관에 제공할 수 있는 정보처리의 경우도 지나치게 포괄적인 예외사유이다. 이 규정에서는 원칙적으로 법률의 규정이 있는 경우에만 개인정보를 다른 기관에 제공할 수 있다고 하면서도 소관업무를 수행하기 위하

82) 그 한 예로 정부는 현재 올해 안으로 아래의 20개 행정정보를 민원을 위하여 공동이용하기로 하였다. 주민등록정보, 전산호적정보, 개별공시지가확인서, 토지(임야)대장, 사용승인서, (일반/집합)건축물대장, 토지등기부등본, 건물등기부등본, 자동차등록원부(갑/을), 이륜자동차사용신고필증, 건설기계등록원부(갑/을), 사업자등록증명원, 휴업사실증명원, 폐업사실증명원, 법인등기부등본, 납세증명서, 지방세납세증명서, 자동차세납세증명서, 소득금액증명, 납세사실증명원.

여 당해 처리정보를 이용할 상당한 이유가 있는 경우와 같은 광범위한 예외 규정[83]을 두어 사실상 행정의 목적을 위해서라면 언제라도 개인정보를 다른 기관에 제공할 수 있는 것으로 규정하고 있다. 이런 규정 하에서라면 공공기관이 보유하고 있는 개인정보는 행정목적을 달성하기 위해서라면 거의 무제한적으로 공동이용이 가능한 것이 된다. 공공기관의 개인정보에 대한 보호는 행정의 목적이라는 관점이 아닌 개인정보의 침해의 정도라는 관점에서 기준이 마련되어야 한다. 더구나 최근에는 자동처리되는 데이터베이스로 인하여 개인정보의 공유는 과거와는 그 파급력에서 차이가 난다. 이 규정도 좀더 구체적으로 허용사유를 열거하는 방식으로 바뀌어야 한다.

그리고 법은 행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다는 규정을 두어서(법 제11조), 행정정보의 공동이용을 강제하고 있다. 그러나 행정기관은 원칙적으로 동일한 내용의 정보라도 각각의 목적에 따라 정보를 따로 수집해야 한다. 이것은 개인정보 수집에 있어서 목적특정성의 원칙에 의한 것이다. 이 규정은 이런 원칙을 근본적으로 거스르고 있는 규정이다. 특히 행정정보의 경우는 반드시 동일한 내용의 정보가 겹칠 수 밖에 없으며, 우리나라의 경우 행정기관이 불필요한 개인정보를 요구하는 경우가 많기 때문에 겹치는 범위는 더욱 더 광범위하다. 법의 동일한 행정정보의 공동처리의 원칙은 행정정보의 통합을 가속화시킬 것이며, 개인정보의 목적특정성의 원칙을 형해화시킬 것이다.

한편 법은 정보화촉진기본법 제8조의 규정에 의한 정보화추진위원회가 행정기관간 공동이용이 필요하다고 인정하는 행정정보를 공동이용할 수 있다고 규정하고 있는비 이것도 문제이다. 이는 행정부가 행정정보의 공동이용의

83) 예외조항은 1) 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, 2) 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우, 3) 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, 4) 통계작성 및 학술연구등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우, 5) 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, 6) 범죄의 수사와 공소의 제기 및 유지에 필요한 경우, 7) 법원의 재판업무수행을 위하여 필요한 경우임.

범위를 정할 수 있게 하고 있는 것이어서, 민주주의와 인권보장의 기본원리에도 정면으로 위배되는 것이다.

행정정보의 공동이용의 범위에 대하여 법은 아무런 규정을 두고 있지 않다. 행정정보의 공동이용의 범위는 개인정보의 통합의 범위를 결정하는 중요한 문제이기 때문에 반드시 법에 규정을 두어야 한다. 특히 개인정보의 식별자의 기능을 하는 정보에 대해서는 특별한 보호조치가 마련되어야 한다. 개인정보의 식별자 기능을 하는 정보를 통하여 동일한 행정부처 내에서도 분리되어 수집되어야 할 정보가 통합될 수 있기 때문이다. 행정정보의 공동이용은 그 범위가 최소한으로 제한되어야 하며, 행정정보의 공동이용에 대해서는 3권분립의 원칙에 의거한 반감시위원회의 통제가 있어야 한다. 행정정보의 공동이용의 범위를 확정하는 문제에 대해서는 그것이 미칠 인권침해의 가능성 등을 고려하여 반감시위원회의 사전의견을 듣도록 제도를 보완해야 한다.

정부는 전자정부를 추진하면서 국민의 개인정보를 담고 있는 전산망을 통합할 계획을 발표한 바 있다. 예컨대 주민전산망과 부동산전산망, 자동차전산망, 교육전산망, 납세와 관련한 전산망, 4대보험 전산망 등이 통합될 경우 그것이 가져올 개인정보의 침해와 인권침해의 문제는 여간 심각한 것이 아니다. 통합되는 전산망에 포함된 개인정보가 무엇인지를 검토하고, 각각의 전산망이 수집하고 있는 개인정보의 수집목적이 통합되어도 되는 것인지를 검토해야 한다. 특별한 법적 근거도 없이 전자정부구현을 위한 행정업무 등의 전자화 촉진에 관한 법률의 행정정보의 공동이용 규정을 근거로 각 전산망을 통합하는 것은 위헌적이고 위법한 것이 아닐 수 없다.

(7) 정보수집 심사위원회

현재의 국가의 정보수집과 관련하여 그 필요성 여부와 민주주의와 인권침해의 가능성 여부 등을 심사하여 업무를 재설계하여야 할 것이다. 이를 위하여 프라이버시 위원회와 문서감축위원회의 협력으로 정보수집 업무에 대한 재설계가 이루어질 수 있도록 하여야 할 것이다.

마. 전자정부의 성공의 선결조건

이상에서 보았듯이 현행 전자정부법과 그에 기초한 전자정부는 프라이버시의 보호, 민주주의와 인권의 보호라는 측면에서 보았을 때 매우 심각한 문제점을 안고 있다. 따라서 법적 제도적 장치가 보완되지 못할 경우 전자정부는 정부가 주창하고 있는 바와는 달리 민주주의와 인권보장에 중대한 위험요소로 작용할 수도 있다. 현재 제기되고 있는 문제점들이 선결되지 않을 경우 전자정부는 국민의 지지를 받지 못하여 실패하거나, 국민에 대한 거대한 감시기구로 민주주의의 저해요소가 될 수도 있다.

3. 국가의 개인정보의 수집, 이용에 관하여 - 공공기관의 개인정보 보호에 관한 법률의 문제점

가. 개관

공공기관의 개인정보보호에 관한 법률은 공공기관이 컴퓨터에 의하여 처리하는 개인정보의 보호에 대한 법률이다. 공공기관의 개인정보보호에 관한 법률은 OECD의 개인정보처리에 대한 원칙에 근거하여 제정된 것인데, 개인정보주체의 권리가 각종 예외규정으로 형해화되어 있다.

나. 문제점과 개정방안

(1) 적용범위의 확장

법은 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 공공기관의 개인정보보호에 관한 법률이 정하는 바에 의한다(제3조 제1항)라고 하여 공공기관의 컴퓨터에 의하여 처리되는 개인정보만을 그 보호의 대상으로 하고 있다. 현재 대다수의 개인정보들이 컴퓨터에 의하여 처리되고 있기는 하지만, 어차피 공공기관이 개인정보를 수집, 활용함에 있어서 필요한 사항들에 대하여 규정하고 있는 것이므로 적용범위를 컴퓨터 처리정보로 국한시키지 말고 포괄적으로 규정해야 한다.

(2) 적용배제범위의 모호함

국가안전보장과 관련된 정보분석을 목적으로 수집 또는 제공 요청되는 개인정보의 보호에 관하여는 이 법을 적용하지 아니한다(제3조 제2항)고 하여, 이러한 정보에 대해서는 전면적으로 공공기관의 개인정보보호에 관한 법률의 적용을 배제하고 있으나, (i) 국가안전보장이라는 것이 지나치게 포괄적이며, (ii) 오히려 이런기관의 감시와 개인정보 침해의 문제가 더 심각하며, (iii) 이러한 정보에 대하여도 전면적으로 법의 적용를 배제하는 것보다는 일부 조항을 개별적으로 배제하여야 한다.

(3) 개인정보 수집의 범위

개인정보의 수집에는 제한을 두어야 하고, 어떠한 개인정보도 합법적이고 공정한 절차에 의하여 수집하여야 한다. 그리고 가능한한 정보주체로부터 직접 정보를 수집하여야 한다. 이러한 원칙에 입각하여 공공기관의 개인정보 수집은 법령에 정해진 업무를 수행함에 있어서 개인정보의 수집이 필요한 경우, 그 목적달성에 필요한 범위 내에서 목적달성에 가장 적절한 개인정보만을 수집해야 한다. 미국의 프라이버시 보호법(Privacy Act of 1974; 5 USC Section 552a)의 (e)의 (1)은 이러한 원칙을 천명하고 있다.

그리고 개인정보를 수집할 때에는 개인정보주체에게 (i) 개인정보 수집의 근거, (ii) 개인정보의 제공이 강제되는 것인지 여부, (iii) 개인정보 수집의 목적과 개인정보의 용도, (iv) 보유기간, (v) 정보를 제공하지 않을 경우 개인에게 미치는 효과 등에 대하여 알려야 한다는 조항을 두어야 한다.[84]

개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보는 아예 수집을 금지하거나, 법률에 규정을 두고 제한적으로만 허용하여야 할 것이다. 이런 관점에서 공공기관의 개인정보보호에 관한 법률 제4조[85]를 보면, 개인

84) 미국의 프라이버시 보호법 Sec. 552a (e) (3)

85) 제4조 (개인정보의 수집) 공공기관의 장은 사상 · 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는

정보 수집의 자유를 원칙으로 해 놓고, 사상, 신조 등 양심의 자유와 관련되어 있는 정보들(이런 정보들은 수집해서는 안되는 정보이거나, 법률의 규정이 있는 경우에만 수집이 허용될 정보들이다)에 대해서만 동의나 법률의 근거를 요하는 것으로 규정하고 있어서 큰 문제를 안고 있다. 한편 법에서 다른 법률의 규정이 있는 경우에만 개인정보를 수집할 수 있다고 규정하고 있는데, 여기에서의 법률은 형식적 의미의 법률, 즉, 법률의 형식을 띤 것만을 의미하는 것으로 해석해야지, 시행령이나 시행규칙 등은 여기에 해당하지 않는 것으로 해석해야 할 것이다.

(4) 개인정보화일의 보유범위와 사전통보

"개인정보화일"이라 함은 특정개인의 신분을 식별할 수 있는 사항에 의하여 당해 개인정보를 검색할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 컴퓨터의 자기테이프·자기디스크 기타 이와 유사한 매체에 기록된 것을 말한다(법 제1조 제4호). 따라서 개인정보화일의 보유범위란 곧 공공기관이 개인정보를 보유할 수 있는 범위를 의미한다. 결국 공공기관의 개인정보화일의 보유범위는 공공기관이 개인에 대한 정보를 어느 범위까지 확보할 수 있는 것인지를 정하는 것이므로, 그것은 법률로 정해진 업무수행에 적합한 범위 내에서만 보유할 수 있어야 할 것이다.

이러한 관점에서 공공기관의 개인정보보호에 관한 법률 제5조[86]는 공공기관은 법률에 정해진 업무를 수행함에 있어서 개인정보의 수집이 필요한 경우에는 그 목적달성에 필요한 범위 내에서 목적달성에 가장 적절한 개인정보화일만을 보유할 수 있다는 규정으로 바꾸어야 할 것이다. 또한 이 경우에도 수집하는 개인정보가 적절한지에 대한 반감시위원회의 통제권이 인정되어야 한다.

그리고 수집된 개인정보의 보유기간과 목적을 달성한 개인정보들의 폐기

경우에는 그러하지 아니하다.

86) 제5조 (개인정보화일의 보유범위) 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보화일을 보유할 수 있다.

에 대해서도 규정을 두어야 한다.

(5) 보유정보화일에 대한 공개의 원칙

법은 보유정보화일에 대하여 공공기관 상호간의 내부적인 공개의 원칙을 천명하고 있는데, 그 내용을 보면 부실하기 짝이없다. 현행 법령은 공개의 범위도 제한적이며, 예컨대 개인정보 개인정보화일보유에 관한 법령상 근거가 있는 경우에만 법령상의 근거를 공개하도록 하고, 기간의 정함이 있는 경우에만 기간을 공개하는 등 많은 문제점을 안고 있다(법 제6조 제1항, 시행령 제5조).

그리고 법 제6조 제2항과 시행령 제6조에 의하면 개인정보화일 공개에 대하여 광범위한 예외사유를 두고 있는데, 여기에도 문제의 소지가 있는 조항들이 많이 있다.

법 제6조 제2항의 제1호 국가의 안전 및 외교상의 비밀 기타 국가의 중대한 이익에 관한 사항을 기록한 개인정보화일이란 규정은 지나치게 추상적이어서 문제가 있으며, 제2호 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보화일, 제3호 조세범처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한 사항을 기록한 개인정보화일의 경우는 그 범위가 지나치게 넓고, 이와 같은 국가공권력의 행사에 대해서는 비밀의 유지도 필요하지만, 그와 함께 이에 대해서는 더욱 더 엄격한 통제가 필요하고, 또한 이 경우는 특히 잘못된 정보로 인한 개인의 사생활의 침해가 치명적일 수 있다는 측면에서 오류의 정정이 필요하므로, 정보의 공개와 비밀의 유지 사이에 적절한 조화를 이룰 수 있는 방안이 필요하다. 제4호 컴퓨터의 시험운영을 위하여 사용되는 개인정보화일의 경우 역시 개인정보 유출의 위험을 감안한다면 시험운영을 위해 개인정보화일을 사용한다는 것이 문제의 소지가 있는 조항이다. 제6호의 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보화일의 경우는 그것이 구체적으로 어떤 개인정보화일을 의미하는 것인지도 애매하고(국민들의 개인정보화일을 내부적으로 사용하는 것을 의미하는 것인지, 아니면 공공기

관의 내부성원들의 개인정보화일을 의미하는 것인지), 개인정보화일의 공개가 필요한 이유가 무엇인지를 망각한 조항이다. 제7호의 대통령령이 정하는 일정한 수 이내의 정보주체를 대상으로 하는 개인정보화일의 경우는 대통령령에서 일정한 수를 1000명으로 구체화하고 있는데, 이것 역시 지나치게 자의적인 규정으로서 법의 취지를 몰각시키는 규정이 아닐 수 없다.

예컨대 미국의 프라이버시 보호법은 법의 집행을 위하여 수사기록에 축적된 정보로서 정보의 공개로서 연방법에 의하여 부여된 권리, 특권, 혜택이 부정되거나, 정보의 유지나 공개로 인하여 비밀이 유지될 것이라는 명백한 약속 아래 정부에 정보를 제공한 사람의 신원이 밝혀질 정보, 대통령이나 법에서 정하고 있는 요인들의 경호와 관련되어 유지되는 정보, 통계목적만으로 법에 의하여 유지되는 정보, 연방 민간 고용, 대, 연방계약의 적합성, 적정성, 자격을 판단할 목적만으로 수집된 수사자료, 연방서비스의 채용이나 승진의 자격을 결정하는 것만을 목적으로 사용되는 시험에 관한 정보로서 공개되면 시험이나 평가의 공정성이나, 목적에 야합이 개입될 수 있는 정보, 군대의 장래의 승진 관련된 판단을 하기 위한 평가정보로서 비밀을 유지해 주겠다는 명백한 약속 아래 정부에 정보를 제공한 자의 신분이 밝혀질 정보에 대해서만 개인정보화일의 공개를 제한하고 있다.

(6) 개인정보화일의 공고

1980년의 OECD의 이사회 권고인 프라이버시 보호원칙은 개인정보의 수집시에 개인정보의 존재, 성질 및 그 주요 이용 목적을 공개해야 한다는 원칙을 천명하고 있다. 이 원칙이 구체화 된 것이 개인정보화일의 공고제도이다. 개인정보화일의 공고는 공공기관의 개인정보의 보유범위에 대한 정보공개로서 개인정보의 열람청구와 정정청구의 수단이 된다는 측면에서 매우 중요한 역할을 한다. 이때 공고되어야 할 내용으로는, 정보시스템의 이름, 정보시스템에 정보가 포함되어 있는 사람들의 범주, 정보시스템에 포함되어 있는 정보의 범주, 정보시스템에 포함되어 있는 정보의 모든 통상적인 사용, 이용자의 범주와 이용의 목적, 정보의 저장과 복구와 접근통제, 보유, 폐기의 정책과 지침, 정보시스템의 책임자의 직함과 근무처 주소, 자신에 관한 정보를

포함하고 있는 정보시스템에 대한 정보주체의 요청에 대하여 통지해 줄 기관과 절차, 자신의 정보를 정보시스템 안에 포함하고 있는 정보시스템에 접근할 수 있는 방법, 절차, 정보의 내용에 대하여 다툴 수 있는 방법, 정보시스템 안의 정보의 출처의 범주 등이 포함되어야 한다. 이에 비하여 우리의 현행법상의 개인정보화일의 공고는 형식적이고 부실하기 그지없다.

그리고 법은 관계중앙행정기관의 장은 제6조제1항의 규정에 의한 통보를 받은 때에는 대통령령이 정하는 바에 따라 통보받은 사항을 연 1회 이상 관보에 게재하여 공고하여야 한다고 하면서, 적정한 업무수행을 현저하게 저해할 우려가 있다고 인정되는 때에는 대통령령이 정하는 바에 따라 당해 개인정보화일에 기록되어 있는 항목의 전부 또는 일부를 공고하지 아니할 수 있다고 규정하고(법 제7조), 시행령에서는 법 제13조의 규정에 의하여 열람을 제한할 수 있는 처리정보에 해당하는 항목에 대하여는 그 항목의 전부 또는 일부를 공고하지 아니할 수 있다고 규정하여, 광범위한 제한사유를 두고, 열람을 제한할 수 있는 정보에 대하여 아예 보유여부에 대하여도 공개를 하지 않고 있어서 큰 문제이다.

(7) 개인정보의 목적외 이용의 금지 및 타 기관에의 제공의 제한

법 제10조는 다른 법률에 의하여 개인정보를 보유기관의 내부에서 이용하거나 보유기관외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화일의 보유목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니된다고 하여 개인정보의 목적외 이용과 타 기관에의 제공을 제한하고 있다.

그러나 법은 이에 대한 단서조항을 두어 단서조항에 해당하는 경우에는 당해 개인정보화일의 보유목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있다고 규정하고 있다.

그 단서조항은 1) 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, 2) 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를

이용할 상당한 이유가 있는 경우, 3) 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, 4) 통계작성 및 학술연구등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우, 5) 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, 6) 범죄의 수사와 공소의 제기 및 유지에 필요한 경우(지나치게 넓은 규정), 7) 법원의 재판업무 수행을 위하여 필요한 경우, 8) 기타 대통령령이 정하는 특별한 사유가 있는 경우(대통령령은 이 부분에 대해서는 아무런 규정을 두고 있지 않다) 등으로 구성되어 있다.

그런데 단서조항 2)의 경우는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우라고 하여, 행정의 편의를 위해서는 사실상 언제나 정보주체의 동의없이도 정보를 다른 기관에 제공할 수 있는 것으로 하고 있어서 개인정보의 목적외 이용금지 및 다른 기관에의 제공의 금지원칙을 유명무실하게 만들고 있다. 단서조항 6), 7)의 경우도 지나치게 포괄적이다. 이 경우도 영장주의나 이에 준하는 요건과 절차가 규정되어야 할 것이다. 한편 법 제10조 제2항에 의하여 제정된 시행령 제11조 제2항에 의하면 처리정보를 제공하는 보유기관의 장은 처리정보대장에 개인정보화일의 명칭, 제공받는 기관의 명칭 등을 기재하도록 하고 있는데, 제공의 근거를 법령상 제공근거가 있는 경우에만 기재하도록 한다거나, 이용기간도 이용기간이 정해져 있는 경우에만 그 기간을 기재하도록 하고 있어서 처리정보대장 작성의 취지를 퇴색시키고 있다(시행령 제11조 제2항 제4호, 제8호).

한편 미국의 프라이버시 보호법에서는 원칙적으로 정보의 공개를 금지하면서 일정한 요건하에서 정보의 공개가 허용되는 것으로 하면서 다른 기관에의 정보의 제공도 정보의 공개의 한 측면으로 다루고 있다. 이 법은 아래의 경우에 해당하지 않는 때에는 정보주체로부터 서면에 의한 동의나 요구가 있지 않고서는 다른 기관이나 어떠한 사람에게도 공개(제공 포함)하지 못하도록 하고 있다. 즉, 공개가 허용되는 경우란 (1) 공공기관의 내부에서 직무수행을 위하여 해당 공공기관의 관리나 직원이 이용하는 경우, (2) 수집된

정보의 수집목적(compatible)의 통상적인 이용으로 미리 공지된 경우(미국 내에서 이에 대해 많은 비판이 있다), (3) 인구조사 목적으로 통계청에 제공하는 경우, (4) 통계목적으로 사용하는 경우, (5) 계속 보존할 역사적 가치가 있어서 국가 문서 기록청에 제공하는 경우, (6) 법률에 규정된 활동으로서 민, 형사상의 법률의 집행을 위한 활동을 하는 기관의 장이 필요한 정보의 부분에 대하여 상세하게 정리하여 서면요청이 있는 경우, (7) 정보의 제공을 받지 아니하면 생명, 건강의 위험에 처하게 된 자에게 제공, (8) 의회의 공동위원회에 대하여 직무의 범위 내에서, (9) 법원의 명령, (10) 소비자 보고기관에서 사용하는 경우

(8) 개인정보의 열람과 정정청구

법은 정보주체는 개인정보화일대장에 기재된 범위안에서 서면으로 본인에 관한 처리정보의 열람(문서에 의한 사본의 수령을 포함)을 보유기관의 장에게 청구할 수 있다고 규정하고 있다(제12조 제1항). 이 경우 보유기관의 장은 제1항의 규정에 의한 열람청구를 받은 때에는 제13조 각호의 1에 해당하는 경우를 제외하고는 청구서를 받은 날부터 7일 이내에 열람의 허용여부, 열람일시, 장소를 결정하여 열람결정 통지서를 송부하여야 하고(령 제14조 제1항), 15일 이내에 청구인으로 하여금 당해 처리정보를 열람할 수 있도록 하여야 한다(법 제12조 제2항).

한편 보유기관의 장이 처리정보의 전부 또는 일부에 대하여 열람을 허용하지 아니하기로 결정한 때에는 그 사유와 법령상 근거 및 당해 결정에 대한 불복절차에 관한 사항을 기재한 열람제한결정서를 청구인에게 송부하여야 한다(령 제14조 제2항).

한편 법은 보유기관의 장은 열람을 청구한 청구인으로 하여금 당해 처리정보를 열람하도록 하는 것이 아래의 예외사유에 해당하는 경우에는 그 사유를 통지하고 당해 처리정보의 열람을 제한할 수 있다고 규정하고 있다.

그 예외사유로는 조세의 부과·징수 또는 환급에 관한 업무, 교육법에 의

한 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, 토지 및 주택 등에 관한 부동산투기를 방지하기 위한 업무, 증권거래법에 의한 불공정 증권거래를 방지하기 위한 업무로서 당해 업무의 수행에 중대한 지장을 초래하는 경우와, 개인의 생명·신체를 해할 우려가 있거나 개인의 재산과 기타의 이익을 부당하게 침해할 우려가 있는 경우 등을 두고 있다.

그런데 위의 예외사유들 중 조세의 부과·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 산정 등 평가 또는 판단에 관한 업무 등은 열람제한의 필요성이 있다고 볼 수 없는 경우들이다.

예컨대 미국의 프라이버시 보호법에서는 CIA의 보유 정보, 형사법의 집행을 위한 목적으로 유지되는 정보 중 개인식별 정보, 체포일, 형기, 출소일 등의 정보와 같은 것에 대해서만 열람이 제한될 뿐이다.

또한 법은 개인정보의 열람과 정정청구에 대해서는 근거규정을 두고 있지만 개인정보의 삭제청구에 대해서는 아무런 규정을 두고 있지 않아서 문제이다. 개인정보가 근거없이 수집되었을 경우 삭제청구를 할 수 있다는 조항을 명시해 놓을 필요가 있다.

(9) 처벌조항의 미비

이 법은 처벌조항에 있어서는 부실하기 짝이 없다. 정보통신망 이용촉진 및 정보보호에 관한 법률과 비교해 보더라도 확연히 드러난다. 위법한 정보의 수집, 처리, 각 의무의 위반에 대하여 민간영역보다 더 엄격한 처벌조항을 두어야 할 것이다.

(10) 구제수단의 실효성 보장

개인정보의 침해는 일단 침해가 이루어진 후에는 침해의 결과가 언제 나타날지 모른다는 특징이 있다. 따라서 신속한 권리구제가 필수적이다. 그리고 공공기관의 개인정보 보호에 대한 일반법인 본 법의 성질상, 공공기관의 개인정보 보호에 관한 구제수단이 망라적으로 입법화되어야 할 것이다. 그래서 개인정보 침해의 우려가 있는 제도의 도입시의 개인들의 정보공개권, 그러한 제도에 대한 사전적인 구제청구권까지도 보장되도록 입법이 정비될 필요가 있다.

4. 통신비밀보호의 문제

가. 정보통신망의 발달과 최근의 통신의 특징

헌법 제18조는 모든 국민은 통신의 비밀을 침해받지 아니한다고 규정하여 통신의 비밀보호와 통신의 자유를 기본권으로 보장하고 있다. 전통적으로 공적인 영역에 속하는 표현을 보호하는 것은 표현의 자유의 문제로 보고, 그 보호의 측면을 달리하여 사적인 영역에 속하는 것은 통신의 비밀과 자유의 보호라는 차원에서 보호되는 것으로 해석되어져 왔다. 그런데 오늘날은 정보통신매체의 발달과 통신수단의 발달로 인하여 통신이 과거의 우편이나 전화를 이용한 통신이 주를 이루던 시대와는 다음과 같은 점에서 큰 차이가 있다.

매체	침해의 대상	침해방법	특징
대화	대화의 내용, 상대방	녹음, 청취	미리 준비하지 않으면 침해하기 어렵다.
우편	우편의 내용, 상대방, 발송회수, 발송시점	검열	침해가 용이한 편이나 자동화하기 어려워서 시간이 많이 걸린다. 일단 발송이 된 후에는 비밀을 침해하기 어려움.
전화	통화의 내용, 상대방, 통화시간, 통화회수	감청	침해가 훨씬 용이한 편. 통화가 끝난 후에도 통화기록이 남으므로 사후적인 통신비밀 침해도 이루어짐.
이동통신	통화장소 문자메시지	감청	침해가 매우 용이함. 통화의 장소가 노출되고, 문자메시지의 경우는 통화의 내용이 저장됨.
전기통신	통신의 내용, 상대방, 통신시간, 장소, 회수, ip주소	감청	통신의 위치가 노출되고, 통신의 거의 모든 내용이 저장됨.

