2005년도 인권상황실태조사
연구용역보고서

# 사업장 감시시스템이 노동인권에 미치는 영향

국가인권위원회

이 보고서는 연구용역수행기관의 결과물로서,
국가인권위원회의 입장과 다를 수 있습니다

# 사업장 감시시스템이 노동인권에 미치는 영향

2005년도 국가인권위원회 인권상황실태조사
연구용역보고서를 제출합니다

2005. 12.


연구수행기관 한국노동사회연구소

연구책임자 박준식 (한림대학교 사회학과 교수)

연구원 김유선 (한국노동사회연구소 소장)

김인재 (상지대학교 법학과 교수)

이병훈 (중앙대학교 사회학과 교수)

정진주 (한국여성개발연구원 연구위원)

김현우 (한국노동사회연구소 연구위원)

# - 목 차 -

## 1장. 서론



## 2장. 사업장 감시시스템의 일반적 현황

## 3장. 사업장 실지조사



## 4장. 조합원 설문조사

## 5장. 국제 기준과 해외 제도의 사례



## 6장. 법적 규제 개선방향

## 7장. 결론

# 1장. 서론

## 1. 정보기술의 발전과 전자감시 체제의 등장

조직과 권력이 존재하는 사회에서 '감시'(surveillance)는 어디에서나 존재할 수 있는 인간 사회의 보편적 현상의 하나로 볼 수 있다. 감시는 전자정보의 시대뿐 아니라 권력의 남용과 이로 인한 인권 침해의 가능성이 존재하는 모든 사회 조직의 보편적 문제의 하나로 볼 수 있을 것이다. 전통적 의미의 감시는 감시하는 존재와 감시당하는 존재의 '시·공간적 거리'를 일정한 부분 불가피한 것으로 전제하고 있었다. 그러나 정보기술의 발전과 더불어 시시각각 새롭게 등장하는 고도의 소프트웨어와 하드웨어는 감시의 내용과 성격을 그 본질에서부터 뒤바꿀 조짐을 보이고 있다.

전자감시가 오늘날의 정보기술사회에서 특별히 문제시되는 이유는 무엇인가? 전자감시 체제를 우리가 문제시해야 하는 근본 이유의 하나는 이것이 인간의 '신체'와 '정신', '시간'과 '공간', '공적 영역'과 '사적 영역'을 가리지 않고 무한대로 그 영역을 확장할 수 있는 새로운 기술적 가능성을 현실화시켰기 때문으로 볼 수 있다. '유비쿼터스'(ubiquitous)라는 형용사의 사전적 의미는 '한 번에 모든 곳에 존재하는', 혹은 '모든 곳에 존재하는 것처럼 느껴지는'이라는 의미를 담고 있다.

오늘날 정보기술은 전통적 의미의 감시가 갖는 시·공간적 제약을 완전히 넘어서는 '범신론적' 개념으로 확장되고 있다. 우리가 존재하는 어떤 시간, 어떤 공간에서도 누군가에 의한 감시가 존재할 수 있고, 우리가 그러한 감시 시스템의 존재를 항상적으로 느끼며 살아가는 사회가 도래했다는 것은 정보기술로 상징되는 '도구적 이성', '기술적 합리성'이 자유인의 본질적 내용을 구성하는 '프라이버시', '개인', '자유', '인권' 등을 원천적으로 침해할 수 있는 모든 가능성을 열어두고 있

음을 의미하는 것이다.

감시기술의 고도화는 근대 세계의 탄생과 더불어 새로운 시대의 이념적 틀을 구상하였던 사상가들의 생각 속에 이미 상당한 부분 그 단초가 담겨져 있었음을 볼 수 있다. 제레미 벤담이 제안했던 '판옵티콘'(panopticon)의 구상은 근대적 조직 세계가 확장되는 과정에서 사회 조직의 구석구석에 명시적 혹은 묵시적 형태로, 의식적 혹은 무의식적 양상으로 파고들어 갔음을 볼 수 있다.

지난 세기의 초반기에 미국의 엔지니어였던 테일러는 작업장에서 이루어지는 노동자들의 모든 신체적 동작에 '과학적 분석'의 틀을 입히려는 시도를 전개하였다. 사회 시스템에 의해 체계적으로 격리된 사회적 집단 뿐 아니라 일터에서 정상적으로 일하는 노동의 세계를 수치화 된 정보로 전환시킴으로써 감시의 영역을 노동의 영역으로 확장시킨 것이다. 작업장의 곳곳에 설치된 카메라, 모니터, 바코드, 전자카드, 도구적 하드웨어와 결합된 실시간의 데이터베이스 시스템은 근대적 감시 시스템의 꿈을 현실로 전환시켜주고 있다. 20세기 후반부터 작업장과 일상생활의 전 영역에 걸쳐 급속히 파급된 전자감시 시스템의 등장이 판옵티콘의 가능성을 현실화시켜가고 있는 것이다.

새로운 전자감시 기술은 인간 활동의 전 영역에 걸쳐 총체적 차원에서 효과적인 감시를 가능케 하고 있다는 점에서 권력의 입장에서는 가장 유용한 통제 도구가 되고 있는 반면, 사회적 차원에서는 인권과 프라이버시에 대한 대단히 심각한 도전이 아닐 수 없다.