표 5 각 매체별 통신비밀의 침해의 특징

(1) 매체가 다양화와 통신의 범위의 확장

인터넷을 비롯한 정보통신망의 발달로 인하여, 과거의 우편이나 전화를 이용하여 통신이 이루어지던 시대에 비하여 통신의 양과 질이 비약적으로 확장되게 되었다. 인터넷을 통한 전자우편, 채팅, 메신저를 이용한 통신은 물론, 전자게시판은 물론 홈페이지를 통한 통신, 무선인터넷, 이동전화를 통한 통신, 이동전화의 문자메시지 등 그 수단이 다양해지고, 양도 대폭 늘어났으며, 통신의 방법도 문자, 소리, 영상 등 다양해지고 있다. 어디까지가 헌법상 표현의 자유에 의하여 보호되는 공개적인 표현이고, 어디부터가 통신인지를 구분하기 어려운 표현과 통신의 융합현상이 일어나고 있는 것이다.

(2) 통신의 저장성의 증대

기술의 발달과 정보통신망의 특징으로 인하여 통신의 즉시성이 사라지고, 통신은 점점 저장성이 증대하고 있다. 전화의 경우에도 과거에는 요금의 산정을 위한 발신번호, 수신번호, 통화시간 정도가 저장되는 기록이었으나, 최

근에는 통화위치[87]까지 저장되고 있다. 그리고 문자메시지의 경우는 메시지의 수신자 뿐만 아니라 내용까지도 저장될 수 있다. 인터넷을 통한 통신의 경우는 수신자와 발신자에 대한 기록은 물론, 접속위치, 통신의 모든 내용이 저장되어진다. 특히 문자메시지나 인터넷의 통신의 경우 수신자나 발신자가 자신의 컴퓨터에서 통신의 내용을 삭제하더라도 서버에는 그 내용이 남아있게 되며, 로그기록은 당사자가 그것이 저장되는지를 모르는 경우가 많다.

(3) 검색과 접근의 용이성

이렇게 저장된 정보는 매우 쉽게 검색될 수 있다. 심지어는 마음만 먹으면 인터넷을 통하여 유통되는 모든 통신을 실시간으로 검색할 수도 있다. 그리고 검색을 하더라도 당사자에게 알리지 않는 이상 당사자는 검색을 했는지 여부를 알 수 없다.

(4) 공개성과 비공개성의 구분의 모호함

특히 인터넷을 통한 통신의 경우에는 그것이 공개적인 것인지, 비공개적인 것인지를 구별하는 것이 쉽지 않다. 전자우편이나 메신저 등을 통한 통신의 경우에는 비공개적인 것임이 분명하지만, 채팅방에서의 통신이나, 전자게시판을 통한 통신, 커뮤니티에서의 통신 등은 그것이 공개적인 것인지, 비공개적인 것인지를 판단하기가 쉽지 않다. 그러나 인터넷에서의 통신이 특정인을 전제로 하는 것이거나, 익명성을 전제로 한 것일 경우에는 특정인의 범위를 벗어나는 자에 대하여는 비공개성을 띤 것이고, 익명성을 침해하는 경우에는 통신의 비밀을 침해하는 것으로 보아야 할 것이다.

나. 통신비밀보호의 중요성[88]

87) 통화위치를 통신회사가 고객의 동의없이 저장기록하고 있는 것이 고객에게 서비스 제공을 위하여 불가피한 것으로 보기는 어렵다고 생각한다. 따라서 이는 위법한 것으로 판단된다.

88) 통신비밀보호이 중요한 문제로 떠오르면서 유럽연합은 회원국에서 법적 효력을 갖는 지침을 발표하기도 하였다.

-DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

이상에서 보다시피 과학기술의 발달은 통신과 표현의 경계를 모호하게 하고 있다. 표현의 자유의 보호영역과 통신의 자유의 보호영역이 중첩되게 된 것이다. 이러한 현실 속에서 통신의 비밀과 자유의 보장이 갖는 의미는 더욱 더 크다고 볼 수 있다. 그리고 최근에는 저장성이 증대하고 검색과 접근이 용이해짐에 따라 통신비밀이 침해될 가능성도 그만큼 커지게 되었다.

다. 적용범위

현행법은 공개되지 않은 대화와 우편물과 전기통신[89]을 보호의 범위로 하고 있다. 특히 우리법은 전기통신의 경우 비밀을 전제로 한 전기통신에 대하여 감청을 금지하고 있는 것이 아니라, 당사자의 동의를 받지 않은 감청을 금지하고 있기 때문에, 앞서 보았듯이 불특정다수인을 상대로 공개되는 것을 전제로 하는 전기통신의 경우가 아니라면 이러한 통신에 대해서는 감청은 엄격히 금지되는 것으로 보아야 할 것이다. 최근의 인터넷상에서의 메일링리스트 서비스나 이동전화의 문자메시지나 전화의 그룹전송 서비스의 경우를 보아도 알 수 있듯이 특정인들 사이에서의 통신의 비밀도 보호되어야 할 것이며, 익명권이 보호되어야 하기 때문이다.

라. CCTV를 통한 대화비밀의 침해금지를 분명히 명시해야 한다

-DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL- of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

89) 1. "통신"이라 함은 우편물 및 전기통신을 말한다

2. "우변물"이라 함은 우편법에 의한 통상우편물과 소포우편물을 말한다

3. "전기통신"이라 함은 전화 · 전자우편 · 회원제정보서비스 · 모사전송 · 무선호출 등과 같이 유선 · 무선 · 광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향 · 문언 · 부호 또는 영상을 송신하거나 수신하는 것을 말한다

9. "전자우편"이라 함은 컴퓨터 통신망을 통해서 메시지를 전송하는 것 또는 전송된 메시지를 말한다.

10. "회원제정보서비스"라 함은 특정의 회원이나 계약자에게 제공하는 정보서비스 또는 그와 같은 네트워크의 방식을 말한다.

11. "통신사실확인자료"라 함은 가입자의 전기통신일시, 전기통신개시 · 종료시간, 발 · 착신 통신번호 등 상대방의 가입자번호, 사용도수 그 밖에 대통령령으로 정하는 전기통신사실에 관한 자료를 말한다.

법은 통신비밀보호법과 형사소송법과 군사법원법의 규정에 의하지 아니하고는 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못하도록 하고 있다(법 . 이처럼 현행법은 공개되지 아니한 타인간의 대화를 '녹음' 또는 '청취'하지 못한다고 하고 있어서, 대화를 녹음없이 녹화나 촬영만 하는 경우에 대해서는 보호가 미치지 않는다. 그러나 대화를 녹음하거나 청취하지 않더라도 공개되지 아니한 타인간의 대화를 녹화하거나 촬영하는 경우에는 대화의 내용상의 비밀 뿐만 아니라 대화의 상대방, 시간, 장소 등이 침해되므로, 공개되지 아니한 타인간의 대화를 청취하거나, 녹음, 녹화, 촬영 기타의 방법으로 기록하거나 저장하는 행위도 엄격히 금지해야 할 것이다.

마. 범죄수사를 위한 통신제한조치의 문제

(1) 통신제한조치의 특징

검열과 감청과 같은 통신제한조치는 비록 법원의 영장에 의하여 제한적으로 허용되다 하더라도, 당사자가 감청이나 검열당하고 있다는 사실 그 자체를 전혀 모르고 있는 상태에서 이루어지는 것이기 때문에 개인의 사생활이 침해될 우려가 매우 높다. 특히 헌법상 영장주의가 의미하는 특정성, 공개성, 영장제시와는 달리 감청이나 검열은 일반성, 비밀처분성, 영장제시의 결여라는 특성으로 인하여 사실상 헌법상 영장주의에 대한 예외적인 절차이기 때문에 그 적용이나 실행은 매우 한정적, 특정적이어야 한다. 나아가서 사회공공의 안녕질서 유지라는 공익적 목적을 달성하기 위하여 희생되어야 하는 개인의 사생활 침해가 최소한에 그치도록 운영되어야 한다[90].

(2) 긴급통신제한조치를 폐지해야 한다.

현행법은 법원에 대하여 통신제한조치의 허가를 신청할 수 없는 긴급한 사유가 있는 때에는 법원의 허가없이 통신제한조치를 할 수 있다고 규정하고 있다(법 제8조). 앞서 보았듯이 통신제한조치는 개인의 사생활 침해가 매우 큰 수사방법으로 최후의 수단으로 인정되는 것이다. 통신제한조치는 사

90) 통신비밀보호법상 감청제도의 문제점, 성낙인, 시민과 변호사 1999. 7. 96p.

실상 영장주의에 대한 예외인 셈이다. 이처럼 영장주의의 예외에 해당하는 통신제한조치를 법원의 사전허가 없는 긴급통신제한조치로까지 확장하는 것은 예외에 대한 예외로서 인권침해의 소지가 지나치게 커지므로 허용되어서는 안된다. 긴급통신제한조치는 폐지되어야 한다. 아니면 차선책으로는 야간당직영장제도를 도입하여 긴급한 상황에서 야간에 영장을 발부받도록 할 수도 있을 것이다[91].

(3) 통신제한조치의 허용 대상범죄가 너무 포괄적이고, 허용기간이 지나치게 길다.

현행법은 통신제한조치의 대상범죄를 광범위하게 규정하고 있는데, 통신제한조치는 최소화해야 할 수사방법이라는 점에서 대상범죄를 대폭축소할 필요가 있다. 예컨대 뉴질랜드의 경우는 마약범죄와 조직범죄와 중대한 폭력범죄로 국한하고 있으며[92], 오스트리아는 전화도청의 경우에는 1년 이상의 징역에 처해질 범죄에 대해서만, 전자통신의 도청에 대해서는 조직범죄나 10년 이상의 징역에 처해질 범죄에 대해서만 허용하고 있으며[93], 이탈리아의 경우에는 5년 이상의 징역에 처해질 범죄에 대해서만 도청을 허용하며[94], 룩셈부르크의 경우에는 2년 이상의 징역에 처해질 범죄에 대해서만 도청을 허용하며[95], 일본의 경우에는 총기, 약물, 밀입국, 조직적인 살인과 관련된 조직범죄의 수사를 위해 도청이 허용된다고 한다[96].

현행법은 도청의 허용기간을 2개월로 하고 있는데, 오늘날 통신의 빈도나 통신에의 의존도 등을 고려할 때, 2개월 동안의 통신제한조치 기간동안 당사자는 수사와 관련이 없는 통신의 비밀을 당사자가 알지도 못하는 상태에서

---

91) 현재 미국의 경우 야간당직 영장제도를 활용하고 있다.
92) 뉴질랜드 Law Commission Study Paper 12, Electronic Technology and Police Investigations Some Issues, 1페이지. the Misuse of Frugs Amendment Act 1978, the Crime Amendment Act (No 2) 1987, 1997.
93) Privacy and Humanrights 2002, 117 페이지. §149a - 149p Strafprozessordnung - StPO.
94) Privacy and Humanrights 2002, 232 페이지, Penal Procedure Code article 266-271.
95) Privacy and Humanrights 2002, 262 페이지, Criminal Code Art 88-1 - 88-4.
96) Privacy and Humanright 2002, 237 페이지. 통신도청법에 반대하는 웹사이트 (http://www.geocities.co.jp/Milkyway/8332/what.html)

침해당할 것인바, 2개월 동안 비밀성을 갖는 일반영장을 부여하는 것은 지나치게 길다고 보지 않을 수 없다. 30일로 줄이거나 그보다 더 짧은 기간으로 줄여야 할 것이다.

(4) 국가안보를 위한 통신제한조치

현행법은 정보수사기관의 장은 국가안전보장에 대한 상당한 위험이 예상되는 경우에 한하여 그 위해를 방지하기 위하여 이에 관한 정보수집이 특히 필요한 때에는 통신의 일방 또는 쌍방당사자가 내국인인 경우에는 고등법원 수석부장판사의 허가를 받아서, 외국인인 경우에는 대통령의 승인을 얻어 통신제한조치를 할 수 있다고 규정하고 있다.

이 규정은 '국가안전보장', '상당한 위험', '위해방지', '정보수집' 등 매우 추상적인 표현으로 이루어져 있어서 남용될 가능성이 높다. 대상범죄나, 적용되는 경우를 쉽게 예측할 수 있도록 표현을 보다 구체화해야 할 것이다.

그리고 외국인인 경우에는 법원의 영장을 발부받지 않고 대통령의 승인을 얻도록 하고 있는 것도 남용의 소지가 있다. 법원의 관여가 인정되어야 한다.

(5) 통신제한조치의 절차상의 요건과 집행결과의 봉인

법원에서 영장을 발부 받기 위하여는 전자감시의 목적이 되는 통신수단 등이 특정하고 심각한 범죄에 사용되고 있다는 것을 보여주는 다음과 같은 요건이 갖추어져야 한다. (i) 다른 수사기법을 시도하였거나 실패하였고, 또는 실패할 가능성이 높거나 너무 위험한 경우라야 한다. (ii) 전자감시에 필요한 기간이 명시되어야 한다. (iii) 동일 인물에 대하여 이전에 행하였던 전자감시를 명시하여야 한다. (iv) 전자감시를 연장하기 위한 영장청구서에는 이전에 행한 전자감시로 인하여 얻은 결과물이 있어야 한다.

영장발부는 판사 중 전자감시에 관하여 특수한 교육을 받은 사람만이 전자감시를 허가하는 영장발부를 할 수 있도록 하여야 할 것이다. 이때 영장이

발부되기 위해서는 다음과 같은 요건이 충족되어야 한다. (i) 전자감시의 대상이 되는 자가 범죄를 행하고 있거나, 급박하게 행할 상당한 이유가 있어야 한다. (ii) 전자감시를 통하여 범죄와 관련이 있는 특정 정보를 취득할 수 있는 상당한 이유가 있어야 한다. (iii) 일반적인 수사기법이 이미 시도되어 실패하였거나 혹은 성공할 가능성이 없거나 너무 위험한 경우라야 한다. (iv) 전자감시의 대상이 되는 특정 통신수단이 범죄에 사용되었거나 막 사용되려고 하거나, 그 범죄와 관련하여 감시대상자에 의하여 보통 사용되고 있는 상당한 이유가 있어야 한다.

영장집행의 단계에서는 수사기관은 감청도구를 작동시키지 않았다가 수분 간격으로 이를 작동시키는 등 범죄와 관련이 없는 대화, 특히 가족생활 등 사생활에 관한 이야기를 감청 대상에서 제외시킴으로써 사생활침해를 최소화하여야 할 것이다. 이렇게 최소화 되지 않은 전자감시결과는 그 증거능력이 부정되어야 할 것이다.

한편 전자감시의 결과는 검찰이 그 원본을 보관하되, 복사본은 범죄의 확정적 증거가 되는 것만으로 편집된 것이어야 할 것이다.

목적한 증거를 수집하였거나 영장의 유효기간이 경과하였다면, 영장의 집행은 중지되어야 하며, 새로운 영장을 발부받아야만 전자감시를 계속하는 것이 가능하다.

감시의 결과물(원본)은 법원의 판단에 증거로 사용될 수 있고, 법원의 감시아래 봉인되고 정해진 기간동안 봉인된 채 보관되어야 한다. 현행 법 시행령은 통신제한조치의 집행으로 취득한 결과의 요지를 조서로 작성하고, 그 결과를 봉인하여 열람제한하여 보존하도록 하고 있는데(시행령 제16조 제1항), 수사기관의 통신제한조치의 집행의 적법성과 결과물에 대한 조작가능성을 막기 위하여는 통신제한조치 집행결과물을 법원의 감시아래 봉인하고 법원으로 제출하도록 하는 절차를 마련하는 것이 바람직하다.

전자감시가 종료된 후 또는 영장청구가 기각된 후, 판사와 검사는 전자감

시에 관한 사항을 법무부 장관과 국회에 보고하도록 하는 것이 좋을 것이다. 이러한 보고결과에는 영장발부여부, 기간, 감시대상 기구나 장소, 범죄의 종류, 하나의 감시기구에 포착된 평균 감시 · 감시자 · 범죄수, 감시비용, 감시의 종류, 수사 또는 재판의 진행정도가 포함되어야 한다. 이러한 자료는 감시영장 발부에 대한 기준을 정하는데 도움을 주며, 입법과정에서도 도움을 주게 될 것이다.[97]

(6) 통신사실확인자료 열람, 제출요청 제도의 문제점

(i) 현행법의 규정

현행법은 검사 또는 사법경찰관은 검사장의 승인을 얻거나 긴급한 경우에는 사후승인을 얻어서 가입자의 전기통신일시, 전기통신개시, 종료시간, 발, 착신 통신번호 등 상대방의 가입자번호, 사용도수, 그 밖에 대통령령으로 정하는 전기통신사실에 관한 자료(한편 시행령 제3조의 2는 1. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, 2. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치 추적자료, 3. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료를 추가하고 있다)를 통신사실확인자료라고 하여 수사 또는 형의 집행을 위하여 필요한 경우 열람이나 제출을 요청할 수 있다고 규정하고 있다. 심지어는 서면으로 통신사실확인자료제공을 요청할 수 없는 긴급한 사유가 있는 경우에는 사후에 통신사실확인자료 요청서를 제출해도 된다고 하고 있다.

(ii) 영장주의가 적용되어야 한다

통신의 비밀에는 통신의 내용 뿐만 아니라 통신의 상대방, 통신의 시간, 장소 등도 포함된다. 따라서 통신의 상대방, 통신의 시간, 장소 등에 대한 자

97) 'wiretap laws and procedures what happens when the U. S. government taps a line' Donald P. Delaney, Dorothy E. Denning, John Kaye, Alan R. McDonald, September 23, 1993의 미국법 소개를 참조하였음.

료를 공개할 경우에도 원칙적으로 영장주의가 적용되어야 할 것이다. 물론 통신의 상대방에 대한 정보에 비하여 영장주의가 적용되는 정도는 완화될 수 있을 것이다. 그러나 대통령령에 규정된 통신사실확인자료(컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치 추적자료, 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료)의 경우는 인터넷에 익명으로 올린 글의 발신자를 확인할 수 있는 자료로서 통신의 내용의 비밀을 직접 침해하는 것으로서 상위법률의 위임범위를 넘는 것이기도 하고, 엄격하게 영장주의가 적용되어야 할 것들이다. 그러나 현행법은 이러한 것들을 모두 법원의 관여없이 검사장의 승인만을 얻어서 열람하거나 제출을 요청할 수 있게 하고 있어서 통신의 비밀을 침해하고 있다.

(iii) 요건이 강화되고 절차가 엄격해져야 한다

현행법은 통신사실확인자료 요청의 요건을 수사 또는 형의 집행을 위하여 필요한 경우 열람이나 제출을 요청할 수 있도록 하고 있다. 그리고 이 경우 요청사유, 해당가입자와의 연관성, 필요한 자료의 범위를 기재한 서면이나 긴급한 경우에는 사후에 서면을 제출함으로써 가능하도록 하고 있다(법 제13조 제4항). 통신사실확인자료의 경우에도 엄격하게 범죄혐의를 기재하고 소명하도록 하여야 할 것이다.

(7) 컴퓨터 시스템의 압수, 수색에 관한 문제

컴퓨터 시스템을 압수, 수색영장을 발부받아 압수, 수색하는 경우가 있는데, 이때에도 당사자의 통신의 비밀이 침해되지 않도록 유의해야 할 것이다. 특히 컴퓨터 시스템에 다른 사람으로부터 받은 통신이 있거나, 자신이 다른 사람에게 보낸 통신이 포함되어 있는 경우에는 이를 분리하여 압수수색을 하여야 할 것이다.

Ⅴ. 민간영역에서의 감시와 프라이버시의 보호

1. 신용정보의 보호에 대한 문제

가. 현대사회에서 신용정보가 갖는 의미

개인의 임금이나 소득수준, 재산상태 등에 대한 정보는 해당 세무관청에 대해서는 신고하거나 공개해야 할 정보일 수도 있지만, 그 밖의 자에 대해서는 공개되어서는 곤란한 개인정보에 해당한다. 개인의 금융거래정보도 개인의 민감한 정보에 해당한다는 것은 두말할 필요도 없다.

한편 신용공여기관은 신용을 받으려는 자의 상환능력 등을 정확하게 파악하고 싶어하며, 이를 통하여 사회적으로는 금융거래의 안전성을 확보하고, 거래위험과 거래비용을 줄일 수 있다. 따라서 어느 정도는 신용정보가 공정하게 관리되면서 신용공여기관 사이에서 공유될 사회적 필요성도 있다.

그러나 개인의 재산상태에 대한 정보, 금융거래에 대한 정보는 기업이나 국가의 입장에서는 경제적 가치가 매우 높은 정보로서 오용될 가능성과 남용될 가능성이 매우 높으므로 각별한 주의가 요망된다. 국가나 민간의 입장에서 보면 임금, 소득수준, 재산상태, 일반거래현황, 금융거래현황 등과 같은 개인의 경제활동에 관한 정보는 매우 가치있는 정보가 된다. 기업의 입장에서도 개인의 재산상태는 개인의 구매력을 판단할 수 있는 정보이고, 개인의 거래현황은 개인의 기호나 상품의 구매패턴을 보여주는 정보로서 광고나 타겟 마케팅의 중요한 근거자료가 될 수 있기 때문에 매우 경제적 가치가 높은 정보이다. 또한 채권자의 입장에서 보면 개인의 재산상태나 금융거래현황은 채권확보를 위한 근거자료가 된다. 국가의 입장에서도 이러한 정보는 조세부과를 위한 정보가 되고, 조세채권의 확보를 위한 정보가 되기도 한다. 개인의 경제활동에 관한 정보가 갖는 이러한 유용성 때문에 정부와 기업은 국민과 소비자의 신용에 관한 정보를 수집하고 이용하려는 것이다.

그런데, 특히 예컨대 신용불량정보와 같은 신용정보에 대해 과신하고, 이

를 남용하게 될 경우에는 한번 신용불량자로 기록된 사람은 그 후로는 경제활동을 제대로 해 나갈 수 없게 된다. 수치화된 데이터베이스에 대한 과신은 정당한 항변의 기회를 봉쇄하고, 개인을 결정론적으로 범주화하여 판단하기 때문에 이를 통한 차별과 배제의 문제가 생기게 된다.

따라서 신용거래의 활성화와 거래비용의 절감을 위해서는 올바른 신용정보의 수집 및 평가체계가 수립되고 공유되어야 한다는 필요성과 신용정보의 공유는 그로 인한 개인정보의 침해가능성과 오, 남용의 가능성도 크다는 점을 감안하여, 이러한 충돌되는 가치를 조화롭게 해결하는 선에서 신용정보에 대한 수집 및 공유가 허용되어야 할 것이다.

나. 신용정보의 수집, 이용, 제공에 대한 원칙

(1) 신용정보 수집시 동의의 원칙

우선 신용거래의 당사자 사이에서의 신용정보의 수집은 그것이 거래의 내용을 구성하는 것일 때에는 그 범위 내에서는 신용정보 주체의 동의를 얻을 필요가 없을 것이다. 그러나 수집된 신용정보가 거래의 이행을 위한 목적 이외의 목적(예를 들어 거래상대방의 신용판단의 근거로 이용하는 경우)으로 이용되는 경우, 그리고 수집된 신용정보를 당해 거래의 종결 후에도 보유하고 있는 경우(예컨대 은행의 경우는 금융거래 관련 정보를 영구보존한다고 한다)에는 원칙적으로 신용정보주체의 동의를 얻어야 할 것이다. 이때 동의는 신용정보의 수집범위, 이용목적, 보유기간 등을 명시하여 사전에 얻어야 할 것이다.

(2) 신용정보의 제3자 제공시 동의의 원칙과 신용정보의 집중

한편 신용정보를 제3자에게 제공할 때에도 당연히 신용정보주체의 동의를 얻어야 할 것이다. 이때에는 제공되는 신용정보의 내용, 제공받는 자, 제공목적 등을 구체적으로 명시하여야 할 것이다.

한편 금융거래정보에 대하여 특별한 보호를 하고 있는 취지에 비추어 볼 때, 개인의 신용정보를 제공받을 수 있는 제3자의 범위를 제한할 필요가 있다.

신용정보의 집중의 경우는 사회적 필요에 의하여 인정될 수 있을 것인데, 이것은 매우 민감한 개인정보의 누출의 문제를 야기하며, 개인에 대한 경제적인 블랙리스트로 작용하므로, 이 때에는 당사자에게 쉽고, 평이하며, 그 의미를 확실하게 전달할 수 있는 해설문의 형식으로 서면동의를 받아야 하고, 신용정보를 집중관리할 수 있는 자와, 집중되는 신용정보의 범위, 이를 이용할 수 있는 자의 범위를 한정하여 허용하여야 할 것이다.

(3) 수집된 신용정보에 대한 신용정보주체의 권리

이와 같이 수집된 신용정보에 대해서 신용정보주체는 열람을 청구할 수 있어야 하며, 잘못된 내용을 정정할 권리를 가지고 있어야 하며, 언제든지 신용정보의 제3자 제공에 대한 동의를 철회할 수 있는 권리를 가지고 있어야 한다. 특히 열람의 청구와 정정청구 및 동의의 철회권은 무료로 손쉽게 행사할 수 있도록 하여야 할 것이다.

(4) 신용정보에 대한 보다 엄격한 보호

한편 신용정보는 매우 민감한 정보이며, 오류가 포함되거나 그것이 남용될 경우에는 신용정보주체에게 막대한 손해를 끼치게 된다. 이런 점에서 (i) 신용정보를 취급할 수 있는 자의 범위와 자격을 제한할 필요가 있고 이들을 엄격하게 관리할 필요가 있다. - 신용정보업자의 제한. 그리고 (ii) 신용정보주체로부터 동의를 받아 신용정보집중기관이 집중하여 보관 관리를 할 수 있는 신용정보를 제한하고, - 신용정보집중기관의 정보의 제한. (iii) 신용정보집중기관이 보유하고 있는 신용정보를 이용할 수 있는 자의 범위도 제한하여야 한다 - 신용정보의 이용제한. (iv) 그리고 신용정보에 대한 신용정보주체의 접근권이 보장되어야 하며, 잘못된 내용에 대한 시정요구권이 보장되어야 한다.

(5) 그 밖의 경제활동에 관한 정보의 특별한 보호

특히 요즘에는 거의 모든 경제활동이 신용카드나 전자화폐를 이용하여 이루어지고 있고, 거래기록이 보다 세분화되어 상세히 기록되고, 데이터마이닝의 기법을 통하여 분석, 가공되면서, 신용카드나 전자화폐의 거래정보나 금융거래정보는 단순히 개인의 경제활동에 대한 정보의 의미를 넘어서서 개인의 취미나 기호, 생활습관, 가치관 등을 파악할 수 있는 매우 민감한 개인정보가 되고 있다. 따라서 이러한 정보에 대해서는 보다 더 각별한 보호가 있어야 한다.

다. 우리나라 법제의 태도와 개정방향

(1) 신용정보의 보호

(가) 신용정보의 이용 및 보호에 관한 법률

(i) 현행규정

현행 신용정보의 이용 및 보호에 관한 법률은 “금융거래 등 상거래에 있어서 거래상대방에 대한 식별·신용도·신용거래능력 등의 판단을 위하여 필요로 하는 정보로서 대통령령이 정하는 정보[98]”를 신용정보라고 정의하여,

98) 대통령령 제2조 제1항

1. 개인의 성명·주소·주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호)·성별·국적 및 직업 등과 기업 및 법인의 상호·법인등록번호·사업자등록번호·본점 및 영업소의 소재지·설립연월일·목적 및 임원에 관한 사항 등 특정 신용정보주체를 식별할 수 있는 정보(제2호 내지 제6호의 1에 해당하는 정보와 결합되는 경우에 한한다)
2. 대출·보증·담보제공·가계당좌예금 또는 당좌예금·신용카드·할부금융·시설대여 등의 금융거래 등 상거래와 관련하여 신용정보주체의 거래내용을 판단할 수 있는 정보로서 재정경제부령이 정하는 정보
3. 금융거래 등 상거래와 관련하여 발생한 연체·부도·대지급 또는 허위 기타 부정한 방법에 의한 신용질서 문란행위 등 신용정보주체(신용정보주체가 회사인 경우에는 다음 각목의 자를 포함한다)의 신용도를 판단할 수 있는 정보로서 재정경제부령이 정하는 정보
   가. 국세기본법 제39조제2항의 규정에 의한 과점주주로서 최다출자자인 자
   나. 국세기본법 제39조제2항의 규정에 의한 과점주주인 동시에 당해 회사의 이사 또는 감사로서 당해 회사의 채무에 연대보증을 한 자
   다. 당해 회사의 발행주식총수 또는 지분총액의 100분의 30이상을 소유하고 있는 자로서 최

이에 대하여 특별한 보호를 하고 있다.

이러한 신용정보는 그 성질에 따라 (i) 식별정보{대통령령 제2조 제1항 제1호의 정보 : 개인의 성명 · 주소 · 주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호) · 성별 · 국적 및 직업 등과 기업 및 법인의 상호 · 법인등록번호 · 사업자등록번호 · 본점 및 영업소의 소재지 · 설립연월일 · 목적 및 임원에 관한 사항 등 특정 신용정보주체를 식별할 수 있는 정보}, (ii) 신용거래정보(대통령령 제2조 제1항 제2호의 정보 : 대출 · 보증 · 담보제공 · 가계당좌예금 또는 당좌예금 · 신용카드 · 할부금융 · 시설대여 등의 금융거래 등 상거래와 관련하여 신용정보주체의 거래내용을 판단할 수 있는 정보로서 거래의 종류, 거래당사자의 성명 또는 상호, 거래의 기간 · 금액 및 한도 등의

다출자자인 자

라. 당해 회사의 무한책임사원

4. 금융거래등 상거래에 있어서 신용도등의 판단을 위하여 필요한 개인의 재산 · 채무 · 소득의 총액, 납세실적등과 기업 및 법인의 연혁 · 주식 또는 지분보유현황 등 회사의 개황, 판매내역 · 수주실적 · 경영상의 주요계약 등 사업의 내용, 재무제표 등 재무에 관한 사항, 주식회사의외부감사에관한법률의 규정에 의한 감사인의 감사의견 및 납세실적 등 신용정보주체의 신용거래능력을 판단할 수 있는 정보
5. 금융거래등 상거래에 있어서 신용정보주체의 식별 · 신용도 및 신용거래능력을 판단할 수 있는 법원의 심판 · 결정정보, 조세 또는 공공요금 등의 체납정보, 주민등록 및 법인등록에 관한 정보 및 기타 공공기관이 보유하는 정보로서 재정경제부령이 정하는 정보
6. 제2호 내지 제5호와 유사한 신용정보로서 재정경제부령이 정하는 정보

재정경제부령

제2조 (정의) ①영 제2조제1항제2호에서 "재정경제부령이 정하는 정보"라 함은 거래의 종류, 거래당사자의 성명 또는 상호, 거래의 기간 · 금액 및 한도등을 말한다. <개정 1999.5.25>

②영 제2조제1항제3호에서 "재정경제부령이 정하는 정보"라 함은 거래의 종류, 거래당사자의 성명 또는 상호, 연체 · 부도 · 대지급등의 금액과 발생 · 해소등의 시기를 말한다. <개정 1999.5.25>

③영 제2조제1항제5호에서 "재정경제부령이 정하는 정보"라 함은 다음 각호의 1에 해당하는 정보를 말한다. <개정 1999.5.25>

1. 법원의 금치산선고 · 한정치산선고 · 실종선고의 심판, 파산선고의 결정, 채무불이행자명부에 등재하는 결정 및 경매개시결정 · 경락허가결정등 경매에 관련된 결정에 관한 정보
2. 국세 · 지방세 또는 관세의 체납관련정보
3. 벌금 · 과태료 및 공공요금등의 체납관련정보
4. 개인의 주민등록관련정보로서 출생 · 사망 · 이민 · 부재등에 관한 정보 및 법인등록관련정보로서 설립, 휴업 · 폐업, 양도 · 양수, 주식 또는 지분변동등에 관한 정보
5. 다른 법령에 의하여 국가 또는 지방자치단체로부터 받은 행정처분에 관한 정보중에서 금융거래등 상거래와 관련된 정보

정보), (iii) 신용불량정보(대통령령 제2조 제1항 제3호의 정보 : 금융거래 등 상거래와 관련하여 발생한 연체 · 부도 · 대지급 또는 허위 기타 부정한 방법에 의한 신용질서 문란행위 등 신용정보주체의 신용도를 판단할 수 있는 정보로서 거래의 종류, 거래당사자의 성명 또는 상호, 연체 · 부도 · 대지급등의 금액과 발생 · 해소등의 시기 등의 정보}, (iv) 신용능력정보(금융거래등 상거래에 있어서 신용도등의 판단을 위하여 필요한 개인의 재산 · 채무 · 소득의 총액, 납세실적등과 기업 및 법인의 연혁 · 주식 또는 지분보유현황 등 회사의 개황, 판매내역 · 수주실적 · 경영상의 주요계약 등 사업의 내용, 재무제표 등 재무에 관한 사항, 주식회사의외부감사에관한법률의 규정에 의한 감사인의 감사의견 및 납세실적 등 신용정보주체의 신용거래능력을 판단할 수 있는 정보), (v) 공공정보(대통령령 제2조 제1항 제5호의 정보 : 금융거래 등 상거래에 있어서 신용정보주체의 식별 · 신용도 및 신용거래능력을 판단할 수 있는 법원의 심판 · 결정정보, 조세 또는 공공요금 등의 체납정보, 주민등록 및 법인등록에 관한 정보 및 기타 공공기관이 보유하는 정보로서 법원의 금치산선고 · 한정치산선고 · 실종선고의 심판, 파산선고의 결정, 채무불이행자명부에 등재하는 결정 및 경매개시결정 · 경락허가결정등 경매에 관련된 결정에 관한 정보, 국세 · 지방세 또는 관세의 체납관련정보, 벌금 · 과태료 및 공공요금등의 체납관련정보, 개인의 주민등록관련정보로서 출생 · 사망 · 이민 · 부재등에 관한 정보 및 법인등록관련정보로서 설립, 휴업 · 폐업, 양도 · 양수, 주식 또는 지분변동등에 관한 정보, 다른 법령에 의하여 국가 또는 지방자치단체로부터 받은 행정처분에 관한 정보중에서 금융거래등 상거래와 관련된 정보)로 나누어 볼 수 있다.

(ii) 개정방향

그런데 앞서도 보았듯이 신용정보는 개인의 민감한 정보에 해당하는데, 특히 신용정보가 집중될 경우에는 민감성은 더욱 커지게 된다. 그리고 신용정보 중에서 신용불량정보의 경우는 개인에 대한 경제활동에 있어서의 블랙리스트로 작용하게 된다. 따라서 이러한 점을 고려하여, 법률로서 수집하고 집중할 수 있는 신용정보의 범위를 대폭 제한하여 엄격하게 규율할 필요가 있다. 따라서 현재, 금융거래 뿐만 아니라 상거래 등의 일반적인 연체정보에

대하여까지 신용정보로 정의하여 수집, 집중할 수 있도록 하고 있는 것을 개정하여, 신용정보를 특정한 여신에 관련된 정보로 엄격하게 제한하고(그 중에서 소비자 여신의 경우는 소액여신이 많은바, 이를 신용정보로 집중관리할 필요성은 낮다. 수집, 집중할 수 있는 경우를 일정금액 이상으로 제한하든가, 제외시켜야 할 것이다), 일정액 이상으로 금액의 범위도 한정하여 운영할 필요가 있다.

(나) 금융실명거래 및 비밀보장에 관한 법률의 보호

(i) 금융거래정보의 비밀보호

법은 금융기관에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래(금융기관이 금융자산을 수입ㆍ매매ㆍ환매ㆍ중개ㆍ할인ㆍ발행ㆍ상환ㆍ환급ㆍ수탁ㆍ등록ㆍ교환하거나 그 리자ㆍ할인액 또는 배당을 지급하는 것과 이를 대행하는 것 기타 금융자산을 대상으로 하는 거래)의 내용에 대한 정보 또는 자료(이하 "거래정보등"이라 한다)를 타인에게 제공하거나 누설하여서는 아니되며, 누구든지 금융기관에 종사하는 자에게 거래정보 등의 제공을 요구하여서는 아니된다고 규정하고 있다.

(ii) 비밀보호의 예외

그러나, 법원의 제출명령 또는 법관이 발부한 영장에 의한 거래정보등의 제공의 경우, 조세에 관한 법률에 의하여 제출의무가 있는 과세자료등의 제공과 소관관서의 장이 상속ㆍ증여재산의 확인, 조세탈루의 혐의를 인정할 만한 명백한 자료의 확인, 체납자의 재산조회, 국세징수법 제14조제1항 각호의 1에 해당하는 사유로 조세에 관한 법률에 의한 질문ㆍ조사를 위하여 필요로 하는 거래정보등의 제공 등의 경우나, 국정감사및조사에 관한법률에 의한 국정조사에 필요한 자료로서 해당 조사위원회의 의결에 의한 금융감독원장 및 예금보험공사사장의 거래정보등의 제공, 재정경제부장관, 금융감독위원회(증권ㆍ선물시장의 불공정거래조사의 경우에는 증권선물위원회를 말한다), 금융

감독원장 및 예금보험공사사장이 금융기관에 대한 감독·검사를 위하여 필요로 하는 거래정보등의 제공, 동일한 금융기관의 내부 또는 금융기관 상호간에 업무상 필요한 거래정보등의 제공, 기타 법률에 의하여 불특정다수인에게 의무적으로 공개하여야 하는 것으로서 당해 법률에 의한 거래정보등의 제공 등의 경우에는 거래정보를 제공할 수 있다고 하고 있다.

이 중 동일한 금융기관의 내부 또는 금융기관 상호간에 업무상 필요한 거래정보 등을 제공하는 경우에는 명의인의 인적사항, 요구대상 거래기간, 요구의 법적근거, 사용목적, 요구하는 거래정보 등의 내용, 요구하는 기관의 담당자 및 책임자의 성명과 직책 등 인적사항 등을 적시하여 문서에 의하여 요청하도록 하고 있다.

(iii) 개정방향

금융거래의 비밀보호의 예외규정으로 두고 있는 동일한 금융기관의 내부 또는 금융기관 상호간에 업무상 필요한 거래정보등의 제공에 관한 규정을 어떤 업무상의 필요에 의하여 거래정보를 상호제공할 수 있는지를 구체적으로 밝혀(예를 들어 계약의 이행을 위하여 필요한 경우처럼) 명시해 두어야 할 것이다.

(2) 신용정보업자 등의 신용정보 수집, 조사의 방법

(가) 신용정보의 수집, 조사는 누가 할 수 있는가?

(i) 현행규정

법은 신용정보의 수집, 조사를 누가 할 수 있는지에 대하여 아무런 규정을 두고 있지 않다. 다만 법은 신용정보업자[99], 신용정보집중기관[100] 및 신용

99) 신용조회업자, 신용조사업자, 채권추심업자, 신용평가업자.

100) 신용정보를 집중하여 수집·보관하여 체계적·종합적으로 관리하고 신용정보업자 등 상호간에 신용정보를 교환·활용(이하 "집중관리·활용"이라 한다)하고자 하는 자로서 금융감독위원회에 신용정보집중기관으로 등록한 자. 여기에는 종합신용정보집중기관(대통령령이 정하는 금융기관 전체로부터 신용정보를 집중관리·활용하는 신용정보집중기관)과 개별신용정보집중기관(제1

정보제공 · 이용자(이하 "신용정보업자 등"이라 한다)는 신용정보를 수집 · 조사함에 있어서 이 법 또는 정관에서 정한 업무범위 안에서 수집 · 조사의 목적을 명확히 하고 그 목적의 달성에 필요한 범위 안에서 합리적이고 공정한 수단에 의하여야 한다(법 제13조)고 규정하고 있다. 이러한 법의 태도가 신용정보의 수집, 조사를 신용정보업자 등에게만 제한적으로 허용하고 신용정보업자 등이 아닌 자는 신용정보를 수집할 수 없다는 것인지, 아니면 신용정보업자 등이 신용정보를 수집, 조사하는 경우의 준수사항에 대하여 규정하고 있는 것인지는 분명하지 않다.

한편 우리 법은 신용정보제공 · 이용자를 중소기업, 유통사업자 등을 포함하여 지나치게 넓게 규정하고 있다. 신용정보제공 · 이용자는 신용정보집중기관으로부터 신용정보를 모두 이용할 수 있게 되는바, 이는 신용정보의 집중제도가 갖는 본래의 의미인 신용공여시의 신용평가의 취지를 벗어나는 것이다. 신용정보제공 · 이용자의 범위를 금융기관과 여신행위를 행하는 자로 제한하여야 할 것이다.

또한 법은 신용정보집중기관을 지나치게 방만하게 허용하고 있다. 예컨대 한국정보통신진흥협회의 경우는 통신사업자들의 신용정보집중기관인데 이를 통하여 실질적으로 이동통신요금미납자에 대한 블랙리스트제도를 운영하고 있다. 이는 이동통신요금 납부실적을 높이기 위한 제도로서 신용정보 집중의 취지를 악용하고 있는 대표적인 사례인 것이다. 신용정보집중기관의 범위도 제한하고, 집중되는 신용정보의 범위도 한정하여, 이러한 악용사례를 막아야 할 것이다.

(ii) 개정방향

호의 규정에 의한 금융기관 중 동종의 금융기관으로부터 신용정보를 집중관리 · 활용하거나 금융기관외의 동종의 사업자가 설립한 협회 등의 협약에 의하여 신용정보를 집중관리 · 활용하는 신용정보집중기관)이 있다. 모든 신용정보가 집중되는 종합신용정보집중기관으로는 전국은행연합회가 있으며, 업종별로 해당업체의 소비자관련 신용정보를 집중 · 제공하는 개별신용정보집중기관은 한국정보통신진흥협회 · 생명보험협회 · 대한손해보험협회 · 여신전문금융업협회가 있다.

아무런 규정을 두지 않은 현행법의 태도를 바꿔 신용정보의 수집, 조사를 신용정보업자 등에게만 제한적으로 허용하고, 신용정보업자 등이 아닌 자는 신용정보를 수집할 수 없는 것으로 분명히 밝혀두는 것이 바람직하다. 그리고 신용정보의 범위도 여신에 관한 것으로 제한하여야 할 것이다.

(나) 신용정보의 수집, 조사시 신용정보주체의 동의가 필요한지?

(i) 현행규정

법은 신용정보의 수집, 조사시 신용정보주체의 동의가 필요한지에 대하여 아무런 규정을 두고 있지 않다. 다만 법은 신용정보업자 등은 이 법 또는 정관에서 정한 업무범위 내에서 수집, 조사를 하여야 한다고만 규정하고 있을 뿐이다.

생각건대 신용거래의 당사자 사이에서의 신용정보의 수집은 그것이 거래의 내용을 구성하는 것으로서 신용정보의 수집이 계약의 이행을 위하여 필요한 경우에는 그 범위 내에서는 신용정보 주체의 동의를 얻을 필요가 없다고 볼 수 있을 것이다. 그러나 수집된 신용정보가 거래의 이행을 위한 목적 이외의 목적(예를 들어 거래상대방의 신용판단의 근거로 이용하는 경우)으로 이용되는 경우나, 수집된 신용정보를 당해 거래의 종결 후에도 보유하고 있는 경우(예컨대 은행의 경우는 금융거래 관련 정보를 영구보존한다고 한다), 거래의 당사자 사이의 당해 거래에 관한 신용정보의 수집 외의 경우에는 원칙적으로 신용정보주체의 동의를 얻어야 하는 것으로 볼 것이다. 그리고 이때 동의는 신용정보의 수집범위, 이용목적, 보유기간 등을 명시하여 사전에 얻어야 할 것이다.

(ii) 개정방향

신용정보의 수집, 조사시 신용정보주체의 동의가 있어야 함을 명시해야 한다. 그리고 이때 동의는 신용정보의 수집범위, 이용목적, 보유기간 등을 명시하여 사전에 얻어야 하는 것으로 해야 할 것이다.

(다) 수집이 제한되는 정보

(i) 현행규정

법은 신용정보업자 등은 국가의 안보 및 기밀에 관한 정보, 기업의 경영 비밀 또는 독창적인 연구개발정보, 개인의 정치적 사상, 종교적 신념 기타 신용정보와 무관한 사생활에 관한 정보, 불확실한 개인신용정보, 다른 법률에 의하여 수집이 금지된 정보를 수집할 수 없으며, 신용정보업자 등이 개인의 질병에 관한 정보를 수집·조사하고자 할 경우에는 본인의 동의를 얻어야 하며 보험업법 제5조의 규정에 의하여 금융감독위원회의 허가를 받은 인보험사업자가 개인의 질병에 관한 정보를 보험계약업무와 관련하여 이용하는 경우에 한하여 당해 정보를 이용하여야 한다(법 제14조)는 규정을 두고 있다.

(ii) 개정방향

신용정보업자 등이 수집할 수 있는 정보와, 집중할 수 있는 정보에 대하여 분명한 규정을 두고, 수집할 수 있는 정보인 여신에 관한 정보 외의 정보는 수집하거나 집중할 수 없다고 명시하여야 할 것이다.

(3) 신용정보업의 허가제 등

법은 신용정보업을 신용조회업, 신용조사업, 신용평가업, 채권추심업으로 구분하여 일정한 요건을 갖춘 자에 대하여만 허가를 해 주고 있다(법 제4조, 제4조의 2).

(4) 개인신용정보의 집중·관리

(가) 신용정보를 집중할 때나, 제3자에게 제공하는 때에는 그에 대한 신용정보주체의 동의를 받아야 한다

(i) 현행규정

법은 금융거래에 관한 정보와 개인의 질병에 관한 정보, 개인을 식별할 수 있는 정보, 신용거래정보, 신용능력정보를 신용정보업자 등에게 제공하고자 하는 경우에는 당해 개인으로부터 서면[101]에 의한 동의를 받아야 한다고 규정하고 있다(법 제23조). 현행법은 집중되는 신용정보의 범위에 대해서도 상거래 채권을 포함시키는 등 사실상 아무런 제한을 두고 있지 않다.

(ii) 개정방향

금융감독원이 정한 동의서는 그 내용을 알기도 어려울 뿐만 아니라 제공되는 정보가 어떤 절차를 통해 누가 이용하게 되는지에 대하여 도저히 알 수 없게 되어 있다. 따라서 동의서는 평이한 문장으로, 쉽게, 수집되는 정보의 구체적인 내용, 그 정보의 보존기간, 수집되는 정보가 이용되는 절차, 그 정보를 이용하게 될 자, 구제수단, 동의의 철회방법 등에 대하여 상세한 내용을 적은 서면으로 해야 할 것이다.

그리고 신용정보의 집중이용의 경우는 그것이 모든 거래주체에게 무차별 공개가 되는 것이므로 이러한 취지가 명시되어야 할 것이다.

또한 집중되는 신용정보의 범위도 엄격하게 여신에 관한 정보로 한정해야 할 것이다.

(나) 신용정보집중기관에 신용불량정보, 공공정보를 제공할 때에는 신용정보주체의 동의를 받을 필요가 없는가?

---

101) 개인신용정보의 제공 · 활용동의서

_____기관(신용정보제공 · 이용자) 귀하

이 계약과 관련하여 귀사가 본인으로부터 취득한 다음 신용정보는 신용정보의이용및보호에관한법률 제23조의 규정에 따라 타인에게 제공 · 활용시 본인의 동의를 얻어야 하는 정보입니다. 이에 본인은 귀사가 다음의 신용정보를 신용정보집중기관, 신용정보업자, 신용정보제공 · 이용자등에게 제공하여, 본인의 신용을 판단하기 위한 자료로서 활용하거나 또는 공공기관에서 정책자료로서 활용하도록 하는 데 동의합니다.

* 제공할 신용정보의 내용 :

년 월 일

서명 또는 인

(i) 현행규정

법은 금융거래에 관한 정보와 개인의 질병에 관한 정보, 개인을 식별할 수 있는 정보, 신용거래정보, 신용능력정보를 신용정보업자 등에게 제공하고자 하는 경우에는 당해 개인으로부터 서면에 의한 동의를 받아야 한다고 규정하고 있을 뿐, 신용정보집중기관에 신용불량정보와 공공정보를 제공할 때 신용정보주체의 동의를 받아야 하는지 여부에 대해서는 아무런 규정을 두지 않고 있다. 그러나 금융감독원은 이 법의 취지를 제한적으로 해석하여 신용정보집중기관에는 신용불량정보를 제공할 때 신용정보주체의 동의를 받을 필요가 없으며, 이 경우 (i) 신용정보제공ㆍ이용자와 동 신용정보제공ㆍ이용자가 신용정보를 제공한 신용정보 집중기관 사이와, (ii) 신용정보집중기관과 신용정보업자간, (iii) 신용정보집중기관 사이에서는(시행령 제9조 제9항), 상호간에 신용정보를 집중하여 수집, 보관하고 체계적 종합적으로 관리하고 상호간에 신용정보를 교환, 활용할 수 있도록 허용하고 있다.

나아가 금융감독원이 제정한 신용정보업감독규정에 의하면 금융기관은 영 제9조제5항에서 정하는 집중관리ㆍ활용대상 신용정보를 집중관리하기에 적합한 형태로 처리하여 종합신용정보집중기관에 등록하여야 한다고 의무사항으로 규정하고 있다(제11조 제1항).

(ii) 개정방향

신용불량정보를 포함하여 모든 신용정보에 대하여 그것이 제3자에게 제공되거나 집중될 때 당사자의 동의를 받도록 법률을 개정해야 할 것이다.

(다) 개인신용정보의 수집체계

(i) 현행규정

* 법률상 당연한 집중 : 신용정보업감독규정에 의하여 금융기관은 집중관리ㆍ활용대상 신용정보를 종합신용정보집중기관에 집중해야 하므로, 집중관리ㆍ활용대상 신용정보는 모두 집중되어 활용되게 된다. 이를 개별신용정보

집중기관, 신용조회업자, 신용정보제공ㆍ이용자가 이용하게 된다.

* 신용정보주체의 동의에 의한 것 : 한편 신용정보제공ㆍ이용자는 신용정보주체로부터 서면에 의한 동의를 받아서 신용정보를 신용정보업자나 신용정보집중기관으로 집중할 수 있다. 이와 같이 집중된 신용정보는 개별신용정보집중기관, 종합신용정보집중기관, 신용조회업자, 신용정보제공ㆍ이용자가 이용할 수 있다.

(ii) 개정방향

법률상 당연하게 집중되는 집중관리ㆍ활용대상 신용정보 제도를 폐지하고, 당사자의 동의를 얻어서 집중할 수 있는 것으로 해야 한다. 그리고 신용정보주체의 동의가 있더라도 수집과 집중이 허용되는 특정한 신용정보를 제외한 나머지 정보는 수집과 집중을 할 수 없도록 하여야 한다.

(라) 신용정보집중기관을 통하여 법률상 당연히 집중관리, 공동활용되는 신용정보의 범위

(i) 현행규정

대통령령은 다음과 같이 신용정보집중기관을 통하여 법률상 당연히 집중관리, 공동활용되는 신용정보의 범위를 정하고 있다(령 제9조 제5항). 한편 대통령령 제9조 제5항의 규정에 의하여 제정된 신용정보감독규정은 아래의 신용정보의 범위를 확장하여 아래와 같이 신용정보집중기관을 통하여 집중관리, 공동활용되는 신용정보의 법위를 아래와 같이 추가하여 정하고 있다.

대통령령 [별표 2] 〈개정 99. 4. 30, 2001. 6.30〉

종합신용정보집중기관을 통하여 집중관리ㆍ활용되는 신용정보의 범위(제9조제5항관련)

가. 개인

	집중관리 · 활용대상정보
1. 식별정보	성명, 주소, 주민등록번호(외국인의 경우 여권번호 또는 외국인 등록번호)
2. 신용불량 정보	가. 대출금등의 연체, 용도의 유용사실 나. 지급보증대급금(또는 대위변제) 발생사실 다. 어음 또는 수표거래정지처분을 받은 사실 라. 신용카드대금 미결제등 신용카드거래질서를 문란하게 한 사실 마. 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실
3. 신용거래 정보	가. 대출현황 나. 당좌 · 가계당좌예금개설 및 해지사실 다. 신용카드의 발급 · 해지사실 및 결제금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우에 한한다)

나. 기업 및 법인

	집중관리 · 활용대상정보
1. 식별정보	기업의 상호 또는 법인명, 대표자성명 및 주민등록번호, 사업자등록번호, 법인등록번호, 본점소재지
2. 신용불량 정보	가. 대출금등의 연체, 용도의 유용사실 나. 지급보증대급금(또는 대위변제) 발생사실 다. 신용보증대급금 발생사실 라. 어음 또는 수표거래정지처분을 받은 사실 마. 리스자금 또는 리스료의 연체사실 바. 신용카드대금 미결제등 신용카드거래질서를 문란하게 한 사실 사. 무보증사채상환불이행사실 아. 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실
3. 신용거래 정보	가. 대출 · 지급보증등 신용공여현황 나. 시설대여현황 다. 신용보증현황 라. 보증보험현황 마. 담보 및 채무보증현황 바. 당좌 · 가계당좌예금개설 및 해지사실 사. 신용카드의 발급 · 해지사실 및 결제금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우에 한한다)
4. 신용능력 정보	가. 재무제표 나. 계열기업체현황 다. 자본금증자 및 사채발행현황 주 : 비공개자료로서 당해 법인이 공개를 희망하지 아니하는 사항은 교환 · 활용대상에서 제외

신용정보업감독규정에 의한 신용정보 등록 및 이용기준

1. 식별정보

등록정보	등 록 기 관	등 록 기 준		이 용 기 관
		대 상 주 체	등 록 시 기	
영 별표2의 식별정보	영 제9조제6항 금융기관중 당해 등록정보 보유기관	당해 개인 및 기업체	수 시	식별정보와 연결된 정보의 이용기관

2. 신용불량정보

등록정보	등 록 기 관	등 록 기 준		이 용 기 관
		대 상 주 체	등 록 시 기	
영 별표2의 신용불량정보	영 제9조제6항 금융기관중 당해등록정보 보유기관	당해 개인과 법인 · 기업체 및 회사인 경우 그 관련인[1]	신용정보협의회가 정함	○영 제9조제6항 금융기관 ○법 제4조의 신용정보업자 ○영 제2조제2항제27호에 해당하는 자
어음 · 수표부도사실 [2]	은행(농 · 수협 포함)	당해 법인 · 기업체	상동	상 동

주 1) 영 제2조제1항제3호 각 목의 1에 한함

2) 신용정보협의회는 전산수용능력, 당해 정보집중의 실효성 등을 감안하여 등록기관, 등록기준, 이용기관, 집중시기 등에 관하여 제한을 둘 수 있음

3. 신용거래정보

(1) 개인

등록정보	등 록 기 관	등 록 기 준		이 용 기 관
		대 상 주 체	등 록 시 기	
대출일자, 대출금액 (신용카드 현금서비스 실적 포함)	영 제9조제6항 금융기관 중 당해 등록정보 보유기관	당해 개인 (단, 종합신용정보집중기관은 전산수용능력등을 감안하여 대출금 집중기준을 조정할 수 있음)	신용정보협의회가 정함	○영 제9조제6항 금융기관 ○법 제4조에 의한 신용정보업자 (단, 신용정보업자는 당해 정보를 가공하여 영 제9조제6항의 규정에 의한 금융기관에 대해서만 제공할 수 있음) ○영 제2조제2항제27호에 해당하는 자
채무보증일자, 채무보증금액	영 제9조제6항 금융기관중 당해등록정보 보유기관	당해 개인	상 동	○영 제9조제6항 금융기관 ○법 제4조에 의한 신용정보업자 (단, 신용정보업자는 당해 정보를 가공하여 영 제9조제6항의 규정에 의한 금융기관에 대해서만 제공할 수 있음) ○영 제2조제2항제27호에 해당하는 자
가계당좌예금 개설 및 해지 사실, 신용카드 발급·해지 사실 및 결제금액주)	은행(농·수협 포함)	당해 개인	상 동	○영 제9조제6항 금융기관 ○법 제4조의 신용정보업자 ○영 제2조제2항제27호에 해당하는 자
신용카드 발급·해지사실 및 결제금액주)	여신전문금융회사	상 동	상 동	상 동

주) 신용카드결제금액은 해당 신용정보를 보유한 신용카드사가 동의하는 경우에 한함

4. 능력정보

등록정보	등록기관	등 록 기 준		이 용 기 관
		대 상 주 체	등록시기	
증자 및 사채발행 계획 확정내용	협조기관 (금융감독원)	○당해 기업체(단, 종합신용정보집중기관은 전산수용능력 등을 감안하여 집중기준을 조정할 수 있음) ○주채무계열 및 기타계열 기업군 소속기업체	신용정보협의회가 정함	○영 제9조제6항 금융기관 ○법 제4조의 신용정보업자 ○영 제2조제2항제27호에 해당하는 자
영 제2조제1항제4호에 의한 회사의 개황, 사업의 내용, 재무에 관한 사항, 감사인의 감사의견 및 납세실적 등과 영 별표2에 의한 신용 능력정보[주]	영 제9조제6항 금융기관 중 당해 등록정보 보유기관	당해 법인 · 기업체	상 동	상 동

주) 신용정보협의회는 전산수용능력, 당해 정보집중의 실효성 등을 감안하여 등록기관, 등록기준, 이용기관, 집중시기 등에 관하여 제한을 둘 수 있음

5. 공공기록 정보

등록정보	등 록 기 관	등 록 기 준		이 용 기 관
		대 상 주 체	등 록 시 기	
경제법령 위반	영 제9조제6항 금융기관중 당해 등 록 정 보 보유기관	위반자	신용정보협의회가 정함	○영 제9조제6항 금융기관 ○법 제4조의 신용정보업자 ○영 제2조제2항제27호에 해당하는 자
○법원의 심판 및 결정정보 ○조세, 벌금 · 과태료, 공공요금 등의 체납정보 ○기타공공정보 (특허권,법인등 록에 관한 정보 등)	공공기관	당해주체	상 동	○영 제9조제6항 금융기관 ○법 제4조의 신용정보업자 ○영 제2조제2항제27호에 해당하는 자 (단, 관련법령의 규정에 의하여 공개가 허용되는 정보에 한함)

(ii) 개정방향

당사자의 동의를 받아야 하는 것으로 개정해야 하고, 수집, 집중될 수 있는 정보의 범위도 제한하여야 할 것이다.

(마) 업계의 현황

(i) 금융거래 관련 정보의 집중

금융기관은 공동활용대상 신용정보를 중앙신용정보집중기관으로 집중시킨다.

(ii) 각 협회를 통한 가입자 정보와 연체정보의 집중

한국정보통신산업협회, 생명보험협회, 대한손해보험협회, 여신전문금융업협회 등도 각 회원사들로부터 가입자(또는 계약자)정보, 연체정보 등을 집중하여 회원사에게 동 정보를 제공하고 있다. 이 경우 가입자 또는 계약자로부터 동의를 얻어 두었어야 한다.

(iii) 통신사업자, 유통업자, 중소기업으로부터 연체정보의 집중

신용조회업자는 전국은행연합회로부터 집중된 신용정보를 제공받는 이외에 통신사업자, 유통업자, 중소기업 등으로부터도 이동통신요금 체납정보, 백화점카드대금 연체정보, 상거래채권 연체정보 등의 신용정보를 수집하여 DB를 구축하고, 금융회사 등 회원사들에게 그 내용을 제공하고 있다. 이 경우에도 통신사업자, 유통업자, 중소기업 등은 신용정보주체로부터 신용정보의 제공 및 이용에 대한 동의를 얻어 두었어야 한다.

<table>
<tr><th>집중기관</th><th>등록대상</th><th>정보제공기관</th><th>이용기관</th></tr>
<tr><td rowspan="3">전국은행연합회</td><td>개인대출금(신용카드 현금서비스 포함)*</td><td rowspan="3">금융회사</td><td rowspan="3">금융회사</td></tr>
<tr><td>채무보증현황 (보증일자/보증금액)</td></tr>
<tr><td>가계당좌예금, 당좌예금, 신용카드 거래처</td></tr>
<tr><td rowspan="3">신용조회업자</td><td>신용거래자 및 구매자</td><td rowspan="3">비금융회사 (백화점, 의류업계, 이동통신업체 · PC통신업체 등)</td><td rowspan="3">금융회사 및 비금융회사</td></tr>
<tr><td>카드 개설자 및 구매자</td></tr>
<tr><td>신용거래자의 연대보증인</td></tr>
</table>

* 금융회사별로 5백만원 이상 1천만원 미만의 개인대출금과 신용카드 현

금서비스금액는 2002.9.1부터 금융회사에 제공되며 5백만원 미만은 2003.1.1부터 금융회사에 제공됨

(iv) 신용불량정보는 본인동의 없이도 등록되고 있으며, 등록일 1개월 전까지 채무자에게 통보한 후 전국은행연합회에 신용불량정보가 등록된다.

신용불량정보의 등록 및 집중시기

집중기관	등록대상	등록사유	집중시기	이용기관
전국은행연합회	대출금연체	30만원 초과금액을 3개월이상 연체 다만, 30만원 이하라도 3건이상을 3개월이상 연체시에는 등록	신용정보협의회가 정함	금융회사
	신용카드대금 · 카드대출 연체			
	할부금 연체			
	대위변제 · 대지급금	대지급금 · 구상채무 등을 3개월 이상보유		
	어음 · 수표 부도발생	가계 · 당좌수표, 약속어음 부도시		
	금융질서 문란행위	금융사기, 부정대출, 허위서류제출, 대출금용도외 유용 등		

* 종전에는 금융회사이외에 이동통신사업자, 백화점사업자, 중소기업 등이 신용조회업자에게 연체정보, 외상판매미수금 등을 신용불량정보로 등록하였으나 '02.7.1부터 신용조회업자는 신용불량정보를 등록할 수 없도록 변경됨

(v) 공공기록정보

공공기록정보는 국세청 · 지방자치단체 등에 의하여 전국은행연합회에 집중되고 있다.

공공기록정보의 등록

집중기관	정보종류	등록사유	집중시기	기록보존기간	이용기관
전국은행연합회	국세/지방세 체납	1년 이상 또는 1년에 3회이상 500만원 이상 체납자	신용정보협의회가 정함	없음	금융회사
	행정제재	미귀국 병역의무자 등			
	부실채권인수	한국자산관리공사가 인수한 부실채권 차주		500만원 초과 보유거래처의 경우 1~2년	

(바) 개인신용정보의 이용제한

법은 개인신용정보는 당해 신용정보주체와의 금융거래등 상거래관계의 설

정 및 유지여부 등의 판단목적으로만 제공·이용되어야 한다고 규정하고 있다.

다만, 개인이 서면에 의하여 금융거래등 상거래관계의 설정 및 유지여부 등의 판단목적 외의 다른 목적에의 제공·이용에 동의하거나 개인이 자신의 신용정보를 제공하는 경우나 신용정보업자 및 신용정보집중기관 상호간에 집중관리·활용하기 위하여 제공·이용되는 경우나 채권추심, 고용, 인·허가의 목적 등 대통령령이 정하는 목적으로 사용하기 위하여 제공·이용되는 경우에는 그렇지 않다(법 제24조 제1항). 그런데 예외규정으로 명시된 것 중에서 고용의 목적으로 신용정보를 이용할 수 있다는 것은 당사자의 동의없이도 고용의 목적으로 신용정보를 제공받을 수 있다는 내용인데, 구직자의 프라이버시를 과도하게 침해하는 규정으로 문제가 있는 조항이다.

(5) 신용불량자 등록[102]

(가) 신용불량자의 정의

(i) 현행규정

법에는 명시적으로 신용불량자의 정의가 없다. 다만 대통령령 제2조 제1항 제3호의 정보 즉, '금융거래 등 상거래와 관련하여 발생한 연체·부도·

---

102) 전국은행연합회는 2002년 9월말 현재 신용불량자 관리현황을 다음과 같이 공개하였다.
* 2002년 9월말 현재 개인신용불량자는 2,455,127명으로 전월대비 73,410(3.08%)이 증가하였음.
 - 은행, 카드사, 할부금융사, 상호저축은행에서 등록한 신용불량자수 증가가 주요인임.
* 연령별 및 금액별 현황 (단위 : 천명, %)

연 령 별 금 액 별(2002.9.30)

구 분	2001.12.31	2002. 9.30	구 분	누적인원	누적비율
10대	12(0.5)	9(0.4)	50만원미만	98	4.0
20대	408(16.7)	423(17.2)	100만원미만	241	9.8
30대	704(28.7)	703(28.6)	500만원미만	859	35.0
40대이상	1,326(54.1)	1,320(53.8)	1000만원미만	1,268	51.6
계	2,450(100.0)	2,455(100.0)	1000만원이상	1,187	48.4

대지급 또는 허위 기타 부정한 방법에 의한 신용질서 문란행위 등 신용정보주체의 신용도를 판단할 수 있는 정보로서 거래의 종류, 거래당사자의 성명 또는 상호, 연체·부도·대지급등의 금액과 발생·해소 등의 시기 등의 정보'를 시행령에서는 신용불량정보라고 부르고 있다.

(ii) 개정방향

이러한 신용불량정보는 현대사회에서 개인에 대한 경제적, 사회적 블랙리스트로 작용하게 된다.[103] 더구나 신용불량정보에 대해서는 당사자의 항변도 인정되지 않으며, 현대사회에서 신용의존도가 높아지고 있고, 신용불량정보

---

103) 신용불량자가 안게되는 문제점에 대하여 잘 정리한 글이라서 길지만 인용을 한다.
"신용불량자가 양산되는 모습은 앞으로 우리 경제에 몇 가지 어두운 그림자를 드리울 것으로 예상된다. 첫째는 신용불량자 자신에 대한 문제이다. 일단 개인이 신용불량자로 등록되는 경우, 해당자에 대한 경제적 불이익은 지금까지 상상한 것 이상으로 개인에게 크나큰 타격을 줄 것이다. 일반적으로 생각할 때 어느 사람이 신용불량자가 되었다면 앞으로 은행이나 금융기관과 거래를 하지 않으면 되지 않겠느냐고 쉽게 생각할 수 있을 것이다. 그러나 이런 생각은 크게 잘못된 것이다. 왜냐하면 오늘날 경제생활 속에서 금융기관과 거래를 할 수 없다는 것은 실질적으로 그 사람의 경제활동을 봉쇄하는 것이나 마찬가지가 될 것이기 때문이다. 한 예로 어느 개인이 신용불량자로 등록되어 있는 경우, 취직자리를 찾는 것부터 어려움을 겪게 될 것이다. 어느 회사가 신용불량자를 사원으로 채용하려 할지 한 번 생각해 보라. 비록 운이 좋아서 취직이 되었다 하더라도 대출금이나 카드대금이 연체되어 신용불량자가 되었다면 은행이나 카드회사가 월급에 대한 압류조치를 통하여 미수된 대금을 회수하려고 할 터이니 경제생활이 불안하기 짝이 없을 것이다. 더욱이 앞으로는 신용불량자로 등록되는 경우 그 정보를 모든 종류의 금융기관이 서로 공유하여 알 수 있게 됨으로써 어떤 종류의 금융거래도 하기가 어려워지게 된다. 이를테면 신용카드를 발급받을 수 없으므로 모든 결제를 현금으로 하여야 한다. 따라서 친구들과 점심을 하고 대금을 낼 때에도 신용카드가 없으니 현금으로 지불해야 하는 모습을 보여야 한다.
또한 신용불량자가 증권거래를 하기 위하여 증권회사에 계좌를 열 때에도 신용불량자로 등록되어 있으므로 여러 가지 불이익을 받게 된다. 따라서 우리 경제생활에 있어 중요한 증권거래에서조차 제약을 받게 되는 것이다.
그뿐만 아니라 앞으로 집을 장만하기 위하여 은행에서 대출을 받고자 할 때에도 신용불량자에게는 주택구입을 위한 대출이 허용되지 않을 것이다. 게다가 신용불량자가 개인 사업이라도 하기 위하여 금융기관과 접촉하는 경우, 대출은 물론이고 당좌계좌를 개설하는 것조차 여의치 않을 것이다. 이와 같이 크게는 금융기관과의 거래가 어려워질 뿐만 아니라 작게는 그 흔한 전자상거래에서 책이나 가전제품을 구입하려고 해도 신용카드가 없으니 거래를 할 수가 없을 것이다.
이처럼 신용불량자가 앞으로 경제생활 속에서 당면할 문제들을 꼼꼼히 생각해 보면, 이는 단순히 금융거래에서만의 문제가 아니라, 신용불량자들이 제대로 경제생활을 할 수 없게 되는 것을 의미한다. 따라서 신용불량자가 된다는 것을 간단한 문제로 볼 것이 아니라 앞으로 경제활동에서 입을 여러 가지 손해나 장애를 심각히 받아들여야 할 것이다."(곽수일, 신용불량자의 비참함 중에서, 금융 2002. 10.)

에 대한 접근가능성도 커지고 있는바, 한번 신용불량자로 등재가 되면 그로 인한 개인의 사회, 경제적 폐해는 이루 말할 수가 없다. 따라서 이런 점을 고려하여 법률에서 신용불량정보의 범위를 분명히 규정하여, 허용되는 신용불량정보가 아닌 정보로 함부로 신용불량자로 등재하는 것을 막아야 한다. 예컨대 통신사업자들이 통신요금 미납자에 대한 정보를 집중관리하면서 신용불량자로 등재하여 블랙리스트로 활용하는 것이나, 백화점 카드의 미납정보를 집중관리하여 블랙리스트로 활용하는 것들은 허용되어서는 안된다.

또한 신용불량자로 등재되는 자의 범위도 대폭적으로 줄여야 한다. 현재의 기준은 너무 쉽게 신용불량자로 등재되게 함으로써 채권회수에 압박을 가하기 위한 목적으로만 활용되고 있다. 또한 신용불량자 등재절차는 매우 엄격한 요건을 정해 놓아야 한다.

(나) 신용불량정보와 신용불량정보 대상자

시행령은 종합신용정보집중기관을 통하여 집중관리·활용되는 신용정보의 범위에서 개인의 경우, 대출금등의 연체, 용도의 유용사실, 지급보증대급금(또는 대위변제) 발생사실, 어음 또는 수표거래정지처분을 받은 사실, 신용카드대금 미결제등 신용카드거래질서를 문란하게 한 사실, 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실을 종합신용정보집중기관을 통하여 집중관리, 활용되는 신용불량정보로 규정하고 있고, 기업의 경우에는 대출금등의 연체, 용도의 유용사실, 지급보증대급금(또는 대위변제) 발생사실, 신용보증대급금 발생사실, 어음 또는 수표거래정지처분을 받은 사실, 리스자금 또는 리스료의 연체사실, 신용카드대금 미결제등 신용카드거래질서를 문란하게 한 사실, 무보증사채상환불이행사실, 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실을 신용불량정보로 규정하고 있다. 한편 금융감독원이 제정한 신용정보업감독규정은 농수협을 포함한 은행의 어음, 수표 부도사실을 신용불량정보로 추가하고 있다.

한편 종합신용정보집중기관인 전국은행연합회는 신용정보관리규약(2002. 7.)에서 다음 각호의 1에 해당하는 사유를 발생시킨 거래처를 신용불량정보 대상

자로 규정하고 있다. 1. 대출금 등의 연체, 용도외 유용사실, 2. 지급보증대지급금(또는 대위변제) 발생사실, 3. 신용보증대지급금 발생사실, 4. 어음 또는 수표부도사실(2002. 4. 26. 신설), 5. 어음 또는 수표거래정지처분을 받은 사실, 6. 리스자금 또는 리스료의 연체사실, 7. 신용카드대금 미결제등 신용카드거래질서를 문란하게 한 사실, 8. 무보증사채 상환불이행 사실, 9. 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실, 10. 손실을 초래케 한 사실 등.

한편 개별신용정보집중기관인 생명보험업협회의 경우는 신용정보관리규약에서 전국은행연합회와 동일한 조항을 두고 있다.

(다) 신용불량자 등재절차

(i) 현행규정

법은 신용정보업자등이 제공받은 신용정보를 근거로 개인에게 신용불량자 등록 등 대통령령이 정하는 불리한 조치를 취하고자 하는 때에는 재정경제부령이 정하는 바에 의하여 미리 당해 개인에게 통보하여야 한다고 규정하고 있다(법 제24조 제3항). 이에 의하여 재정경제부령은 신용정보업자등이 개인의 신용불량정보를 신용정보집중기관을 통하여 집중관리·활용하는 행위를 하고자 하는 때에는 당해 조치를 취하기 1월 전까지 자신이 알고 있는 당해 개인의 최종주소지로 그 내용을 서면으로 통보하여야 한다고 규정하고 있다(시행규칙 제12조).

(ii) 개정방향

신용불량자 등재절차에 관하여는 시행규칙이 아닌 법률에서 상세한 규정을 두는 것이 바람직하다.

(라) 신용불량자 등재의 말소

(i) 현행규정

신용불량자 등재기록의 보유기간과 폐기기간 등에 대하여 법에는 아무런 규정을 두고 있지 않다. 다만 금융감독원이 제정한 신용정보업감독규정은 (i) 신용정보집중기관 및 신용정보업자에게 등록되는 어음부도거래정보를 제외한 신용불량정보의 경우는 불량해제사유의 발생일로부터 최장 5년의 기간 내에서 관리하며 등록사유발생일로부터 7년이 경과한 경우에는 7년이 경과한 날을 당해 신용불량정보의 불량해제사유 발생일로 본다, (ii) 어음부도거래정보를 제외한 신용불량정보는 다음 각호에서 정한 기간이 만료된 이후에는 신용정보집중기관 또는 신용정보업자에게 등록할 수 없다. 1. 불량사유 발생일로부터 7년, 2. 소멸시효가 완성된 채권관련정보는 소멸시효기간이 완성된 날, (iii) 신용정보제공ㆍ이용자 및 신용정보업자가 신용정보집중기관으로부터 입수하여 활용하는 신용불량정보의 관리기간은 당해 신용불량정보를 제공한 신용정보집중기관이 정하는 관리기간을 따른다고 규정하고 있다(제11조).

(ii) 개정방향

등재말소절차도 법률에서 규정하고 있어야 할 것이다. 불량해제사유의 발생일로부터 5년까지 관리할 수 있다고 한 것은 지나치게 길다. 원칙적으로 불량해제사유가 발생하면 즉시 기록을 폐기하는 것으로 바꾸어야 할 것이다.

(6) 조회기록, 신용정보의 보존기간 등

현재 신용조회업자는 개인신용정보 조회서비스를 이용하는 회원에 대해 개인신용정보 조회시 과거 조회기록을 제공하고 있다고 한다. 일부 금융회사에서는 이때에 제공되는 조회기록을 가지고 개인의 신용도를 판단하는 참고자료로 쓰거나, 때로는 금융거래를 기피하는 수단으로 사용하기도 한다고 한다. 신용조회업자가 과거 조회기록을 제공하는 것은 법적 근거가 없는 것이다.

또한 각 금융기관이나 신용정보제공ㆍ이용자들은 수집하여 보유하고 있는 일부 신용정보를 기간의 제한없이 무기한 보존하고 이용한다고 한다. 이것 역시 위법한 것으로 보아야 할 것이다.

2. 보험관련 정보의 보호

가. 보험관련 정보의 보호 필요성

(1) 보험관련 정보 수집의 필요성

보험은 위험의 사회적 분산을 통하여 보험계약자에게 예측가능성을 보장해 주고, 이를 통하여 생활의 안정을 가져다 준다. 보험이 담당하는 이러한 기능이 효과적으로 작동하도록 하기 위해서는 보험계약자 집단의 위험도를 정확하게 판단하여 보험계약자 집단의 균질성을 확보하고, 위험도에 따른 합리적인 비용의 분담이 이루어질 수 있도록 해야 한다. 즉, 보험의 실패를 야기하는 '역선택'(adverse select)과 '도덕적 해이'(moral hazard)를 방지하여 보험이 공정하고 건전하게 운용되도록 하기 위해서는 보험계약자와 보험사고에 대한 정확한 정보의 파악 - 보험계약자에 대한 정확한 위험도의 측정을 통해 보험계약이 공정하게 체결되도록 해야 하고, 보험사기의 방지, 타당한 보험금 산정과 지급 등을 위하여 보험사고와 관련된 정보를 수집 - 이 필요하다. 어찌보면 정보가 정확하면 정확할수록 '역선택'과 '도덕적 해이'는 줄어들게 되고 보험은 더욱 투명해지고 공정해질 수 있는 것이다.

(2) 보험관련 정보 보호의 필요성

(가) 수집되는 정보의 민감성과 정보수집 제한의 필요성

이러한 이유로 보험회사는 보험계약자에 대한 개인정보와 보험사고에 대한 정보를 수집하게 되는데, 보험회사는 공정한 보험계약의 체결, 보험사기의 방지, 타당한 보험금의 산정과 지급을 위하여 보험가입자에 대하여 가능한 한 많은 정보를 수집하려고 한다. 그런데 여기에는 개인의 병력(病歷)에 관한 정보와 개인의 의료정보 및 개인의 내밀한 정보에 해당하는 보험사고에 대한 정보들이 많이 포함되게 된다. 그런데 보험회사가 수집하는 개인정보는 그 성질상 매우 내밀한 것이 될 수 밖에 없는바, 보험회사가 보험계약

의 체결, 유지와 관련하여 무제한적으로 정보수집을 허용하는 경우에는 보험가입자의 인격권, 프라이버시권이 침해될 수 있다. 따라서 개인정보 수집에 대하여 지나친 인권 침해를 야기하지 않도록 적정한 범위를 제한해야 하고, 수집방법의 적정성을 유지하도록 기준이 마련되어야 한다.

(나) 보험의 사회보장적 기능과 불합리한 차별을 막기 위한 정보수집의 제한의 필요성

보험회사가 보험계약 체결시에 개인정보를 오용하거나 남용하여 보험계약의 체결을 거절하거나, 높은 보험료를 요구하여 보험계약자를 차별대우할 위험이 있다. 특히 보험은 아무리 민간영리보험이라 하더라도 어느 정도는 위험의 사회적 배분을 통한 사회부조의 역할을 담당하게 되는데, 사회적, 경제적, 신체적 약자에 대하여 어떤 위험의 분산도 감수하지 않으려고 하고 위험도가 높다는 이유로 이들의 보험가입을 거절한다면 이것은 보험의 공공성에 반하는 것으로 바람직한 현상으로 보기는 어렵다.

그리고 보험회사가 보험가입 희망자로부터 보험계약과는 직접적인 관련이 없는 병력에 대한 정보를 수집하거나, 유전자 정보를 수집한다면 이러한 정보는 보험가입 희망자의 위험도를 평가하는데 부당하게 이용될 가능성이 높다.

(다) 엄격한 비밀보장과 유출금지의 필요성

보험관련 정보는 보험목적을 위하여 수집되는 것이므로 엄격하게 보험목적을 위해서만 이용되어야 하며, 철저하게 비밀이 보장되어야 하고, 외부로의 유출이 금지되거나 제한되어야 한다. 그리고 보험관련 정보는 정확도가 높고 매우 상세하기 때문에 보험회사가 이를 마케팅의 목적으로 사용하고자 하는 유혹을 갖게 되는바, 보험회사에 의한 보험관련 정보의 유용도 엄격하게 제한되어야 한다.

나. 보험정보의 보호에 관한 원칙[104)]

(1) 수집과 처리의 제한에 대한 원칙

보험관련 정보는 보험계약의 체결과 이행을 위하여 필요한 최소한의 범위 내에서만 수집되어야 한다. 즉, 보험계약 체결의 준비나 체결을 위해, 보험료 수금과 청구서 작성을 위해, 보험금 청구 및 기타 보험혜택의 부여에 대한 판단을 위해, 재보험이나 공동보험을 위해, 보험사기의 방지와 조사 및 수사를 위해, 법적 분쟁을 준비 또는 제기하거나 방어하기 위해, 다른 특별한 법률이나 계약에 따른 의무의 이행을 위해, 보험 통계의 작성을 위해서 필요한 최소한의 범위 내에서만 수집되어야 한다[105]. 그리고 개인정보의 수집시에는 당사자로부터 직접 수집하는 것을 원칙으로 하여야 하고, 특히 의료정보의 수집과 처리는 의학전문가나 그에 준하는 비밀준수의무를 지는 사람에 의하여 처리되어야 한다.[106] 그리고 수집되는 정보는 정확하고 최신의 것이어야 한다[107]

(2) 정보주체의 권리

보험관련 정보를 수집할 때에는 정보주체에게 정보수집의 목적과 수집되는 정보의 범주와 내용, 제3자에게 제공되는 경우에는 어떤 목적 하에서 어떤 정보가 누구에게 제공되는지를 분명하고 알기 쉽고 정확하고 알려야 한다. 그리고 정보주체가 미성년자인 경우에는 당사자와 법정대리인으로부터 동의를 얻어야 하며, 무능력자인 경우나, 동의를 할 수 없는 부득이한 상태에 있는 경우에는 법정대리인으로부터 동의를 얻되, 이 때에도 당해 정보주체의 권리와 이익을 해치지 않는 범위 내에서 동의가 이루어져야 하고, 당사자의 의사를 최대한 존중하여야 한다[108]. 특히 정보주체가 태아인 경우에도 태아에게 정보수집에 대한 동의권을 인정하되 그 행사는 부모가 하도록 하

104) COUNCIL OF EUROPE COMMITTEE OF MINISTERS Recommendation Rec(2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes
105) 4.1. 이 지침은 여기에 보험상품의 개발을 위하여 수집하는 경우와 보험회사의 내부적인 경영을 위하여 수집하는 경우를 더하고 있다.
106) 위 지침 3.2
107) 위 지침 4.1
108) 위 지침 4.2

여 부모의 동의를 얻도록 하여야 한다. 그리고 정보주체에게는 보험회사가 수집하는 개인정보를 제공하지 않아도 되는 경우에는 그 점에 대하여 고지를 받아야 하고, 이때 해당 정보를 제공하지 않을 경우에 어떤 효과가 있는지에 대해서도 고지를 받아야 한다.

그리고 정보주체는 자신의 정보에 접근하여 이를 열람하고, 잘못된 것이 있는 경우에는 해당 정보를 수정하거나 삭제할 수 있는 권리가 있어야 한다. 또한 정보주체는 자신의 정보를 누가 관리하고 있는지, 어떻게 관리하고 있는지, 보안은 어떻게 유지하고 있는지에 대하여 고지를 받을 수 있어야 한다.

(3) 보험관련 정보의 이용

보험관련 정보는 엄격하게 보험계약의 체결이나 이행과 관련한 목적으로만 이용되어야 한다. 당사자의 명시적인 동의가 있지 않는 한 보험관련 정보를 보험목적 외의 목적으로 이용해서는 안된다. 그리고 보험관련 정보는 당사자의 동의를 받거나 법률이 허용하는 경우 외에는 제3자에게 제공되어서는 안된다. 그리고 만약 보험관련 정보가 제3자에게 제공되는 경우에는 제공된 제3자, 제공된 정보의 내용, 제공의 목적 등에 대하여 정보주체에게 고지가 되어야 한다.

(4) 민감한 정보

보험관련 정보 중에서 특별히 민감한 정보는 의료정보와 형사기록에 관한 정보이다. 따라서 이러한 정보는 특별히 엄격히 관리되어야 하고, 그 이용도 제한되어야 한다. 예컨대 이러한 민감한 정보는 수집시 정보주체의 서면동의를 얻도록 하고, 그 이용은 보험사기를 막고, 보험금 지급이나 보험 혜택의 부여와 관련한 보험 목적으로만 이용되어야 할 것이다[109].

한편 유전자 검사처럼 과학성이 입증되지 않은 검사방법은 오용되어 보험

109) 위 지침 4. 7

가입자를 차별대우하는 데 사용될 수 있고, 인권침해의 요소가 크기 때문에 보험회사에서 보험가입자나 피보험자의 유전자 검사를 하는 것은 금지하는 것이 바람직할 것이다.

(5) 보안

보험관련 정보의 보존은 엄격한 수준의 보안이 유지되어야 한다. 따라서 보험관련 정보에 접근할 수 있는 자의 범위와 보안수칙 등이 마련되어 있어야 하고, 정보가 안전하게 보존될 수 있도록 엄격한 기술적 보안장치가 마련되어 있어야 한다.

(6) 자동화된 보험관련 결정

보험과 관련한 회사의 결정이 자동화된 처리장치에 의하여 내려지는 경우에는 자동화된 처리장치에만 의존하여 결정이 내려져서는 안될 것이다. 자동화된 처리장치는 오류의 위험이 있으며, 정보주체의 항변권이 제대로 보장되지 않기 때문이다. 따라서 자동화된 처리장치에 의하여 결정이 내려질 경우에는 그와 함께 반드시 사람이 판단을 할 수 있는 절차가 마련되고, 정보주체의 항변기회를 제공해야 할 것이다.

다. 우리나라 현행법의 평가

우리나라 현행법상 보험관련 정보에 대해서는 법률의 규정이 제대로 마련되어 있지 않다. 다만, 신용정보에 대하여는 신용정보의 이용 및 보호에 관한 법률에 의하여, 전산망으로 처리되는 정보에 대하여 정보통신망 이용촉진 및 정보보호등에 관한 법률에 의하여 보호가 될 뿐이다. 따라서 보험관련 정보에 대한 보호에 대한 규정을 신설하여야 할 것이다.

3. 위치정보의 보호

가. 위치정보 기반산업의 발달과 위치정보의 이용현황

최근 무선인터넷과 모바일 컴퓨팅 기술의 급속한 발전으로 다양한 위치기반서비스(Location Based Service)가 개발, 제공되고 있다. 일반적으로 위치기반서비스란 “이동통신망을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하는 응용시스템 및 서비스”라고 정의된다(22). 오늘날 위치기반서비스가 주목받는 이유는 크게 3가지 측면이 있다고 한다. 첫째, 위치기반서비스는 소위 엠커머스(mobile commerce)를 현실적으로 가능하게 하기 때문이라고 한다. 즉, 위치기반서비스를 기반으로 다양한 사용자 위치 기반의 엠커머스가 가능하며, 위치기반서비스가 없다면 엠커머스는 가능하지 않다. 둘째, 위치기반서비스의 도입으로 다양한 응용서비스가 가능하게 됨으로서 이동통신사의 수익을 극대화할 수 있기 때문이라고 한다.(22) 셋째, 위치기반서비스는 향후 급성장할 차량 인터넷 서비스(automotive telematics : 움직이는 차량을 대상으로 제공되는 무선인터넷 서비스)의 핵심기술이기 때문이라고 한다. 이것은 2010년에 시장규모 50조원으로 성장할 것으로 전망된다고 한다.(23)

위치기반서비스에는 비상구조지원 서비스, 각종 위치정보 서비스, 트래픽과 네비게이션 정보서비스(교통량 및 교통정보 등), 위치밀착형 빌링 서비스, 지능형 교통정보 서비스 등이 있는데, 앞으로 다양한 신규분야가 생겨날 것으로 보인다(25).

위치를 측정하는 기술로는 삼각형의 네트워크 망을 이용하는 방법, GPS(Global Positioning System)를 이용하는 방법 과 양자를 결합하는 방식 등이 있다. 삼각형의 네트워크를 이용하는 방식은 이용자로부터 가장 가까운 곳에 있는 세 개의 네트워크 전송탑으로부터 무선 전파신호를 수집하여 이용자의 위치를 계산하여 위치를 측정하는 방식이며, GPS 방식은 항상 같은 위치에 있는 24개의 위성을 이용하는 방식이다. 이 경우 GPS 처리 장치가 단말기에 부착되어 위성으로부터 수신한 GPS 정보를 이용하여 위치를 측정하는 방식이며, 혼합형은 이 두가지를 결합한 방식이다[110].

110) 미국 연방공정거래위원회 공개 워크샵 (2002. 2.) The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues. 8페이지

위치정보란 특정한 시점에서의 개인의 위치를 파악할 수 있는 모든 정보를 말한다고 정의한다면 법률적 관점에서 보호의 수준을 정하기 위하여 위치정보를 다음과 같이 나누어 볼 수 있을 것이다[111].

(i) 고정위치를 나타내 주는 정보(주소, 전화번호, 차량번호, IP 주소 등) : 현재의 상태를 알려주는 것이 아닌 고정된 생활공간에 대한 정보이다.
(ii) 특정 시점의 고정위치를 나타내 주는 정보(전화의 발신자, 수신자 번호 등) : 전화의 발신자와 수신자의 번호는 발신자와 수신자의 위치를 파악할 수 있는 정보가 될 수 있다. 여기에 발신 또는 수신시간이 결합되면 특정시점의 개인의 위치정보가 된다.
(iii) 특정 시점의 고정위치를 나타내 주는 정보로서 위치 및 활동내용이 파악되는 정보(정보의 내용에 인터넷에 남겨진 IP 주소) : 특정시점에서 컴퓨터가 인터넷에 연결되는 IP 주소는 특정시점에서 특정인의 위치정보가 된다. 한편 IP 주소는 통신의 내용이 함께 파악된다는 점에서 다른 위치정보와 차이가 있다.
(iv) 특정시점의 이동하는 특정위치를 나타내 주는 위치정보(이동전화 등의 발신지 정보, GPS 기타 다양한 방법을 이용하여 파악한 현재의 위치정보, 신용카드의 이용정보) : 다양한 방식에 의하여 현재의 위치를 파악하여 알려주는 위치정보들로서 특정시점의 특정위치를 나타내 주기 때문에 가장 민감한 위치정보이다. 신용카드의 이용정보도 신용카드를 이용한 가맹점이 밝혀질 경우에는 위치정보로서 역할을 할 수도 있다.

우리나라의 경우 현재 다양한 위치기반 서비스가 제공되고 있고, 새롭게 연구개발되고 있다. 위치추적을 통한 비상구조지원 서비스도 활성화되었으며, 각종 위치정보 서비스(지도찾기, 친구찾기, 물류정보서비스 등), 트래픽과 네비게이션 정보서비스(교통정보서비스, 자동항법서비스), 이동전화를 통한 각종 콘텐츠 제공서비스 등이 서비스되고 있다[112].

---

111) 위치정보를 특정시점에서의 특정위치를 파악할 수 있게 해 주는 정보라고 정의한다면 (4)만 해당할 것이다. 여기에서는 나머지 (1)-(3)의 덜 민감한 정보도 위치정보로 보고 그에 대한 보호방안도 함께 서술하였다.

112) 정보통신부 입법안 해설자료
o 이동통신업체와 같은 통신사업자가 위치정보(기지국 정보, GPS 정보)를 수집할 수 있는 특정장치를 단말기와 통신망에 설치하여 자사의 통신서비스 가입자를 상대로 LBS를 제공

나. 위치정보의 특성과 보호필요성 및 보호의 수준

(1) 위치정보의 특성과 악용가능성

개인의 위치를 파악할 경우 이를 통해서 그 개인의 활동영역과 활동내용을 파악하거나 추측할 수 있다. 특히 이동전화나 PDA 등을 이용하여 위치정보를 파악하는 경우에는 개인들이 일상생활에서 대부분을 이런 장치들을 가지고 있기 때문에 축적되는 개인의 위치정보의 양은 그 개인의 거의 모든 생활영역을 포괄하므로 과도한 사생활 침해의 결과를 낳는다. 일반적으로 개인들은 자신의 위치를 알리려고 하지 않을 경우가 많으며, 때에 따라 개인의 위치는 개인의 매우 민감한 사생활을 침해할 수도 있다. 결국 위치정보는 개인의 행동의 자유와 양심의 자유를 심각하게 침해할 수 있으며, 내밀한 사생활의 자유가 침해될 수도 있기 때문에 위치정보에 대해서는 특별한 보호가 필요하다.

위치정보가 악용될 가능성은 다음과 같다.

(i) 기업에서 영리적 목적으로 악용

기업에서 개인의 위치정보를 영리적으로 활용하기 위하여 개인의 위치정보를 수집·분석하는 경우, 이로써 개인의 성향을 파악할 수 있는바, 이는 개인의 사생활을 심각하게 침해할 것이며, 이것은 제3자에게 유출되거나 불법적으로 거래되어도 확인하기도 어렵기 때문에 이메일 주소처럼 불법적으로 유출되거나 다른 업체에 판매될 가능성도 매우 높다. 개개인의 위치정보 분

※ 이동통신사업자의 '내친구 찾기 서비스', '주변식당 찾기 서비스' 등

o 보험회사, 물류업체, 경호회사 등은 해당 위치기반서비스를 제공하기 위하여 고객의 동의를 얻어 고객의 차량, 단말기 등의 위치정보 수집장치를 부착하고, 통신사 통신망을 통해 전달받은 위치정보를 가공·처리하여 자사 고객에게 긴급구난, 최적배차 관리, 긴급출동 등의 LBS를 제공

※ 삼성화재(찾아가는 서비스)는 고객차량에 GPS를 부착한 후 차량사고 발생시 차량위치를 KTF 통신망을 통해 삼성화재센터에서 접수 후, 긴급출동 서비스 제공

※ SK(주)(entrac)은 GPS 기기와 특정휴대폰을 물류차량 등에 제공한 후, 차량위치를 SKT 통신망을 통해 엔트랙 센터로 전송받아, 주문연계, 최적배차 서비스를 제공

o 부가통신업체 등이 허가 없이 사용할 수 있는 무선망이나 CCTV 등을 활용하여 파악한 위치정보를 통신망을 통해 수집·가공한 후, LBS를 제공

※ 교통정보 전문회사인 로티스는 계약차량에 위치확인 모뎀을 부착한 후 200MHz대역 무선망을 통해 차량위치를 수집하여, 시간대별, 구간별 정체상황, 최적경로 등을 제공

석 데이터베이스의 공유와 유통이 횡행할 가능성이 높다. 그 결과로써 밀착 마케팅이 개인의 평온한 생활을 깨뜨릴 가능성도 크다.

(ii) 사생활의 폭로나 명예훼손에의 악용

개인의 위치정보가 개인의 사생활을 폭로하거나 개인의 명예를 훼손하는데 이용될 수 있다. 특히 유명인사나 정치인의 경우 그 위험은 더욱 클 것이다. 그리고 이혼소송에서 위치정보가 사생활을 폭로하는 방법으로 사용될 가능성이 높다.

(iii) 노동통제의 강화

고객서비스의 강화나 서비스 품질의 개선이라는 명목으로 개인의 위치정보가 직장에서 활용될 가능성이 높다. 이 경우 개인의 위치를 실시간으로 파악하게 되면 개인의 인권이 침해될 것이며, 이는 부당한 노동통제이다. 모니터링한 위치정보를 근무평정에 활용할 경우 노동강도가 높아지게 된다.

(iv) 범죄수사에서의 악용

위치정보를 범죄수사에서 활용하게 되면, 남용될 가능성이 높다. 이 경우 심각한 인권침해의 문제가 생길 것이다.

(v) 사생활의 노출

위치정보로 인하여 개인의 활동이 보다 공개적으로 노출되게 될 것이다. 이는 전 사회적으로 사생활의 보호가 위축되는 것을 의미한다. 대부분의 사람들이 위치정보서비스에 대한 광고와 위치정보서비스의 편리함 때문에 위치정보의 제공에 동의하게 될 경우 사회적으로 프라이버시 의식이 떨어지게 될 것이다. 특히 일반 소비자들은 위치정보서비스를 이용하면서 그들의 위치정보가 얼마나 정확하며, 어떻게 이용되고 악용될 소지가 있는지에 대하여 잘 모르고 해당 서비스를 이용할 가능성이 높다고 한다.[113]

113) Davidson, Center for Democracy and Technology

(2) 위치정보는 어느 정도로 보호되어야 하는가

위치정보에 대한 적절한 보호의 수준은 그 위치정보의 정확도에 따라서 편차가 있을 수 있으나, 기본적으로 위치정보와 침해의 정도나 민감성에 있어서 유사한 '통신의 내용에 대한 보호'의 수준은 되어야 할 것이다. 즉, 요금부과의 목적으로 수집되는 고정된 전화번호에 대해서는 따라서 위치정보는 개인의 고정된 특성이나 을 식별하는데 그치는 일반적인 개인정보에 비해서 매우 민감한 개인정보로 특별하게 보호되어야 할 것이다. 위치정도에 대한 보호의 정도가 어떠해야 할지에 대하여 에 해당한다는 점에 대해서는 이견이 있을 수 없다. 다. 위치정보에 대한 보호의 정도 위치정보에 대한 보호의 정도는 통신이나 대화에 대한 보호의 수준에 이르러야 할 것이다.

앞에서 본 범주에 따라 각각의 위치정보에 대해 요청되는 보호의 수준을 다음과 같이 정리해 볼 수 있다.

(i) 고정위치를 나타내 주는 정보(주소, 전화번호, 차량번호, IP 주소 등) : 민감한 정보로 보호해야 함

현재의 상태를 알려주는 것이 아닌 고정된 생활공간에 대한 정보이기 때문에 일반적인 개인정보의 보호수준에 따르면 될 것이지만, 생활공간에 대한 정보이기 때문에 상대적으로 민감한 정보에 해당한다고 볼 수 있다.

예컨대 미국의 경우 운전자 프라이버시 보호법(Drivers Privacy Protection Act of 1994)이 1989년 여배우 Rebecca Schaeffer의 자동차 등록 기록을 통해 주소를 알아낸 스토커에 의하여 살해되는 사건이 발생한 후 1994년에 제정되었는데, 이 법은 당사자의 동의가 없는 경우 자동차 등록정보(운전자의 이름, 주소, 전화번호, 사회보장번호, 면허증 번호, 사진, 신장, 체중, 성, 나이, 의료정보, 지문 등)의 제3자에게의 공개를 금지하고 있다. 단 연방이나 주정부의 합법적인 업무수행을 위해 필요한 경우나, 행정절차의 진행을 위해서나, 차량과 운전자의 안전을 위해 필요한 경우나, 자동차의 리콜을 위해 필

요한 경우나, 시장조사를 위해 필요한 경우 등에는 예외적으로 해당 기관이나 해당자에게 공개가 허용된다.[114]

(ii) 특정 시점의 고정위치를 나타내 주는 정보(전화의 발신자, 수신자 번호 등) : 통신의 비밀과 자유에 해당하는 경우 법원의 관여가 필요함

전화의 발신자 번호와 수신자 번호, 통화시간 등의 정보는 개인의 위치를 파악할 수 있는 정보가 되기도 하고, 사적인 내밀한 영역으로서 헌법상 보장되는 통신의 비밀의 보호대상이 되기 때문에 높은 수준으로 비밀보호가 되어야 한다. 그러므로 이러한 통화내역에 대한 정보는 통신사업자가 당해 통신서비스를 제공한 후 즉시 폐기하거나 익명으로 처리해야 한다. 단 요금청구의 목적으로 저장할 필요도 있을 것인데, 이 경우도 요금처리에 필요한 범위 내에서만 요금처리가 진행되는 동안만 보관을 허용해야 할 것이다. 그리고 수사기관에서 이를 수집할 때에는 법원의 관여가 필요하다. 그런데 우리 통신비밀보호법에서는 영장주의나 법원의 관여를 요구하지 않고, 검사장의 승인을 얻어 자료의 열람이나 제공을 요청할 수 있다고 규정하고 있어서 문제이다[115]. 한편 전기통신사업법에 의하면 수신자의 요구가 있는 경우에는 전기통신사업자는 송신인의 전화번호 등을 알려줄 수 있는데, 송신인이 전화번호 등의 송출을 거부하는 의사표시를 하는 경우에는 알려줄 수 없게 되어 있다. 단 이때에도 전기통신에 의한 폭언, 협박, 희롱 등으로부터 수신인을 보호하기 위하여 수신인이 요구하는 경우에는 알려줄 수 있다고 규정하고 있다[116].

한편 전화, 인터넷 통신을 포함한 모든 통신서비스에 적용되는 유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 1997. 12. 15. 지침(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)에서는 통

114) The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record (http://www.epic.org/privacy/drivers/)
115) 통신비밀보호법 제13조
116) 전기통신사업법 제54조의 2

신서비스 가입자나 통신서비스 이용자의 통신서비스 이용정보(traffic data)는 통신이 통신이 끝나면 삭제되거나 익명화되어야 한다고 규정하고 있다. 단, 가입자에 대하여 요금청구를 하거나 상호접속 요금의 지급을 위하여 가입자의 전화국의 번호나 식별정보, 가입자의 주소, 해당 요금부과 기간동안의 요금부과 대상 총 통화수, 걸려온 가입자의 전화번호, 유형과 시작시간과 지속시간 또는 전송된 데이터의 양, 전화나 서비스의 일자를 요금이 수금될 때까지 보관할 수 있다고 한다. 그리고 이용정보나 요금청구에 관련한 정보는 해당 업무를 처리하는 사람이나 고객의 질의에 답하는 사람, 사기행위를 감시하거나 분쟁해결을 위하여 법적으로 허용되는 경우에만 접근가능하도록 하고 있다[117].

(iii) 특정 시점의 고정위치를 나타내 주는 정보로서 위치 및 활동내용이 파악되는 정보(정보의 내용에 인터넷에 남겨진 IP 주소) : 통신의 비밀과 자유에 해당하며, 통신의 내용이 공개되므로 수사기관에서 수집할 경우에는 영장주의가 적용되어야 하며, 통신서비스 제공자는 요금부과 목적으로 필요한 경우에만 보관하고 즉시 폐기

특정시점에서 컴퓨터가 인터넷에 연결되는 IP 주소는 특정시점에서 특정인의 위치정보가 되고, 이러한 IP 주소 정보는 통신의 내용이 함께 파악된다는 점에서 높은 수준의 비밀보호가 있어야 할 것이다. 따라서 원칙적으로 이러한 정보는 수집되어서는 안되고, 즉시 폐기하거나 익명으로 처리되도록 해야 할 것이다. 다만 인터넷 서비스 제공자(Internet Service Provider)가 이용자에게 충분하고 명확하게 수집의 목적, 수집하는 정보의 내용, 거절할 수 있는 방법과 절차 등을 설명하고 동의를 얻는 경우에만 IP 정보의 수집이 허용된다고 보아야 할 것이다. 그러나 우리 정보통신망 이용촉진 및 정보보호에 관한 법률에서는 단순히 명시 및 동의만을 규정하고 있다[118]. 한편 수사기관이 이를 수집하는 경우에는 엄격하게 영장주의가 적용되어야 할 것이다.

---

117) 유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 1997. 12. 15. 지침(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector) Aricle 6.

118) 정보통신망 이용촉진 및 정보보호에 관한 법률 제22조

그러나 우리 통신비밀보호법에서는 검사장의 승인을 얻어 수사기관에서 요청할 수 있다고 하고 있어서 문제이다[119].

한편 앞서 본 유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 1997. 12. 15. 지침(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)에 의하면 통신서비스 가입자나 통신서비스 이용자의 통신서비스 이용정보(traffic data)는 가입자에 대하여 요금청구를 하거나 상호접속 요금의 지급을 위하여 필요한 경우 외에는 통신이 통신이 끝나면 삭제되거나 익명화되어야 한다고 규정하고 있다[120].

(iv) 특정시점의 이동하는 특정위치를 나타내 주는 위치정보(이동전화 등의 발신지 정보, GPS 기타 다양한 방법을 이용하여 파악한 현재의 위치정보, 신용카드의 이용정보 등) : 가장 민감한 정보로써 충분한 설명 후 사전 서면동의가 필요하며, 남용과 오용을 방지해야 함

이것은 가장 민감한 정보로서 이를 수집하는 경우에는 당해 위치정보 주체의 서면에 의한 사전동의가 있어야 할 것이다. 이때 위치정보 주체에게 수집하고자 하는 위치정보의 내용에 대하여 상세히 설명하고 수집의 목적이 충분히 알려져야 할 것이다. 이 경우 수집된 정보는 해당 서비스만을 위하여 이용되어야 할 것이다.

유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 2002. 7. 12. 지침(Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector)에 의하면 위치정보는 익명으로 처리되어야 하나, 단 가입자나 이용자가 부가서

119) 통신비밀보호법 제13조
120) 유럽의회와 회의의 통신분야에서의 개인정보처리와 프라이버시 보호에 관한 1997. 12. 15. 지침 (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector) Aricle 6.

비스를 신청한 경우 그 부가서비스를 제공하기 위하여 필요한 한도와 기간 동안만 처리될 수 있다고 한다. 서비스 제공자는 가입자에게 동의를 얻기 전에 위치정보의 유형과 목적과 정보처리 기간과 그 위치정보가 부가서비스를 위하여 제3자에게 제공되는지 여부를 알려야 한다고 규정하고 있다. 이 경우에도 가입자가 언제든지 간편하게 별도의 비용부담 없이 자신의 위치정보 처리의 중단을 요청할 수 있는 절차를 마련해 놓아야 한다고 한다[121].

Ⅵ. 노사관계에서의 감시에 대한 규제

1. 노동감시기술의 발달

오늘날 감시기술이 고도로 발달하면서 직장 내에서의 노동감시가 심각한 문제로 제기되고 있다. 미국 경영자협회(America Management Association)의 조사결과에 의하면 2001. 현재 전화통화 기록 및 검열을 하는 기업이 전체 기업의 11.9%, 컴퓨터 파일의 저장 및 검사를 하는 기업이 36.1%, 인터넷 접속 모니터링을 하는 기업이 62.0%, 컴퓨터 사용을 감시하는 기업이 18.9%에 달한다고 한다[122]. CCTV를 이용한 감시, 컴퓨터프로그램을 이용한 컴퓨터 이용상황에 대한 감시, 전자우편의 이용현황, 웹사이트 이용현황에 대한 감시, 위치추적장치를 실시간 위치확인 감시, 생체인식 프로그램을 이용한 감시 등이 오늘날 이용되고 있는 감시기술들이다. 여기에 덧붙여 최근에는 노동성과를 측정하는 기술이 발달하여 개별화된 노동자의 작업현황을 실시간으로 모니터링을 하고, 이를 분석, 평가하는 전사적자원관리시스템(ERP)을

121) Aritcle 9.
122)

도입하여 통합관리하는 추세이다.

2. 최근의 노동감시의 특징

가. 은밀한 감시

과거에는 감시기술이 발달하지 못하여 감시당하는 자 몰래 감시를 하기는 어려웠다. 따라서 감시는 감시를 당하는 노동자의 격렬한 저항에 부딪히곤 했다. 그러나 최근에는 감시기술이 발달하여 얼마든지 은밀하게 감시하는 것이 가능해졌다. 예를 들어 전자우편[123]이나 메신저, 인터넷 이용현황에 대한 감시, 그 밖의 컴퓨터 이용현황 감시 등의 전자감시는 감시당하는 노동자가 알지 못하는 사이에 이루어질 수 있으며, 증거를 남기지 않고 감시할 수 있다.

또 다른 은밀한 감시의 방법은 노동자들에게 미리 알리지 않은 용도로 감시를 하는 방법이다. 예를 들어 새로 신분증을 도입하면서 노동자들에게는 외부인의 무단침입을 방지하기 위한 보안조치 때문이라고만 알리고, 실제로는 출퇴근 시간, 이동 현황 등을 감시한다거나[124], 정기적인 건강검진을 한다고 하면서 여성 노동자의 임신여부를 검사한다거나, 사무환경을 전산화하는 것이라고 하면서 네트워크 시스템을 도입하면서, 네트워크 시스템으로 컴퓨터 이용현황, 출퇴근 시간, 작업시간 등을 감시하는 것들이다.

가장 은밀한 감시는 감시당하는 사람이 자신이 감시당하고 있다는 느낌마

---

123) 이메일 감시 솔루션을 설치한 대표적 기업과 기관(출처; 한겨레21 제402호 2002. 3. 27.)
대기업 : 삼성 LG 롯데 현대 하이닉스 현대건설 기아자동차 제일제당
공공기관 : 한국전력공사 대검찰청 대한무역투자진흥공사 한국전자통신연구원 금융감독원 외교통상부 병무청
금융기관 : 한미은행 신한은행 하나은행 농협 삼성투자신탁증권 한빛은행 수협중앙회 서울은행 LG카드 주택은행
정보통신 : 두루넷 데이콤 SK LG텔레콤
기타 : 한국과학기술연구원 효성 두산중공업 대우 금호건설

124) 실제로 지금 회사에서 지급하는 신분증이나 지문, 홍채인식과 같은 생체인식 서비스들 제품들은

저도 들지 않게 하면서 이루어지는 감시이다. 예를 들어 모든 것이 전산화되고 자동정보처리되면서 생산의 전과정이 세밀하게 정보로 처리될 경우, 사용자는 사용자가 배치한 감독자나 CCTV를 현장에서 철수시키거나 철거할 수 있다. 그러나 그렇다고 해서 감시가 완화된 것이 아니다. 오히려 좀 더 철저해진 것이다. 은밀한 감시는 보다 많은 감시를 하면서 보다 세련된 방법으로 이를 수행함으로써 노동자에게 감시의 느낌조차 갖지 못하도록 한다.

은밀한 감시로 감시받는 노동자의 심리적인 저항감을 완화시키면서 감시를 강화할 수 있는 것이다. 이와 같이 은밀하게 이루어지는 감시는 노동자의 통제범위 밖에 놓여질 경우가 많다.

나. 모든 노동자에 대한 24시간 전면감시

최근의 감시기술의 특징은 저렴한 비용으로 모든 노동자에 대하여 24시간 동안 전면적으로 감시를 하고, 개개인을 분석, 평가할 수 있다는 점에 있다. 개별감시가 가능해진 것이다. 과거에는 감시라는 것은 주로 사용자들이 집단에 대해 가하는 통제수단의 의미를 띠거나 개별적인 노동자를 대상으로 이루어진다 하더라도 특이사항에 대한 감시의 수준을 벗어나기 어려웠는데, 최근에는 감시는 개별 노동자에 대한 평가 및 통제시스템으로 성격이 바뀌어 가고 있는 것이다. 따라서 과거에는 노동자들의 집단의 저항이 있었으나, 최근에는 감시가 개별화되어 저항도 분산되게 된다.

다. 초정밀 감시

과거에는 감시를 해도 얻을 수 있는 정보는 한정되어 있었다. 그러나 최근에는 감시기술의 발달로 감시를 통해 얻을 수 있는 정보는 기하급수적으로 늘어나고 있다. 이는 단순히 양적인 증가의 문제가 아니라 감시의 성격을 바꾸는 질적인 전화의 문제이다. 최근의 노동감시의 문제는 단순히 프라이버시의 문제나 다소 폭력적인 양상을 띠는 노동통제의 문제가 아니라 인격권의 침해나, 사상, 양심, 표현의 자유의 침해는 물론 노동과정에 대한 전면적인 통제권에 관한 문제로 되고 있는 것이다.

라. 통합화

과거와 달리 오늘날의 감시기술의 발달과 정보처리기술의 발달로 감시로 획득한 정보의 통합은 가속화된다. 이는 일찍이 개인정보의 보호 원칙으로 인정되어온 개인정보 통합의 금지원칙에도 반하는 것이다. 특히 노동감시의 경우 통합이 쉬운 이유는 모든 노동자에 대한 기본정보가 있기 때문에 쉽게 통합될 수 있으며(식별정보의 존재), 기업의 환경이 정보통신망이나 전산망과 같은 네트워크로 연결되어 있으며, 기업의 업무나 체계가 통합을 지향하고 있기 때문이다. 이러한 감시정보의 통합은 감시정보로부터 얻어 낼 수 있는 정보의 양을 획기적으로 늘려주게 되는데, 이로 인해 노동자는 예측하지 못했던 권리의 침해를 받게 될 우려가 있다.

마. 평가정보화하면서 노동통제수단으로 기능

최근의 감시의 추세는 감시를 점차로 평가수단화 하고 있다는 데 있다. 이는 감시기술의 발달로 인해 가능한 것이기도 하지만, 감시정보를 가장 효율적인 노동통제의 수단으로 이용하는 방법이기도 하다. 이는 감시를 직무평가의 개념에 접근시켜 감시를 정당화하는 논거로 사용되기도 한다.

3. 노동감시의 특수성

가. 침해되는 권리의 다양성

노동감시는 시민사회에서의 일반적인 감시와 마찬가지로 프라이버시의 침해, 인간의 존엄, 평등권, 양심의 자유, 언론의 자유, 표현의 자유, 행동의 자유 및 정치활동의 자유의 침해 문제를 야기한다. 그러나 무엇보다도 노동감시는 노동통제의 일환으로 이루어지게 되므로 기본적으로 근로조건에 대한 침해, 노동3권의 침해와 관련된 문제라는 특징이 있다.

나. 사용자의 권리와의 충돌

한편 노동감시는 노동감시를 합리화하는 사용자의 권리와 노동자의 의무

와 충돌하는 영역이다. 특히 최근 노동감시의 추세가 개인별 평가정보화하는 데 있는바, 어느 범위에서 어떤 방법으로 노동자의 직무수행을 감독하고, 통제할 수 있는 것인지 그 범위를 정하는 것이 매우 중요하다. 사용자는 최대한의 감독권을 주장할 것이고, 노동자는 최소한의 감독권을 선호할 것이다. 노동감시는 노동자의 헌법적 권리와 관계된 문제이고 근로조건을 결정하는 문제이므로 결국 그 적절한 범위는 헌법적 가치와 노동기본권의 관점에서 정해져야 할 것이다.

다. 가장 깊숙한 통제 - 통제의 동기와 방법

노사관계에서는 감시는 노동통제의 가장 효율적인 수단으로 이용된다. 사용자에게 이런 강력한 노동감시의 동기가 있다. 거기에 노사관계는 대등하지 않은 관계이므로 사회법적인 규제의 필요성이 더욱 더 절실하다. 게다가 최근의 감시기술의 발달은 적절한 규제를 하지 않으면 안되는 상황에 이르게 하고 있다.

라. 동의의 문제

일반적인 법원리상 감시는 감시받는 사람의 동의가 있으면 위법성이 없어지는 경우가 많다. 그러나 노사관계에 있어서는 동의의 문제는 노사관계가 기본적으로 비대등관계라는 관점에서 그 의미를 파악해야 한다. 감시에 대한 문제를 집단적인 권리로 볼 필요가 있는 것이다.

4. 노동감시에 대한 입법의 필요성과 기본원칙

가. 노동감시에 대한 현행 입법

우리나라의 현행 법률상 노동감시에 대한 규율은 미비하기 짝이 없다. 대략적으로 아래의 것들이 노동감시에 적용될 수 있는 법률들이다.

(1) 헌법

헌법은 사생활의 보호와 불가침(제17조)[125], 통신의 비밀과 자유(제18조)[126], 양심의 자유(제19조)[127], 언론출판의 자유(제21조)[128], 인간의 존엄과 가치 및 행복추구권(제10조)[129]을 규정하고 있는데, 이것은 노사간의 관계에서 또는 직장 내에서도 적용되어야 한다. 따라서 헌법상의 이러한 권리는 노동감시의 한계를 판단하는 기준이 되어야 한다. 그리고 헌법은 단결권, 단체교섭권, 단체행동권 등의 노동3권을 보장하고 있는바(제33조)[130], 노동감시의 적법여부를 따질 때에는 그것이 헌법이 보장하고 있는 노동3권을 침해하는지 여부를 검토해야 한다. 이러한 규정들이 노동감시에 적용될 수 있는 조항들이다.

예컨대 직장 내에서 사적인 활동을 감시하거나, 사적인 통신을 검열하거나 도청하는 경우 이는 헌법상 보장된 사생활의 보호와 불가침의 권리 및 통신의 비밀의 권리를 침해하는 것이고, 직장 내에서 사용자가 근로자의 작업현황을 몰래 카메라로 촬영을 하는 경우에는 인격권의 침해로 볼 수 있을 것이다. 노동조합의 활동에 대하여 도청을 하거나 이를 몰래 촬영하거나 추적을 하는 경우에는 노동3권에 대한 침해로 볼 수 있을 것이다. 이와 같이 헌법상의 기본권이 침해되는 경우에는 법원에 손해배상을 청구하거나, 침해행

---

125) 헌법 제17조 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.

126) 헌법 제18조 모든 국민은 통신의 비밀을 침해받지 아니한다.

127) 헌법 제19조 모든 국민은 양심의 자유를 가진다.

128) 헌법 제21조 ①모든 국민은 언론·출판의 자유와 집회·결사의 자유를 가진다.
②언론·출판에 대한 허가나 검열과 집회·결사에 대한 허가는 인정되지 아니한다.
③통신·방송의 시설기준과 신문의 기능을 보장하기 위하여 필요한 사항은 법률로 정한다.
④언론·출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니된다. 언론·출판이 타인의 명예나 권리를 침해한 때에는 피해자는 이에 대한 피해의 배상을 청구할 수 있다.

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

130) 헌법 제33조 ①근로자는 근로조건의 향상을 위하여 자주적인 단결권·단체교섭권 및 단체행동권을 가진다.
②공무원인 근로자는 법률이 정하는 자에 한하여 단결권·단체교섭권 및 단체행동권을 가진다.
③법률이 정하는 주요방위산업체에 종사하는 근로자의 단체행동권은 법률이 정하는 바에 의하여 이를 제한하거나 인정하지 아니할 수 있다.

위의 중지를 청구할 수 있을 것이다.

(2) 근로기준법

근로기준법에 의하면 근로조건의 결정은 근로자와 사용자가 동등한 지위에서 자유의사에 의하여 결정하여야 한다[131]. 우리 대법원은 근로조건이란 사용자와 근로자 사이의 근로관계에서 임금 근로시간 후생 해고 기타 근로자의 대우에 관하여 정한 조건을 말한다(대법원 1992. 6. 23. 선고, 91다19210판결)고 보고 있는바, 직장에서 근로조건의 변화를 야기할 수 있는 감시시스템을 도입하고자 하는 경우에는 그 도입여부는 근로기준법에 따라 노사간의 대등한 지위에서 자유롭게 결정되어야 하고, 일방적으로 근로자에게 불이익하게 근로조건을 변경하는 것은 허용되지 않는다(대법원 1977. 7. 26. 선고, 77다355판결).

(3) 노동조합 및 노동쟁의조정법

(가) 부당노동행위

노동조합 및 노동쟁의조정법은 부당노동행위를 금지하고 있다.[132] 따라서 노동감시가 노동조합의 가입이나 조직, 노동조합 활동을 이유로 이루어지는

131) 근로기준법 제3조 (근로조건의 결정) 근로조건은 근로자와 사용자가 동등한 지위에서 자유의사에 의하여 결정하여야 한다.

132) 노동조합 및 노동쟁의조정법 제81조 (부당노동행위) 사용자는 다음 각호의 1에 해당하는 행위(이하 "부당노동행위"라 한다)를 할 수 없다.
1. 근로자가 노동조합에 가입 또는 가입하려고 하였거나 노동조합을 조직하려고 하였거나 기타 노동조합의 업무를 위한 정당한 행위를 한 것을 이유로 그 근로자를 해고하거나 그 근로자에게 불이익을 주는 행위
2-3 (생략)
4. 근로자가 노동조합을 조직 또는 운영하는 것을 지배하거나 이에 개입하는 행위와 노동조합의 전임자에게 급여를 지원하거나 노동조합의 운영비를 원조하는 행위. 다만, 근로자가 근로시간중에 사용자와 협의 또는 교섭하는 것을 사용자가 허용함은 무방하며, 또한 근로자의 후생자금 또는 경제상의 불행 기타 재액의 방지와 구제등을 위한 기금의 기부와 최소한의 규모의 노동조합사무소의 제공은 예외로 한다.
5. 근로자가 정당한 단체행위에 참가한 것을 이유로 하거나 또는 노동위원회에 대하여 사용자가 이 조의 규정에 위반한 것을 신고하거나 그에 관한 증언을 하거나 기타 행정관청에 증거를 제출한 것을 이유로 그 근로자를 해고하거나 그 근로자에게 불리익을 주는 행위

경우, 노동조합 활동을 방해·지배·개입하기 위한 것일 경우, 단체행동에 참여한 것을 이유로 한 경우에는 부당노동행위로 보아야 할 것이다. 예컨대 노동조합의 활동을 감시하기 위한 CCTV의 설치, 컴퓨터 사용에 대한 감시, 전화나 이메일 등의 사용에 대한 감시, 노동조합의 활동을 방해하는 컴퓨터 사용 감시, CCTV 설치, 전화나 이메일 감시, 노동조합이나 상급단체 기타 노동조합 활동을 위하여 필요한 홈페이지의 접속차단 등은 부당노동행위인 것이다. 서울지방노동위원회는 회사가 회사 내의 컴퓨터에서 노동조합과 상급단체로의 홈페이지의 접속을 차단한 것은 부당노동행위에 해당한다고 판정하였다[133].

(나) 단체교섭의무 대상여부

헌법과 노동조합 및 노동관계조정법은 노동조합에게 '근로조건의 결정에 관한 사항'과 '근로조건의 결정에 영향을 미치는 기타 노동관계에 관한 사항'에 관하여 사용자와의 단체교섭권을 부여하고 있다(헌법 제33조 제1항, 노동조합 및 노동관계조정법 제29조 제1항, 제2조 제4호 본문, 제47조, 제48조).[134] 그에 따라 사용자는 '근로조건의 결정에 관한 사항'과 '근로조건의 결정에 영향을 미치는 기타 노동관계에 관한 사항'[135]에 관한 노동조합의 단체교섭요구에 응해야 하며, 사용자가 정당한 사유없이 이를 거부할 때는 부당노동행위가 되며, 이에 대한 단체교섭이 결렬될 경우에는 노동조합은 쟁의행위가 가능하며, 단체교섭이 타결될 경우 노사 양 측은 반드시 단체협약을 체결하여야 한다. 이러한 '근로조건의 결정에 관한 사항'의 예로는 임금, 시업과 종업의 시간, 휴식시간, 승급, 퇴직에 관한 사항, 후생복지시설에 관한 사항, 교육시설에 관한 사항, 안전과 보건에 관한 사항 등을 들 수 있다.[136]

그런데 한편 대법원은 근로조건에 관한 사항이지만 동시에 사용자의 경영

133) 서울지방노동위원회 2002. 11. 19. 최근 컴퓨터 사용이 일반화됨에 따라 일상업무는 물론 노동조합 활동까지도 컴퓨터 사용이 필수불가결하기 때문에 사용주가 노조 홈페이지 접속을 차단하는 것은 사용자의 시설관리권의 범위를 넘는 권한행사로 부당노동행위에 해당한다.
134) 사법연수원, 노동조합 및 노동관계조정법, 2002, 178-179 페이지
135) 사법연수원, 노동조합 및 노동관계조정법, 2002, 180 페이지
136) 사법연수원, 노동조합 및 노동관계조정법, 2002, 181 페이지

상의 권한에 속하는 사항의 성격을 갖고 있는 경우에는 그것이 근로조건에 직접적으로 관련되거나 중대한 영향을 미칠 정도로 밀접하게 관련되어 있는 경우에는 사용자의 경영권을 근본적으로 제한하지 않는 범위 안에서 단체교섭의 대상이 된다고 보고 있다[137]. 이런 관점에서 운수업체에서의 조합원의 차량별 고정승무 발령, 배차시간, 대기기사 배차순서 등에 관한 사항을 단체협약의 대상이 될 수 있다고 판시한 바 있다(대법원 1994. 8. 26. 선고 93누8993판결).

따라서 사용자가 예를 들어 작업현장에 CCTV를 설치하는 것과 같이 새로운 노동감시 도구를 도입하고자 하는 경우 다소 논란의 여지가 있지만, 그것은 근로조건에 중대하게 영향을 미칠 것이므로 대법원의 현행법 해석상으로도 의무교섭사항으로 볼 수 있을 것이므로 노동조합의 교섭요구가 있을 경우 사용자는 교섭에 응해야 할 것이다. 그러나 대법원의 현행법의 해석태도에 비추어 볼 때, 전자우편의 감시시스템의 도입, 컴퓨터 사용의 감시시스템의 도입의 경우, 전사적자원관리시스템(ERP)의 도입의 경우에 이를 의무교섭사항으로 볼지는 의문의 여지가 있다.

(4) 통신비밀보호법

통신비밀보호법은 당사자의 동의가 없는 우편물과 전기통신[138], 대화의 검열이나 감청, 비밀침해를 금지하고 있다. 이 법은 당연히 노사관계 하에서도 적용된다[139]. 따라서 당사자의 동의를 받지 않고 우편이나 통신을 검열할 경

137) 반면 학설 중에서는 인사경영에 관한 사항이라 하더라도 근로조건과 관련된 것은 의무적인 교섭대상으로 보아야 한다는 견해도 있다. 사법연수원, 앞의 책, 180.

138) 통신비밀보호법 제2조
2. "우편물"이라 함은 우편법에 의한 통상우편물과 소포우편물을 말한다
3. "전기통신"이라 함은 전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말한다

139) 통신비밀보호법 제3조 (통신 및 대화비밀의 보호) ①누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다.
다만, 이 법은 5가지의 예외사유를 들고 있으나, 그 예외사유에는 직장에서 업무수행에 관한 통신이나 대화를 이 법의 비밀보호의 대상에서 제외한다는 내용은 없다.

우에는 설사 그 우편이나 통신이 직장 내에서 근무시간 중에 사용자가 제공한 컴퓨터나 전화기 등을 이용해 이루어진다 하더라도 위법한 행위가 된다. 우리 법원은 이런 취지에서 사용자가 근로자의 컴퓨터에 보관된 전자우편을 당사자의 동의를 받지 않고 접근하여 열람한 사건에서 사용자에게 통신비밀보호법 위반죄를 인정한 사례가 있다.

(5) 정보통신망이용촉진 및 정보보호에 관한 법률

정보통신망이용촉진 및 정보보호에 관한 법률은 OECD의 8원칙이나 EU의 개인정보 보호에 관한 여러 지침에서 제시된 원칙을 구체화하여 전자적으로 처리되는 개인정보 수집 · 보관 · 이용과 관련하여 개인정보 수집자와 개인정보 제공자의 권리와 의무를 규정하고 있다. 즉, 이 법은 개인정보 수집자는 개인정보 수집시 당사자의 동의를 얻어야 하고, 개인정보 수집시 목적을 특정하여 미리 고지하여야 하고[140], 민감한 정보는 수집해서는 안되고[141], 그 목적 외로 사용해서는 안되고, 당사자의 동의없이 개인정보를 제3자에게 제공해서는 안되고[142], 개인정보 주체는 자신의 개인정보에 대한 열람, 수정요

---

140) 제22조 (개인정보의 수집) ①정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 당해 이용자의 동의를 얻어야 한다. 다만, 다음 각호의 1에 해당하는 경우에는 그러하지 아니하다.
1. 정보통신서비스 이용계약의 이행을 위하여 필요한 경우
2. 정보통신서비스 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우
②정보통신서비스제공자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 각호의 사항을 이용자에게 고지하거나 정보통신서비스이용약관에 명시하여야 한다.
1. 개인정보관리책임자의 성명 · 소속부서 · 직위 및 전화번호 기타 연락처
2. 개인정보의 수집목적 및 이용목적
3. 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용
4. 제30조제1항 · 제2항 및 제31조제2항의 규정에 의한 이용자 및 법정대리인의 권리 및 그 행사방법
5. 그 밖에 개인정보 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항

141) 제23조 (개인정보의 수집의 제한 등) ①정보통신서비스제공자는 사상 · 신념 · 과거의 병력 등 개인의 권리 · 이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 이용자의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.
②정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보외의 개인정보를 제공하지 아니한다는 이유로 당해 서비스의 제공을 거부하여서는 아니된다.

142) 제24조 (개인정보의 이용 및 제공 등) ①정보통신서비스제공자는 당해 이용자의 동의가 있거나 다음 각호의 1에 해당하는 경우를 제외하고는 개인정보를 제22조제2항의 규정

구를 할 권리가 있고, 언제든지 자신이 한 개인정보 제공 동의를 철회할 권리가 있다고 규정하고 있다[143].

그러나 이 법은 정보통신서비스제공자[144]와 정보통신서비스이용자[145] 사이에서만 적용될 뿐, 노사관계에서는 적용되지 않는다[146]. 따라서 노동자는 자

에 의한 고지의 범위 또는 정보통신서비스이용약관에 명시한 범위를 넘어 이용하거나 제3자에게 제공하여서는 아니된다.
1. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
2. 통계작성·학술연구 또는 시장조사를 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우
3. 다른 법률에 특별한 규정이 있는 경우
②정보통신서비스제공자로부터 이용자의 개인정보를 제공받은 자는 당해 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제공받은 목적외의 용도로 이를 이용하거나 제3자에게 제공하여서는 아니된다.
③정보통신서비스제공자등(정보통신서비스제공자와 그로부터 이용자의 개인정보를 제공받은 자를 말한다. 이하 같다)은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.
④이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니된다.

143) 제30조 (이용자의 권리 등) ①이용자는 정보통신서비스제공자등에 대하여 언제든지 제22조제1항 본문, 제23조제1항 단서 및 제24조제1항 본문의 규정에 의한 동의를 철회할 수 있다.
②이용자는 정보통신서비스제공자등에 대하여 자신의 개인정보에 대한 열람을 요구할 수 있으며, 자신의 개인정보에 오류가 있는 경우에는 그 정정을 요구할 수 있다.
③정보통신서비스제공자등은 이용자가 제1항의 규정에 의하여 동의를 철회한 경우에는 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하여야 한다.
④정보통신서비스제공자등은 제2항의 규정에 의하여 열람 또는 정정요구를 받은 경우에는 지체없이 필요한 조치를 취하여야 한다.
⑤정보통신서비스제공자등은 제2항의 규정에 의하여 오류의 정정요구를 받은 경우에는 그 오류를 정정할 때까지 당해 개인정보를 제공 또는 이용하여서는 아니된다.
⑥정보통신서비스제공자등은 이용자로부터 제1항 및 제2항의 규정에 의한 동의의 철회, 개인정보의 열람 또는 정정의 요구를 받은 경우에는 제22조 및 제23조의 규정에 의하여 개인정보를 수집하는 방법보다 쉽게 할 수 있도록 필요한 조치를 취하여야 한다.
⑦제1항 내지 제6항의 규정은 영업양수자등에 이를 준용한다. 이 경우 "정보통신서비스제공자등"은 "영업양수자등"으로 본다.

144)정보통신망 이용촉진 및 정보보호에 관한 법률 제2조 제1항
3. "정보통신서비스제공자"라 함은 전기통신사업법 제2조제1항제1호의 규정에 의한 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

145) 정보통신망 이용촉진 및 정보보호에 관한 법률 제2조 제1항
4. "이용자"라 함은 정보통신서비스제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.

146) 정보통신망 이용촉진 및 정보보호에 관한 법률 제58조에서는 정보통신서비스제공자 이외의 자에 대하여 이 법의 준용규정을 두고 있는데, 여기에도 근로자와 사용자는 포함되지 않는다.
제58조 (정보통신서비스제공자외의 자에 대한 준용) 제22조 내지 제32조의 규정은 정보

신의 개인정보에 관하여 사용자에 대하여 정보통신서비스 이용자에게 부여되는 권리를 주장할 수 없게 되어 있다. 따라서 사업자가 목적을 고지하지 않고 노동자의 개인정보를 수집하거나, 이를 제3자에게 제공하는 경우에도 사업자에 대하여는 정보통신서비스제공자에게는 가해지는 형사처벌[147]이 가해지지 않는다. 그러나 오히려 노동자와 사용자 사이에서는 노동자의 개인정보 보호의 필요성이 더욱 크고, 사용자가 노동자의 개인정보를 수집하여 이용함에 있어서 이를 악용하거나 남용할 위험성도 크다. 그럼에도 불구하고 그에 대한 법적 규율이 없다는 것은 중대한 입법의 흠결이 아닐 수 없다. 실제로 아래에서 보다시피 외국의 경우에는 많은 국가에서 노동자의 개인정보 보호에 관한 법률을 가지고 있다.

나. 노동감시에 대해 규율하는 입법의 필요성

헌법상의 기본권을 침해하는 노동감시 행위가 있을 경우에는 헌법상의 기본권 침해를 이유로 그 중단을 구하거나, 그 행위에 대한 손해배상을 청구할 수 있을 것이다. 그리고 근로조건의 변경을 가져오는 노동감시행위에 대해서는 노동조합이 단체교섭을 요구하고, 단체협약을 통하여 도입여부를 정할 수 있을 것이다[148]. 그러나 이러한 헌법의 규정과 노동관계법의 규정만으로는

통신서비스제공자외의 자로서 재화 또는 용역을 제공하는 자중 대통령령이 정하는 자가 자신이 제공하는 재화 또는 용역을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에 이를 준용한다. 이 경우 "정보통신서비스제공자" 또는 "정보통신서비스제공자등"은 "재화 또는 용역을 제공하는 자"로, "이용자"는 "재화 또는 용역을 제공받는 자"로 본다.

147) 제62조 (벌칙) 다음 각호의 1에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.<개정 2002.12.18>
1. 제24조제1항(제58조의 규정에 의하여 준용되는 경우에 해당되는 자를 포함한다)의 규정을 위반하여 개인정보를 제22조제2항의 규정에 의한 고지의 범위 또는 서비스 이용약관에 명시한 범위를 넘어 이용하거나 제3자에게 제공한 자 및 그 정을 알고 영리 또는 부정한 목적으로 개인정보를 제공받은 자
2. 제24조제2항(제58조의 규정에 의하여 준용되는 경우에 해당되는 자를 포함한다)의 규정을 위반하여 이용자의 개인정보를 제공받은 목적외의 용도로 이용하거나 제3자에게 제공한 자 및 그 정을 알고 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제24조제4항(제58조의 규정에 의하여 준용되는 경우에 해당되는 자를 포함한다)의 규정을 위반하여 이용자의 개인정보를 훼손·침해 또는 누설한 자
4. 제48조제2항의 규정을 위반하여 악성프로그램을 전달 또는 유포한 자
5. 제48조제3항의 규정을 위반하여 정보통신망에 장애를 발생하게 한 자
6. 제49조의 규정을 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자

다양한 노동감시 행위와 노동자의 개인정보에 대한 침해를 효과적인 보호받기가 어렵다. 특히 현행 법률규정상으로는 사용자가 수집하는 노동자의 개인정보에 대해서는 노동자에게 아무런 권리도 보장되지 않는다.

노동감시는 노사간의 근로조건의 핵심적인 부분에 해당하며, 헌법상의 기본권 보장에 관한 문제이다. 그리고 노사관계에 있어서는 그 어느 부문에서보다 노동자의 개인정보의 보호필요성이 크다. 게다가 최근 무제한적으로 발전하고 있는 노동감시기술의 실태에 비추어 볼 때 이에 대한 법적 규제는 그 어느 때보다 절실하다. 시급히 법제화를 통해 사회적 기본선을 마련할 필요가 있다. 이때 사회적 기본선의 확정은 해당하는 노동감시나 노동자의 개인정보 침해가 근로조건에 어떤 영향을 미치는지를 면밀히 검토하여 이루어져야 한다. 이런 점을 고려할 때 노동감시에 대한 규제와 노동자의 개인정보의 보호를 위한 입법의 기본원칙으로는 다음과 같은 것을 들 수 있을 것이다.

(1) 노동감시에 대한 규율과 노동자의 개인정보의 보호는 헌법상의 기본권 보장의 측면에서 기준을 마련해야 한다

헌법상의 기본권은 당연히 노사관계에서도 적용되어야 한다. 따라서 노동감시의 문제는 사용자의 시설물 관리권이나 재산권 보호의 측면에서만 바라보아서는 안되고, 헌법상의 기본권 보장이라는 측면에서 판단되어야 한다. 따라서 노사관계에서도 직장에서도 노동자에게는 개인의 존엄을 유지할 수 있는 기본적인 인격권이 보장되어야 하며, 프라이버시권이나 개인정보의 자기결정권이 인간존엄의 근본수단임을 천명한 헌법의 원칙에 따라 기본권이 보장되어야 한다. 그리고 노동감시는 행동의 자유, 사상의 자유, 양심의 자유, 표현의 자유를 침해해서는 안된다는 헌법의 기본원리에 입각해야 한다.

(2) 노동감시 체계의 도입은 노동자의 집단적 권리 보호의 문제로 노동자의 개인정보의 보호에 관한 문제는 사회법적 규율의 대상으로 바라보

148) 물론 이는 앞에서 보았듯이 학설의 대립이 있고, 우리 대법원의 경우는 상당히 제한적인 범위 내에서만 단체교섭권을 인정하고 있다.

아야 한다

노동감시의 문제는 결국 노동통제의 문제로서 근로조건의 결정에 관한 문제이므로 원칙적으로 노동자의 동의가 필요하다. 이때 노동자의 동의는 근로조건에 대하여 단체교섭권을 보장하고 있는 취지에 비추어 노동자의 집단적 권리로 이해해야 한다.

노동자의 개인정보의 보호의 문제도 노동자의 동의가 필요한데, 이때에도 일반적으로 사적관계에서 인정되는 당사자들의 고지와 동의 - OECD 8원칙으로 대표되는 - 사적 자치의 보장의 구조가 아니라, 대등하지 않은 노사관계의 특성에 입각하여 사회법적 관점에서 노동자에게 개인정보 주체로서의 권리보호장치를 특별히 마련해야 한다.

5. 노동감시와 노동자의 개인정보에 대한 해외의 입법현황

가. 해외의 입법현황

(1) OECD

'프라이버시 보호와 개인데이터의 국제유통에 대한 가이드라인에 관한 이사회 권고안, 1980[149]'은 개인정보의 보호에 대한 기본원칙을 정하고 있는데,

149) ① 수집제한의 원칙 : 모든 개인정보는 적법하고, 공정한 수단에 의해 수집되어야 하며, 정보주체에게 알리거나 동의를 얻은 후 수집되어야 한다.
② 정보내용정확성의 원칙 : 개인정보는 그 이용목적에 부합하는 것이어야 하고, 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태로 유지하여야 한다.
③ 목적 명확화의 원칙 : 개인정보를 수집할때는 목적이 명확해야 하고, 이를 이용할 경우에도 애초의 목적과 모순되지 않아야 한다.
④ 이용제한의 원칙 : 개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화된 목적 이외의 용도로 공개되거나 이용되어서는 안된다.
⑤ 안정성 확보의 원칙 : 개인정보의 분실, 불법적인 접근, 파괴, 사용, 수정, 공개위험에 대비하여 합리적인 안전보호장치를 마련해야 한다.
⑥ 공개의 원칙 : 개인정보에 관한 개발, 운용 및 정책에 관해서는 일반적인 공개정책을 취하여야 한다. 개인정보의 존재, 성질 및 주요이용목적과 함께 정보관리자의 신원, 주소를 쉽게 알 수 있는 방법이 마련되어야 한다.
⑦ 개인참가의 원칙 : 정보주체인 개인은 자신과 관련된 정보의 존재확인, 열람요구, 이의제기 및 정정·삭제·보완 청구권을 가진다.
⑧ 책임의 원칙 : 개인정보 관리자는 위에서 제시한 원칙들이 지켜지도록 필요한 제반조치를 위해야 한다.

이권고안은 노사관계에서도 적용되는 것을 전제로 하고 있다. 그런데 이 원칙은 기본적으로 양 당사자가 대등하다는 원칙에서 출발하고 있으므로 노사관계의 특수성이 충분히 반영되어 있다고는 볼 수 없을 것이다.

(2) ILO : 노동자의 개인정보 보호를 위한 권리보호 규약(Code of Practice on protection of workers' personal data 1996)

국제노동기구에서 마련한 이 규약은 강제성은 없고 권고적 효력만을 갖는다. 이 규약은 개인정보의 취득과 관련하여 노사관계에 특수하게 나타나는 여러 가지 문제 및 새롭게 대두하고 있는 감시기술에 대하여 초보적으로 다루고 있지만, 노동통제의 수단으로 최근에 대두하고 있는 노동감시의 문제로 예컨대 전자우편, 인터넷, 컴퓨터 이용현황에 대한 감시, 생체정보를 이용한 감시, 스마트 카드, 위치정보를 이용한 감시의 문제 등에 대하여는 충분히 다루고 있지 못하다.

이 규약은 노동자의 개인정보 수집과 관련하여 ① 노동자는 노동자의 개인정보 수집시 통지를 받아야 하고, ② 노동자의 개인정보는 적법하고 공정하게 수집되어야 하고, ③ 노동자의 개인정보는 고용계약에 최소한의 필요한 범위내에서 수집되어야 하고, ④ 고용주는 노동자에 관한 정보를 반드시 작업과 관련된 범주에서 본인으로부터 직접 취득해야 하고, ⑤ 노동자의 개인정보는 수집된 본래의 목적에 직접적으로 관련있는 범위 내에서만 이용되어야 하고, ⑥ 노동자의 개인정보는 안전하게 보관되어야 하고, ⑦ 노동자는 개인정보에 접근할 수 있어야 하고, ⑧ 노동자의 개인정보는 당사자의 동의없이 제3자에게 제공되어서는 안되며, ⑨ 고용주는 노동자의 성생활이나 정치, 종교적 신념에 관한 정보를 취득하려 해서는 안된다는 점을 규정하고 있다.

그리고 수집된 정보의 처리 및 평가와 관련하여 ① 어떤 노동자에 대한 결정이 그 노동자에 대한 자동 처리된 개인정보에만 의존해서 이루어지면 안되고, ② 전자 감시로 수집된 개인정보가 직무 수행 평가의 유일한 요소가 되어서는 안된다는 점을 규정하고 있다.

한편 이 규약은 노동자는 프라이버시 권리를 포기할 수 없다고 명시하여 노사관계의 특수성을 반영하고 있으며, 새로운 노동감시 방법으로서 약물검사나 거짓말탐지기 등에 대하여 노동자에 대한 마약 복용 여부 검사는 반드시 법률 규정에 따라야 하며 자의적 검사는 허용되지 않는다는 점과 노동자의 의료상 비밀 사항에 해당되는 개인 정보는 비밀로 유지되어야 하며, 다른 인사 정보와 분리돼 안전하게 보관돼야 하며, 거짓말 탐지기와 같은 기술은 사용되어서는 안된다고 규정하고 있다.

한편 ILO 협약 135와 권고 143는 노동조합이 조직이나 단체교섭을 위하여 회사의 시설 등을 이용할 권리를 규정하고 있다. 노동조합은 ILO 협약 135에 따라 조직이나 단체교섭을 위하여 회사의 인터넷 상의 전자게시판 등을 이용할 권리가 보장되어야 할 것이다.

(3) EU 및 유럽 각국

EU와 유럽각국은 노동감시에 관하여 많은 국제적 효력을 갖는 규약, 지침을 가지고 있으며, 각국별로도 많은 법제를 가지고 있다.

(가) EU 유럽의회의 “개인정보의 처리와 자유로운 유통에 관한 개인정보보호지침(Directive 95/46/EC)[150][151]”

유럽의회에서 채택한 개인정보보호지침은 가입국에 대하여 지침의 내용을 국내입법으로 제정할 의무를 부여하고 있다. 그런데 이 지침은 일반 소비자뿐만 아니라 노사관계에 대하여도 적용되게 되어 있다. 따라서 직장에서 사용자가 노동자의 개인정보를 처리하는 경우에도 이 지침을 준수해야 한다.

---

150) (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data)

151) Convention for the protection of individuals with regard to automatic processing of personal data (ETS No.108, the 28 January) 이는 개인정보의 보호에 관하여 국제적인 규범력을 갖는 최초의 협약이다. 이 협약에서는 개인정보 수집이 적법하고, 공정하게 이루어져야 하며, 목적을 특정하고, 목적범위 내에서 최소한으로 이루어져야 한다고 규정하고, 민감한 개인정보(정치적 견해, 신념, 종교, 건강, 인종, 성생활, 범죄 기록 등)에 대하여는 충분한 안전조치가 이루어지지 않은 상태에서는 수집할 수 없다고 규정하고 있다. 이 협약은 개인정보주체의 자신의 개인정보에 대한 열람 및 수정권을 인정하고 있다.

이 지침에 의하면 사용자는 노동자의 개인정보를 처리하는 것과 관련하여 다음의 원칙을 준수하여야 한다.

① 모든 개인정보는 특정한 목적으로, 명시적이고, 합법적인 목적으로 수집되어야 하며, 수집된 목적 외로는 사용되어서는 안된다.

② 노동자에게 사용자가 수집하고자 하는 정보가 무엇인지(직접적이든, 간접적이든), 정보처리의 목적은 무엇인지, 어떻게 처리되는지를 알려 주어야 한다. 노동자는 자신의 개인정보에 접근할 수 있어야 한다.

③ 노동자의 개인정보는 수집의 목적에 비추어 적절한 범위 내에서 수집되어야 하며, 과다하게 수집되어서는 안된다.

④ 노동자의 개인정보는 정확하여야 하며, 노동자는 개인정보의 오류를 수정할 권리가 있다.

⑤ 노동자의 개인정보는 안전하게 보관되어야 한다.

⑥ 개인정보 처리를 담당하는 담당자는 개인정보의 보호에 대하여 잘 알고 적절하게 훈련을 받아야 한다.

⑦ 노동자의 개인정보를 제3자에게 제공하고자 하는 경우에는 노동자의 동의를 받아야 한다.

(나) '인권과 기본적 자유 보호를 위한 유럽협약'(the European Convention for the Protection of Human Rights and Fundamental Freedoms)

인권과 기본적 자유 보호를 위한 유럽협약 제8조는 "누구나 자신의 개인과 가족생활, 집, 통신을 존중받을 권리가 있고", "이러한 권리를 수행하는데 있어 공공기관의 방해가 있어서는 안된다. 다만, 공공의 안전과 경제적 부를 위해 필요한 경우, 그리고 범죄의 예방, 건강과 도덕의 보호, 타인의 자유와 권리의 보호를 위해 필요한 경우 예외가 있을 수 있다"고 규저암으로써 프라이버시의 보호원칙을 천명하고 있다.

그리고 제10조에서는 "누구나 표현의 자유를 누린다. 이 권리는 국경에 상관없이 공공기관의 방해를 받지 않고 생각과 이념을 자유롭게 교환할 수 있

음을 의미한다. 이 조항은 국가가 텔레비전이나 영화를 통해 방송할 수 있는 권리를 요구하는 것을 금지하지 않는다"고 하여 표현의 자유를 보장하고 있다.

그런데 유럽인권재판소는 제8조에 명시된 '사생활'의 보호는 노동자의 집 안 내에서의 생활로만 제한하지 않고 업무 활동도 포함하는 개념임을 명확히 했다. '니미츠(Niemietz) 對 독일' 사건[152]에서 유럽인권재판소는 다음과 같이 판시했다.

"사생활에 대한 존중은 다른 사람들과의 관계를 발전시킬 권리를 어느 정도 포함해야 한다. 나아가 대다수의 사람들은 직장생활을 하는 과정에서 바깥 세상과의 관계를 발전시켜 나갈 중요한 기회를 갖게 되므로 '사생활' 개념에서 업무활동을 배제하자는 주장은 근거가 없다. 이는 업무활동에서 개인적 활동을 명확하게 분리해내기가 어렵다는 점을 보아도 잘 알 수 있다."

'해포드(Halford) 對 영국' 사건[153]에서 유럽인권재판소는 업무중 노동자의 전화를 가로채는 행위는 인권과 기본적 자유 보호를 위한 유럽협약의 제8조을 위반한 것으로 판시했다. 해포드에게는 두 대의 전화가 있었는데, 그 중 하나는 개인용이었다. 그런데 그 전화의 사용에 대한 어떤 지침이나 제한도 없었다. 해포드는 자신의 전화사용을 가로챈 행위는 인권과 기본적 자유 보호를 위한 유럽협약의 제8조을 위반한 것이라고 주장했다. 이에 대해 영국 정부는 개인전화의 사용에 있어서 프라이버시 보호가 기대될 만한 근거가 없기 때문에 회사에서 그녀가 사용한 전화는 인권과 기본적 자유 보호를 위한 유럽협약의 제8조에 해당되지 않는다고 주장했다. 나아가 영국 정부의 변호인단은 고용주는 원칙적으로 노동자에게 사전고지 없이도 고용주가 제공한 전화의 통화내역을 감시할 수 있다고 주장했다.

그러나 유럽인권재판소는 "집에서 뿐 아니라 업무활동에서 사용한 통화내역도 8항이 의미하는 바의 '사생활'과 '통신'의 범위에 포함된다. 내선전화의

152) Niemietz v Germany [1992], 그 외에 Klass and Others v. Germany [1978], Huvig v. France [1990], the A v. France [1993] 등도 같은 취지임.
153) Halford v United Kingdom [1997]

사용자인 해포드에게 시스템이 가로채일 수 있다는 경고를 했다는 증거가 없다. 따라서, 본 재판소는 그녀가 전화통화시 프라이버시 보호에 대한 기대를 했을 것이라 생각한다"고 판시했다. 한편 여기에서의 '통신'은 종이로 주고받는 편지뿐만 아니라 회사에서 사용하는 모든 전자통신 수단을 의미한다고 보아야 한다.

인권과 기본적 자유 보호를 위한 유럽협약 제8조에 관련된 판결들로부터 유추할 수 있는 세 가지 원칙은 다음과 같다.

① 노동자는 통신장비나 사무기구가 고용주가 제공했다는 사실로 인해 침해되어서는 안되는 회사에서의 프라이버시에 대한 정당한 기대가 있다.
② 통신비밀에 대한 일반적 원칙은 작업장에서의 모든 통신을 포함한다. 이메일과 첨부파일도 포함한다.
③ 사생활에 대한 존중은 타인과의 관계를 발전시킬 권리를 포함한다. 그러한 관계가 상당부분 회사에서 이루어진다는 사실은 감시제도에 대한 고용주의 합법적 요구에 제한을 가한다.

(다) 유럽 회의(Council of Europe)의 **노동자들의 기본적인 사회적 권리 헌장(The Charter of the Fundamental Social Rights of Workers)**

헌장은 노동조합이나 노동자의 대표자들이 그들의 역할을 신속하고 효율적으로 수행할 수 있도록 적절한 설비를 제공받을 권리가 보장되어야 함을 분명히 밝히고 있다(제28조).[154] 따라서 노동조합은 이메일을 이용할 수 있는 시설을 제공받아야 하고, 인터넷을 이용할 시설이 제공되고, 이를 이용할 권리가 보장되어야 한다. 그리고 이러한 권리는 노동조합의 역할을 신속학 효과적으로 수행하기에 적절한 수준으로 보장되어야 한다. 이에 따라서 노동조합은 회사의 컴퓨터 시설을 이용할 권리가 보장되어야 한다. Convention for the protection of individuals with regard to automatic processing of personal data (ETS No.108, the 28 January 1981

154) "workers' representatives" must be afforded "such facilities as may be appropriate in order to enable them to carry out their functions promptly and efficiently".

그 밖에도 EU나 유럽회의는 '개인정보의 자동처리과정에서의 정보호호에 관한 협약(81)[155]', '고용관계에서 사용되는 개인정보 보호에 관한 유럽의회 보고서(89)[156]', '의료정보 보호에 관한 보고서(97)[157]', '사회보험을 목적으로 쓰이는 개인정보 보호에 관한 보고서(86)[158]', '통신서비스 영역에서 개인정보 보호에 관한 유럽의회의 권고안(95)[159]'등을 제출하였다.

(라) 프랑스

프랑스 헌법은 명시적으로 프라이버시권에 대하여 언급을 하고 있지는 않지만, 1970년의 프랑스 민법 제9조는 모든 사람은 프라이버시권을 가지고 있음을 규정하고 있으며[160], 근로자의 프라이버시권도 인정되어져 왔다.

노사관계에 있어서는 노동법(the Labour Code) L.120-2항에서 "어느 누구도 개인의 권리를 제한할 수 없다. 이를 제한하기 위해서는 그 제한이 정당하고 적절한 범위 내이어야 한다"고 규정하고 있는바, 이 규정에 근거하여 프라이버시권을 침해하는 사용자에 대하여 법적 조치를 취할 수 있다. 노동자들은 사용자가 도입하고 있는 모든 감시도구에 대하여 고지를 받을 권리가 있다. L.121-8항은 사용자가 노동자에게 알리지 않은 방법으로 노동자의 개인정보를 수집하는 것을 금지하고 있다.

노동자의 프라이버시를 침해하는 행위가 적법하려면 매우 엄격한 판단을 거쳐야 한다. 프라이버시 침해행위가 적법하기 위해서는 문제되는 프라이버시 침해행위가 근로자가 수행하는 업무와 관련성이 있어야 하고, 그 방법은

155) Convention for the protection of individuals with regard to automatic processing of personal data (ETS No.108, the 28 January)

156) Council of Europe's Working document (89) 2 on the Protection of Personal Data used for Employment purposes. Council of Europe's Recommendation (89) 2 on the Protection of Personal Data used for Employment Purposes 도 참조.

157) Council of Europe's Working document (97) 5 on the Protection of Medical Data12

158) Council of Europe's Working document (86) 1 on the Protection of Personal Data used for Social Security Purposes.

159) Council of Europe's Recommendation (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services

160) Law No. 70-643 of 17th July 1970

목적에 합당한 것이어야 한다[161]. 경제적인 이유는 근로자의 프라이버시권을 침해할 수 있는 사유가 되지 못한다[162]. 프라이버시권은 가장 핵심적인 권리이기 때문에 고용관계에서도 희생되어서는 안된다는 것이다[163]. 따라서 근로자가 동의를 하였다거나 침해적인 감시행위를 묵인했다는 사실만으로 프라이버시권의 침해가 정당화될 수는 없다. 프랑스 대법원(the Cour de Cassation)은 민법 제9조는 사업장에서의 비밀스런 감시 도구의 사용을 금지하는 것이라고 판시하였다(the Noecel case).[164] 나아가 사용자는 위법하게 수집한 정보를 가지고 근로자를 징계하거나 해고할 수 없다[165]. 감시가 적법한 안전목적으로 이루어지는 경우에도 안전문제와의 관련성과 무관하게 모든 말과 행동을 감시하는 경우에는 위법하다고 본다.

노동법 L.122-45는 신념, 정치적 의견, 노동조합 활동에 따라 개인이나 집단을 차별하는 행위를 금지하고 있다. 이 조항에 따라 노동조합 활동에 관한 감시는 엄격하게 금지된다. 사용자는 은밀한 감시로 근로자가 노동조합 활동을 하고 있음을 알아내고 이를 근거로 근로자를 해고하거나 징계할 수 없다.

프라이버시권은 여러 기관에 의하여 보호된다. 국립정보자유위원회(The Commission Nationale de lInformatique et des Libertes : CNIL)는 정보 프라이버시 법(The Information Privacy Law : 1978. 1. 6.)[166]에 의하여 설치되었는데, CNIL은 사업장에서의 프라이버시 문제에 관하여 법률적으로 구속력이 있는 의견제시와 권고를 할 권한을 갖고 있다.

공공부문의 사용자가 전자적인 사업장 감시(monitoring/surveillance) 시스템을 사업장에 설치하고자 하는 경우 CNIL의 사전승인을 얻어야 한다[167]. 민간영역의 경우에는 자동 정보 처리 시스템을 도입하고자 할 경우에는 CNIL에 통지를 해야 한다. 만약 이를 이행하지 않을 경우 근로자에게 손해배상책

161) Ministry of Labour Circular No. 93/10 of 15th March 1993
162) Ministre du Travail v Soci랠?Peintures Corona [1980] 6 Dr. Soc. 317
163) Savatier: Individual rights at work, Droit Social, No 1 January 1990.
164) Cass. Soc. 20th November 1991 (RDS 1992(2), 77).
165) Mme Roussard v Ste. Rebouchon et Fils, 대법원 Social Chamber 결정, 1992. 1. 22.
166) the law of 6th January 1978
167) 위 법 제15조

임을 질 수 있다. 어느 경우에도 정보처리 시스템의 특성과 이를 구축하는 목적과 이유, 그 정보에 접근할 수 있는 자에 대하여 CNIL에 설명하여야 한다. CNIL은 요청을 승인하거나 거부할 수 있고, 구제신청에 대하여 수사할 권한을 갖는다.

근로자가 11명 이상인 사업장에서는 노동자위원회(Works Council)가 노동자의 프라이버시 보호에 핵심적인 역할을 한다[168]. 사용자는 새로운 기술을 도입하거나 감시도구를 비롯해서 근로자의 사업장에서의 활동을 통제할 수 있는 새로운 수단을 도입할 경우 미리 노동자위원회(Works Council)에게 알리고 협의를 하여야 한다[169]. 근로자가 11명에서 50명인 사업장에서는 근로자의 프라이버시 권리가 침해될 경우 노동자 대표단(Workers Representative)은 사용자에게 정식으로 신청을 접수할 수 있다. 이 경우 사용자는 노동자 대표단과 함께 신청에 대하여 조사를 하여야 하고, 그 문제에 대하여 해결책을 모색해야 한다[170] 만약 사용자의 대응이 부적절하거나 합의에 이르지 못할 경우에는 근로자나 대표자는 노사심판소(the office of the industrial tribunal)에 조정을 신청할 수 있고, 여기에서는 일종의 가처분 결정이나(emergency interim ruling) 금전배상을 명할 수 있다[171].

(마) 독일

독일헌법도 프라이버시권에 대하여는 명시적인 표현을 하고 있지는 않다. 그러나 프라이버시권은 국가권력의 남용으로부터 인간의 존엄성을 보호하는 권리(Recht auf Scutz der Menschenwurde)[172], 의 하나로서 헌법상의 일반적인 인격권(Allgemeines Personlichkeitsrecht), 개인의 인격발현의 자유(Recht auf freie Entfaltung)[173]로부터 나오는 것으로 인정되고 있다. 연방노동법원은 이 권리가 근로관계에서도 적용된다고 보고 있다. 노동자의 프라이버시 보호는

168) Article L.431-4
169) Article L.432.2
170) Article L.422 - 1- 1.
171) Article L.422-1-1.
172) 헌법 제1조 제1문
173) 헌법 제2조 제1문

헌법과 각종 법률은 물론 노동조합과 회사의 Works Council에 의한 단체협약에 의하여도 보호된다[174].

모든 근로자는 다른 사람의 권리를 침해하거나 헌법에 위반되지 않는한 자유롭게 자신의 개성을 발현할 권리를 갖는다[175]. 이 권리는 오로지 법률에 의해서만 제한될 수 있다[176]. 사업장에서의 노동자의 프라이버시나 인격권의 보호의 본질은 공공부문과 사적부문에 따라 차이가 있다. 공적부문의 노동자들은 법률이나 단체협약에 위배되지 않는 한 노동자의 작업성과를 측정하거나 노동자의 행동을 감시(monitoring)할 수 있는 도구를 도입하거나 운영하는 문제를 결정하는데 참여할 권리가 있다[177] 이와 같이 참여할 권리는 노동자의 이메일이나 인터넷 사용을 모니터할 수 있는 도구의 도입시에도 인정된다.

사적부문에서는 경영조직법(the Works Constitution Act)[178]이 노동자의 인격권을 보장하는 기초가 된다. 경영조직법은 사용자와 노동자평의회(Works councils)로 하여금 정보통신기술의 활용으로 인한 근로자의 프라이버시 침해에 대하여 보호수단을 마련할 의무를 부과하고 있다[179]. 단체교섭에서 노동자에 대한 감시에 관하여 아무런 합의가 이루어지지 않은 상태인 경우에는 사용자와 노동자평의회가 노동자 감시 도구의 도입이 가져올 문제점에 대하여 전문가의 도움을 받아 합의를 하여야 한다. 이때 사용자는 노동자평의회에 정보를 제공해야 한다. 합의에서는 개인의 노동조합 활동범위, 사업장에서의 적법한 감시(monitoring)의 범위에 대하여 정할 수 있다.

사용자가 온라인 감시도구를 비롯해서 근로자를 감시(monitor)하는 도구들을 도입하고자 할 경우에는 노동자평의회는 공동결정할 권리를 갖는다.[180]

---

174) International Labour Organisation Conditions of Work Digest on Workers Privacy Part II Vol 12 1/1993.
175) Article 2 para 1
176) Article 2 para 2
177) Act respecting workers representation of civil servants, 15th March 1974 as amended, section 75(17).
178) 경영조직법(Works Constitution Act), 15th January 1972 as amended.
179) Federal Labour Court, BAG judgment of 17th March 1987

연방노동법원(The Federal Labour Court)은 그와 같은 공동결정권의 범위를 넓게 해석하였다. 공동결정권은 그 도구가 직접 사용자의 행동을 감시(monitor)하기 위한 것인 경우는 물론 그 도구가 도입되는 주요한 목적이 무엇이든간에 노동자를 감시하는데 적합한 도구인 경우에는 노사평의회의 공동결정권이 인정된다고 본다[181]. 거의 대부분의 컴퓨터 시스템이 사용자에 의하여 근로자의 행동을 감시하는 것으로 사용될 수 있으므로 그러한 기술의 도입은 노동자평의회와의 공동결정이 필요할 것으로 보인다. 공동결정권이 인정되는 경우에는 사용자는 노동자평의회의 동의가 없으면 이를 시행할 수 없다. 연방노동법원(The Federal Labour Court)은 몰래 감시하는 도구를 이용하여 노동자의 사적 영역을 방해하는 경우에는 노동자평의회의 동의가 필요하다고 하였다[182]. 동의가 이루어지지 않는 경우에는 양 당사자는 분쟁을 해결하기 위하여 조정위원회(conciliation committee)의 도움을 받을 수 있다. 이 법의 취지는 노동자평의회의 개입을 인정함으로서 사용자의 부당한 간섭으로부터 노동자의 프라이버시권리를 지키려는 것이다.

한편 독일에는 직장에서 유전자검사를 금지하는 법률이 제정되어 있다[183]

(바) 그 외의 국가들

벨기에, 덴마크에는 노동자에 대한 의료정보와 의료검진에 대하여 특별규정을 두고 있다. 핀란드에는 노사관계에서의 프라이버시 보호에 관한 특별입법이 제정되어 있다. 이탈리아에는 노동자에 대한 감시와 모니터링을 제한하는 특별규정이 있다. 네덜란드의 경우는 노동법에서 노동조합에 대한 정보제공과 동의절차를 규정하고 있으며, 질병정보, 임금정보에 대한 법률에서 노동조합에 정보를 제공하고 의견을 들어야 함을 규정하고 있으며, 어떤 경우는 단체협약을 맺어야 한다고 규정하고 있다. 노동자의 ID 번호의 사용과 관련해서는 사용자가 법적 의무를 이행할 필요가 있을 때에만 노동자의 ID 번

180) Section 87(6).
181) . BAGE decision of 9th September 1975.
182) BAGE judgment of 9th September 1975.
183) Genetic Engineering Act No. 510/1994, Sect. 67.

호를 사용할 수 있다고 규정하고 있다. 스웨덴은 카메라 감시장비를 도입할 경우에는 노동조합의 대표와 협의하여야 한다는 법률규정을 두고 있다. 그리고 노동자의 작업수행을 감시(monitoring)하는 것은 당사자에게 알리고 노동조합의 대표에게 그러한 통제기구(mechanism)의 도입시 사전에 의견을 들어야 하는 의무를 부과하고 있다[184]. 노르웨이의 경우도 직장을 감시(monitoring)하는 경우는 이는 단체협약사항으로 노동조합의 대표에게 알리고 협의를 거쳐야 한다.

(4) 미국

미국은 개인정보의 보호나 노동감시에 대하여 법제도를 발전시키지 못해왔다[185]. 그런 관계로 미국의 경우 연방법률로서 노동감시에 대한 규제법률은 거의 전무하다. 통신의 비밀보호를 위하여 제정된 법률인 전자통신 프라이버시 법률(1986, Electronic Communications Privacy Act of 1986)는 전자통신의 불법감청을 금지하고 있는데, 노동자의 통신을 보호하는 거의 유일한 법이다. 그러나 이 법은 사용자가 업무목적의 네트워크를 감시할 수 있도록 허용하고 있으며, 노동자의 명시적, 묵시적 동의(사용자의 사전통보로 갈음하는 경우가 많다)가 있으면 노동자의 통신을 감청할 수 있게 하고 있어서 많은 비판을 받고 있다.

미국의 경우 1993년에 상원의원 폴 사이먼이 소비자와 노동자의 프라이버시법률안(그 내용은 노동감시를 하고자 할 경우에는 사전동의를 받아야 하고, 감시시에는 사전통보와 고지를 하고, 감시자료에 대한 노동자의 접근권, 감시자료의 이용의 제한 등이었다)을 제안하였으나 통과되지 못하였다. 2000년에는 찰스 캐너디에 의하여 전자감시 통지법안이 제안되었으나 역시 통과되지 못하였다. 주 법률로는 코네티컷 주에서 사용자가 노동자에 대하여 전자감시를 할 경우에는 사전 통지를 하도록 하는 법이 시행되고 있다.

---

184) Article 11 Lag (1976:580), Articles 1 and 3 Lag (1998: 150)

185) 그래서 EU는 EU수준의 개인정보 보호가 되지 않는 미국에 대하여 교역의 규제를 가하려고 하였다. 미국은 EU 개인정보보호 지침에서 요구하는 '적절한 수준'을 만족시키기 위하여 'Safe Habor'원칙을 채택하여, EU와 2000년 7월에 합의하여 11월부터 시행에 들어갔다.

(5) 기타

오스트레일리아의 뉴사우스웨일즈에서는 직장에서의 비디오감시에 대한 규제법이 제정되어 시행되고 있다. 이 법은 은밀한 비디오감시의 원칙적인 금지(범죄혐의를 인정할 충분한 근거가 있고, 행정장관으로부터 허가장을 얻은 경우에만 제한적으로 허용), 공개적인 비디오 감시에 대한 규제(14일 전의 사전 통지와 상시적으로 고지) 등을 내용으로 하고 있다. 그 외에 오스트레일리아의 법률에 의하여 노동자의 직장에서의 통신비밀이 보호되며, 비밀녹음이 금지된다. 최근 뉴사우스웨일즈는 감시행위를 포괄적으로 규제하는 반감시법을 제정하려고 추진하고 있다.

6. 노동감시 규제 및 노동자 개인정보 보호에 관한 입법의 체계와 법률의 내용

가. 법률의 체계

노동감시 규제 및 노동자 개인정보 보호에 관한 입법을 (i) 노동감시에 대하여 다루는 특별한 법률로서 규율할 것인지, 아니면 (ii) 일반적인 감시에 대해 규율하는 법률에서 규율할 것인지가 문제가 된다. 반감시에 대한 일반원칙은 감시에 대한 일반법률을 제정하면서 그 법에서 규율하되, 노사관계에서 특수하게 나타나는 여러 문제에 대해서는 따로 특별한 규정을 두는 것이 좋을 것이다.

다음으로 노동감시에 대한 입법체계의 문제인데, (i) 상세한 규정을 모두 법률에 규율할지, (ii) 법률에서는 중요한 내용을 규정하고 세부적인 상세규정은 하위법률에서 규정할 것인지도 문제가 되는데, 우리 법률체계에 맞게 기본적인 내용은 법률에서 규정하되, 상세한 내용은 법률의 위임을 받아 독립적인 반감시위원회(내지는 프라이버시 보호위원회)에서 강제력을 갖는 규율로 규정하는 것이 좋을 것이다.

나. 구체적인 내용

(1) 노동감시를 바라보는 기본원칙

우선 노동감시의 문제가 헌법상의 기본권의 문제이고, 노동통제의 문제로서 근로조건을 결정하는 문제이며, 노동3권의 보장과 관련된 문제임을 확인하고, 노동감시의 대한 기본원칙을 천명하는 것이 필요하다. 이는 법률해석의 기본원칙이 될 것이다. 노동감시를 노동자 개인과 단체의 개인정보의 수집, 처리, 행동, 생각, 업무실적 등을 수집하거나 평가하는 모든 행위로 정의하고, 노동감시는 원칙적으로 금지되며, 헌법상의 기본권을 침해하는 방식으로 이루어져서는 안되며, 노동3권을 침해하는 방식으로 이루어져서는 안된다는 것을 밝히는 것이 필요하다.

(2) 노동자의 개인정보의 처리에 대한 기본원칙

노사관계에서의 개인정보 처리에 관하여도 OECD의 개인정보처리에 대한 기본원칙이 적용되어야 함은 두말할 나위도 없다. 즉, 개인정보 수집시의 당사자의 동의, 개인정보 수집시 목적의 특정, 목적외 사용금지, 개인정보의 제3자에 대한 제공의 금지, 개인정보주체의 개인정보에 대한 열람, 정정청구권 등이 규정되어야 할 것이다. 그러나 여기에서 더 나아가 노사관계의 특성에 맞게 원칙을 변용시킬 필요가 있다.

(3) 노동자의 개인정보 보호에 대한 원칙

(가) 채용시의 구직자의 개인정보의 보호

노동자의 채용시에는 구직자의 개인정보가 침해될 가능성이 높다. 채용시에 사용자는 구직자로부터 보다 많은 정보를 원할 것인데, 그렇게 되면 사용자보다 열악한 지위에 놓여 있는 구직자의 개인정보는 그만큼 침해될 것이다. 따라서 사용자의 알 권리와 구직자의 프라이버시권이 적절히 조화를 이루는 범위 내에서 개인정보의 수집의 범위가 조정되어야 할 것이다. 예컨대 질병에 관한 정보나 형벌에 관한 정보 등은 당해 업무를 수행함에 있어서 필요한 범위 내에서만 수집되어야 할 것이다. 즉, 채용시에 수집할 수 있는

개인정보는 채용여부를 판단하는데 필요한 정보이어야 하며, 민감한 개인정보를 요구해서는 안될 것이다. 고용 후에 필요한 정보(예를 들어 주민등록정보 등)를 미리 요청해서는 안될 것이다. 채용광고를 내면서 사용자가 원하는 개인정보를 명시해야 할 것이다. 그리고 구직자는 사용자가 구직자에 대하여 다른 경로를 통하여 개인정보를 취득하는지 여부를 고지받아야 한다. 채용시에 구직자의 개인정보가 자동화된 처리과정을 통하여 평가되어 결정이 내려질 경우에는 그러한 결정이 자동화된 처리과정에 의하여 왜곡될 소지가 있으므로 자동화된 처리과정에 의한 결정에 의존해서는 안되도록 제한해야 할 것이다.

(나) 구직자의 개인정보의 보관에 대하여

당사자의 명시적인 동의가 없는 한 구직자의 개인정보를 그 구직자를 채용하지 않는 경우에는 보관해서는 안될 것이다.

(다) 고용계약 하에서의 개인정보의 처리

고용계약 하에서 개인정보의 처리는 앞서 본 (1)의 개인정보 처리의 원칙에 따라 이루어져야 할 것이다.

(i) 수집시의 동의의 원칙

(ii) 목적의 특정, 명시의 원칙

(iii) 직무수행과 관련된 정보의 최소수집의 원칙 : 특히 이 경우 노동자로부터 취득할 수 있는 개인정보의 범위는 당해 고용계약 하에서 노동자의 직무의 수행에 필요한 정보로 제한이 되어야 할 것이다. 특히 정치활동에 관한 정보, 신앙에 관한 정보, 사상에 관한 정보와 그 밖의 민감한 개인정보의 취득은 금지되어야 한다. 가족에 관한 개인정보의 경우에도 그것이 업무의 수행을 위하여 필요한 경우가 아니면 수집되어서는 안 될 것이다. 인종에 관한 정보도 민감한 정보로서 수집되어서는 안된다. 질병에 관한 정보는 당해업무 수행과 관련이 있는 범위 내에서만 수집되어야 하며, 이용되어야 한다. 업무와 관련이 없는 질병에 관한 정보를 취득하기 위한 신체검사도 허용되지 않는다.

(iv) 의료정보의 특별한 보호 : 특히 질병에 관한 정보에 대해서는 노동자의 열람권과 항변권, 정정권이 인정되어야 한다.

(v) 정확성, 최신성 유지 : 그리고 노동자의 개인정보는 항상 최신성을 유지하여 정정되어야 한다.

(vi) 목적외 사용의 금지와 제3자 제공의 금지 : 내부적으로도 목적외로 이용되지 않도록 한다. 어떤 노동자에 대한 결정이 그 노동자에 대한 자동 처리된 개인정보에만 의존해서 이루어지면 안되며, 전자 감시로 수집된 개인정보가 직무 수행 평가의 유일한 요소가 되어서는 안된다. 제3자 제공은 당사자의 동의가 있는 경우에만 허용되어야 할 것이다.

(vii) 보안 : 보안이 유지되어야 하며, 안전하게 보관되고, 해당업무를 담당하는 자 외에는 개인정보가 공개되거나 제공되어서는 안될 것이다.

(viii) 정보의 통합 : 개인정보의 통합은 원칙적으로 금지되며, 최초에 수집한 목적을 넘는 개인정보의 통합은 허용되어서는 안될 것이다.

(ix) 접근 : 이때 사용자는 노동자의 개인정보에 접근할 수 있는 업무담당자를 미리 지정해서 통보해야 할 것이다.

(4) 노동자에 대한 감시

노동자에 대한 감시는 허용되어서는 안된다. 다만 아래에서 보는 바와 같은 특별한 경우에 예외적으로 허용될 수 있을 것인데, 이 경우에도 (i) 감시가 이루어지고 있다는 점에 대한 명시적이고 계속적인 고지와 표시가 있어야 하고, (ii) 감시의 결과물에 대한 노동자의 열람 및 정정이 허용되어야 하며, (iii) 감시의 결과물에 대하여 접근할 수 있는 자, 보관 및 폐기의 주기, 보안대책 등이 마련되고 공표되어야 하며, (iv) 어떤 경우에도 감시는 인격권을 침해하지 않는 범위 내에서 가장 침해가 적은 방법으로 이루어져야 하며, (v) 감시의 결과물은 노동자에 대한 평가의 자료나 불리한 평가의 자료로 이용되어서는 안된다. 그리고 감시장치를 도입할 경우에는 사전에 노동조합에 통지하고, 노동조합과의 단체협약을 통하여 동의를 얻어서 도입하여야 한다.

(가) CCTV를 통한 감시

CCTV를 통한 감시는 위험방지를 위해서만 허용될 수 있다. CCTV를 설치하는 경우 이는 근로조건과 밀접한 관련이 있으므로 노동조합의 동의를 얻어야 할 것이다. 이 경우에도 CCTV 감시는 노동자의 작업모습을 직접 촬영할 수 있는 방법으로 이루어져서는 안될 것이다. 한편 CCTV를 촬영하고 있을 때에는 CCTV 촬영중이라는 표시가 크고 선명하게 보이도록 하고, 촬영된 녹화분에 대해서는 당사자의 열람 및 정정이 가능해야 할 것이다. 그리고 촬영된 녹화분의 보호관리에도 만전을 기해야 할 것이다,

(나) 이메일 감시

노동자의 이메일에 대한 감시도 원칙적으로 허용해서는 않는다. 따라서 노동자의 이메일을 사용자가 서버에 저장하는 경우에도 이메일에 대한 접근은 허용되지 않는다. 노동자의 이메일 사용과 관련한 어떤 기록이나 추적도 허용되지 않는다. 노동자는 회사 내에서 이메일을 이용할 자유가 있으며, 이를 시스템의 운용을 위하여 불가피한 경우가 아니라면 제한할 수 없다. 노동자의 이메일이 업무를 내용으로 하는 것인 경우에는 회사의 업무수행의 절차로서 이메일을 열람, 저장할 수 있으나, 이 경우에도 해당 이메일에 노동자의 개인정보가 포함되어 있는 경우에는 개인정보처리에 대한 원칙에 의하여 처리되어야 한다.

(iii) 인터넷 이용 감시

노동자의 인터넷 이용에 대하여 차단, 감시는 허용되지 않는다. 노동자의 인터넷 이용의 자유도 원칙적으로 제한되어서는 안된다. 다만 당해 인터넷의 이용이 범죄행위를 구성하는 경우에는 사용자는 노동자의 해당 인터넷 이용을 차단할 수 있다. 이 경우에도 사전에 인터넷 이용을 차단해야 하며, 노동자의 인터넷 이용을 감시해서는 안된다. 인터넷을 차단할 경우에는 차단하는 인터넷 웹사이트의 목록 등을 공개하여야 하며, 노동자의 이의신청을 허용해야 한다. 노동자의 인터넷 이용에 대한 로그기록 등은 사용자에 의하여 접근, 열람되어서는 안되며, 부득이하게 컴퓨터 시스템의 운영과정에서 자연적으로 노동자의 인터넷 로그기록을 사용자가 서버에 저장하고 있는 경우에도

그 로그기록은 엄격하게 비밀로서 관리되어야 하고, 적절한 주기에 의하여 삭제되어야 한다. 특히 노동자가 인터넷을 이용하여 노동조합과 관련한 활동을 하는 경우, 이것이 정당한 범위 내에서 노동조합활동으로서 이루어지는 경우에는 제한되거나 이를 이유로 불이익한 처우를 받아서는 안된다.

(iv) 기타 컴퓨터 감시

노동자의 컴퓨터 이용에 대한 감시와 컴퓨터의 내용에 대한 감시는 허용되지 않는다. 다만, 바이러스의 체크 등과 같이 컴퓨터시스템의 운영을 위하여 필요한 경우에 그러한 목적으로 내용을 감시하지 않는 범위 내에서만 당사자의 동의를 얻어 컴퓨터의 내용에 대한 감시가 허용될 수 있다. 사용자는 업무수행을 위하여 필요한 경우 노동자의 컴퓨터의 내용 중에서 노동자의 업무와 관련된 부분에 대해서 분리하여 당사자의 사전동의를 얻어 노동자의 컴퓨터 내용을 열람할 수 있다.

(v) 위치추적, 생체정보를 이용한 감시

어떠한 방법으로도 개별적인 노동자의 위치가 파악되는 장치나 기구 등의 이용은 허용되지 않는다. 단, 위험방지를 위하여 필요한 경우로서 다른 방법이 없는 경우 당사자의 동의를 얻어 위치추적을 할 수 있다. 생체정보를 이용한 감시도 위험방지를 위하여 필요한 경우로서 다른 방법이 없는 경우 당사자의 동의를 얻어서만 허용된다. 어떠한 경우에도 노동자에 대한 유전자 검사, 기타 생체정보를 이용한 검사는 허용되지 않는다.

(vi) 스마트카드, ID카드

스마트카드나 ID카드를 도입하고자 할 경우에는 이를 도입함으로써 노동자의 개인정보의 보호에 미치는 영향, 오용가능성 등을 평가하여 사전에 노동자의 동의를 받아야 하며, 도입 이후에도 노동자가 시행평가를 통해 도입 철회를 요구하는 경우에는 그에 따라야 한다.

사. 노동자의 작업수행의 평가

노동자의 작업수행을 평가하는 시스템을 도입하고자 할 경우에는 노동조합에게 사전통지를 하고, 단체협약을 통하여 동의를 얻어야 한다.

이 경우에도 평가정보를 수집하는 것은 (i) 당해 노동자를 식별할 수 없도록 처리가 되거나, (ii) 당해 노동자를 식별할 수 있는 정보로 수집되는 경우에는 주단위나 월단위로 통합된 결과로 처리하여 수집되어야 하며, 이와 같이 수집된 정보가 노동자에 대한 평가의 유일한 근거나 주요한 근거가 되어서는 안된다.

아. 노동감시 기구나 시스템, 제도의 도입시의 노동자의 동의와 사후평가

사용자가 노동감시의 기구나 시스템, 제도를 도입할 경우에는 사전에 노동조합의 동의를 얻어야 하며, 노동자는 이러한 기구나 시스템, 제도에 대하여 동의를 한 후에도 평가를 바탕으로 도입을 철회할 것을 요구할 수 있다.

자. 동의

동의는 개별적인 동의와 집단적인 동의로 나누어 근로조건과 관련된 것은 집단적 동의가 필요한 것으로 하고, 개인적인 동의만 받아도 되는 것은 개인적인 동의를 받아야 하는 것으로 한다.

차. 기타

형사처벌조항, 권리구제 수단(노동위원회 제소, 프라이버시위원회 : 반감시위원회에 제소), 권리포기의 금지

참고 : 우리나라의 행정기관의 보유 데이터베이스 현황 및 공동이용 현황

행정기관 보유 DB 현황

ㅇ 행정정보DB : 960종

구 분	D B 종 류	DB수
중앙행정기관	법령심사정보, 국유재산정보, 지적 · 주민, 공시지가 등	294종
지방자치단체	자치법규, 개별공시지가 산정, 도로전용료 관리,지방세 관리 등	589종
시 · 도교육청	검정고시 합격자화일, 학원관리, 도서관리, 박물관소장자료 등	77종

ㅇ 개인정보DB : 388종

구 분	D B 종 류	DB수
중앙행정기관	국가유공자 취업관리, 학적화일, 입원환자 파일, 소득조회 파일 등	90종
지방자치단체	종합토지세 파일, 재산세 파일, 호적 · 제적관리, 의료보호 파일 등	107종
각 급 학 교	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)

참고 : 행정정보 공동이용 현황(27개 기관, 79종 DB 상호활용)

제공기관	제 공 정 보(DB)	이 용 기 관	용 도
국가보훈처	교육보호, 보상금관리, 취업관리 등 6종	정보통신부, 공무원 연금관리공단 등 6개기관	이체의뢰 등
외교통상부	여권분실정보	법무부	출입국시 위조여부 검사
재정경제부	세입 · 세출결산자료	국세청, 관세청, 정보통신부, 정부회계관서 등	세입자료 입력, 지출액 정리 등
법 무 부	재 · 출소 증명원, 수형자 석방통보, 가석방통보 등 4종	검찰, 경찰, 국민연금관리공단 등	수사자료 및 업무용
국 방 부	장군현황, 군인대부현황, 군인연금 현황 등 7종	행정자치부, 국회, 감사원, 재정경제부 등	-
행정자치부	주민등록정보, 종합토지세자료 등 2종	국세청, 감사원, 경찰청, 서울시 및 지방자치단체	종합토지세부과용DB 구축, 주민DB구축
교 육 부	기관코드	병무청	병무업무전산화
농 림 부	전국유통정보, 가락동유통정보 등3종	해양수산부, 유통공사, 농림수산정보센터 등	기관 게시, 보관, 정책자료, 보도용
산업자원부	등록자료현황	각시도 광업관련부서	광업업무처리
보건복지부	면허정보	행정자치부, 의료인협회 등	비상대비자원관리
환 경 부	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, 환경개선 부담금, 지가검색 등
해양수산부	원양생산통계	통계청	통계자료집 발간
국 세 청	종합소득자료 등 5종	행자부, 재경원 등	주민세 과세, 보험료 산정 등

제공기관	제 공 정 보(DB)	이 용 기 관	용 도
관 세 청	수출입통관자료 등 4종	국세청, 감사원 등	원산지증명발급, 수출입동향 분석 등
조 달 청	외자구매요구서 등 10종	조달요청기관, 조달업체	입찰정보제공 등
통 계 청	통계정보시스템	모든기관	통계자료활용
검 찰 청	피의자인적사항, 검사처분내용 등 4종	법원, 보호관찰소 등	법원판결에 참조
병 무 청	제1국민역 및 징병검사대상자	경찰청	운전면허 발급가부 결정
기 상 청	기상관측, 예보·특보자료, 북한DB, 기후DB 등 4종	행정자치부, 농수산부, 해군, 항공사, 언론사 등	정부기관자료제공 및 연구·보고자료
농촌진흥청	농업기술종합정보	농림수산정보센터	농업인정보제공
산 림 청	임업통계	통계청	통계자료제공
해양경찰청	사건사고정보	해양수산부	상황관리
특 허 청	출원·등록화일, 초록 및 전문명세서	특허기술정보센터	대민서비스
식품의약품 안 전 청	수입식품관련자료, 의약품허가자료 등 3종	관세청, 6개 지방청	수입식품검사업무, 통관업무, 의약품 허가관리 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 - 정부측, 행정자치위원회 수석전문위원 박봉국, 2000. 12. p.31-32)

참고문헌

국내문헌

강경근, 1998. “정보공개법 실천의 의의와 법의 내용” 언론개혁시민연대 정보공개운동 토론회.

강상현, 1996, 『정보통신혁명과 한국사회』, 한나래.

고영삼, 1997, “정보화촉진계획과 개인정보 침해문제”, 97년 전기 한국사회학대회 발표문.

_____, 1998. 『전자감시사회와 프라이버시』, 한울아카데미

권영성, 2002. 『헌법학 원론』, 법문사

김기중, 1997, “우리나라 주민관리제도의 비판적 분석”, 대한변호사협회 토론회 발표문.

김병욱, 1979, “주민등록증 제도에 관하여”, 「사법행정」 1979년 2월호.

_____, 1997, “주민등록제도의 의의와 연혁 개관”, 「사법행정」 1997년 7월호.

김성언, 2001, 『개인정보 침해에 관한 조사 연구』, 한국형사정책연구원.

김종인, 1996, 「행정정보시스템 구축방안에 관한 연구」, 서울대학교 행정대학원 석사학위논문.

김종철, 2001, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 『인터넷법률』, 2001년 4호

김현곤, 1997, “정보공동활용의 방향”, 한국전산원, 「정보화동향」, 4권7호(1997.4.21)

박형준, 1997, “정보화사회론의 쟁점들”, 「동향과 전망」 33호(97년 봄호).

박홍윤, 1994, 「한국의 통합정보관리체계에서 개인정보프라이버시 보호에 관한 연구」, 서울대학교 대학원 행정학과 박사학위논문.

_____, 1997, “전자주민카드, 과연 편리하고 효율적인가?”, 대한변호사협회 토론회 발표문.

법무부, 2000, 『호주제도, 무엇이 문제인가』

변재옥, 1979, 「정보화사회에 있어서의 프라이버시의 권리」, 서울대학교

대학원 법학과 박사학위논문.

_____, 1997, “정보화사회에 있어서 전자주민카드의 의미와 그 폐해”, 대한변호사협회 토론회 발표문.

서울대학교 사회과학연구소, 1989, “행정전산망 구축에 따른 사회적 함의에 관한 조사연구”.

신원철 · 최재혁, 1995, “정보화와 개인의 프라이버시 : 한국의 국가기간전산망사업을 중심으로”, 김진균 엮음, 『정보화와 사회조직』, 서울대학교 대학원 사회학과.

이병희, 2001, 『프라이버시 보호와 범죄자 신상공개』, 한국형사정책연구원.

이성철, 1996, “정보사회와 프라이버시”, 창원대학교 사회과학연구소, 「정보화시대의 공동체」.

이윤희, 1996, “정보사회에서의 통제 양식의 변화”, 한국사회학회, 「정보통신기술발달과 현대사회」.

장영민, 1996, “정보통신망 발전에 따른 개인정보 보호”, 한국형사정책연구원, 「정보사회와 범죄」.

조동기, 1996, “정보화사회에서의 개인의 정체성과 프라이버시의 문제 - 전자공동체의 가능성과 관련하여”, 한국사회학회, 「정보통신기술발달과 현대사회」.

총무처, 1996, 「공공기관의 개인정보화일 목록집」, 1996.10.

최장집, 1993a, “한국 정치균열의 구조와 전개”, 『한국민주주의의 이론』, 한길사.

_____, 1993b, “한국국가론의 비평적 개관”, 『한국민주주의의 이론』, 한길사.

통합전자주민카드 시행반대와 프라이버시권리 보호를 위한 시민사회단체 공동대책위원회, 1997, 「전자감시사회와 전자주민카드」

_____, 1997, ‘이한영 주소유출사건에 대한 성명서’, 1997년 3월 3일.

한국공법학회, 1989, 「정보의 수집 · 관리와 사생활보호」.

한국전산원 엮음, 1999, 『국가 정보화백서』, 한국전산원.

_____, 2000, 『국가 정보화백서』, 한국전산원.

호주제 폐지를 위한 시민연대, 2000, 『양성평등과 호주제 폐지 그리고 그 대안』

외국문헌

Adam White, 1999, "Scoville, Clear Signatures, Obscure Signs", 17 Cardozo Arts & Ent. L.J.

Ann Bartow, 2000, "Our Data, Ourselves: Privacy, Propertization, and Gender", 34 U.S.F.L. Rev.

David Brin, 1998, "The Transparent Society: Will Technology Force Us to Chose Between Privacy and Freedom?", Perseus Press

David Lyon, 1994, 『The Electronic Eye』: The Rise of Surveillance Society, Oxford: Basil Blackwell

_____, 2001, 『The Surveillance Society』 Open Univeresity Press

Gavin Skok, 2000, "Establishing a Legitimate Expectation of Privacy in Clickstream Data", Michigan Telecommunications & Technology Law Review.

Geoffrey A. North, 2002, "Carnivore In Cyberspace: Extending The Electronic Communications Privacy Act's Framework To Carnivore Surveillance", 28 Rutgers Computer & Tech. L.J. 155 Rutgers Computer and Technology Law Journal.

Jerry Kang, 1998, "Information Privacy In Cyberspace Transactions", 50 Stanford Law Review.

Judith Wagner Decew, 1997, "In Pursuit of Privacy: Law, Ethics and the Rise of Technology", Cornell University Press

Karl D. Belgum, 1999, "Who Leads at Half Time?: Three Conflicting Versions of Internet Privacy Policy", 6 Rich. J.L.&Tech.

Ken Gormley, 1992, "One Hundred Years of Privacy", Wisconsin Law Review 1335

Lawrence E. Rothsteinf, 2000, "PRIVACY OR DIGNITY?: ELECTRONIC

MONITORING IN THE WORKPLACE", New York Law School Journal of International and Comparative Law.

Michael Froomkin, 2000, "The Death of Privacy?", 52 Stanford Law Review.

_____, 2002, "The Uneasy Case for National ID Cards as a Means to Enhance Privacy", University of Miami School of Law,

Peter H. Huang, "The Law and Economics of Consumer Privacy Versus Data Mining", http://papers.ssrn.com/paper.taf?abstrate_id=94041

Privacy International, 2001, 2002, "Privacy and Human Rights 2001, 2002".

Roger A. Clarke, 1989, "Human Identification in Record Systems", http://www.anu.edu.au/people/Roger.Clarke/

_____, 1992, "The Resistible Rise of the National Personal Data System", http://www.anu.edu.au/people/Roger.Clarke/

_____, 1994, "Human Identification in Information Systems: Management Challenges and Public Policy Issues" http://www.anu.edu.au/people/Roger.Clarke/

Ronald L. Plesser, James J. Halpert, Emilio W. Cividanes, 2002, "USA Patriot Act For Internet And Communications Companies", Computer and Internet Lawyer.