감시자의 입장에서 볼 때 작업장의 세계는 판옵티콘의 이상을 실현하는 시급한 사회적 장이었다. 산업 자본주의 체제가 요구하는 대규모 작업장과 조직은 그 속에서 일하는 사람들의 일거수 일투족에 대한 철저한 파악과 통제를 요구하였고, 아무도 저항하기 힘든 합리적 감시 시스템의 필요성은 통제에 대한 노동자들의 저항이 커질수록 더욱 절실해졌다. 근대적 작업장은 거대한 조직을 효과적으로 작동시키기 위해 조직의 원리에 부합하지 않는 모든 요소들, 틈새들, 저항들을 제거할 것을 요구하였고, 그러한 일들을 효과적으로 달성한 조직들만이 살아남을 수 있는 도구적 이성의 지배를 허용했던 것이다. 이러한 도구적 이성은 조직의 복잡성이 증가하고, 직접적 감시가 어려운 조직 생활의 모든 영역들을 파고들었을 뿐

아니라, 작업장의 영역이 확장되는 것과 더불어 그 외연을 확대해 왔던 것으로 볼 수 있다.

감시 기술은 권력의 의지와 도구적 합리성이 결합되는 곳에서 최고의 기회를 맞았다. 권력의 소지자들은 조직의 규모와 복잡성이 증가하고, 작업장의 외연이 급속히 확장되면서 직접적 감시가 어려운 공간, 몸, 내면 등에 대하여 복합적 감시를 필요로 하게 되었고, 정보기술은 이러한 권력의 수요에 민감하게 반응하여 그 목적에 적합한 고도의 감시 기술들을 제공했던 것이다. 권력의 주체들 역시 그들의 목적 달성을 위하여 기술적 혁신이 진행될 때 마다 이를 '업데이트'할 필요성이 있었다. 권력과 도구적 합리성의 상호작용은 감시기술에 대한 사회적 통제의 여지를 무력화시켰고, 기술에 대한 민주적 통제의 여지가 약화된 사회에서 감시기술의 무한 증폭은 의지만 있으면 인간의 자유와 인권을 얼마든지 침해할 수 있을 정도의 가공할 능력을 보유할 정도로 가속화되어 온 것으로 볼 수 있다.

전자정보 감시기술의 급속한 확산과 고도화는 기술에 대한 사회적 개입의 필요성을 시급하게 요구하고 있다. 정보감기 기술의 발전이 도구적 이성과 권력의 의지에 의해서만 일방적으로 추동될 될 경우 인간 해방의 수단으로 기술이 활용될 수 있는 가능성을 체계적으로 닫아버릴 수 있기 때문이다. 도구와 기술은 그것이 존재하는 사회적 맥락과 분리될 수 없음에도 불구하고, 효율성 중심의 경쟁 자본주의와 권력에 대한 민주적 통제가 부재한 비민주적 사회는 통제 기술의 활동 공간을 마음껏 허용해 왔다. 그 결과 인간의 가능성과 해방을 위해 활용되어야 할 기술이 도리어 자유와 인권을 심각하게 침해할 수 있는 수단으로 전환되어 활용되고 있는 것이다.

어떠한 기술도 궁극적으로 그 기술을 만들어 낸 사회의 맥락과 독립적으로 존재할 수 없는 것처럼 이제 우리 사회에서도 정보감시기술의 민주적 활용과 규제에 대한 본격적인 관심과 연구가 절실히 요구되고 있다. 정보감시기술은 태생적으로 정치사회와 권력의 맥락에서 벗어날 수 없다. 그러한 기술을 탄생시키고, 발전시켜 오늘날의 수준에 도달하도록 만든 핵심 배경에 정치사회적 맥락이 작용해 왔기 때문이다. 그러한 의미에서 감시기술의 민주적, 인간적 활용을 위해서는 기술의 활용을 심각하게 왜곡해 온 사회 영역에서의 민주적 개입이 반드시 필요한

것이다.

감시기술의 발전 과정을 사회적 맥락과 더불어 역사적으로 볼 때 오늘날의 고도화 된 전자감시 기술 역시 권력, 시장, 정치, 행정의 복잡한 상호 작용을 통해서만 제대로 이해될 수 있다. 역으로 기술의 발전과 적용 과정에서 사회적 요인이 핵심 위치를 차지한다는 것은 인간의 자유와 인권에 결정적인 영향을 미치는 기술의 개발, 도입, 형성 및 발전 과정에서 민주적 통제, 시민적 참여, '공론장'(public sphere)을 통한 '숙의'(deliberation)가 반드시 요구된다는 것을 의미한다. 이러한 점에서 볼 때 정보기술의 인간적 활용을 위한 사회의 민주적 개입 정도는 정보기술 중심 사회의 성숙과 선진화 정도를 가늠하는 중요한 지표로 볼 수 있다.

근대 세계를 넘어 탈근대를 향한 사회의 재구성이 빠른 속도로 진행되는 오늘날의 상황에서 감시기술이 인간의 생활과 노동 세계의 전 영역에 급속히 확산되고, 더욱 깊숙이 파고들고 있는 오늘날 노동의 고통으로부터 인간을 해방시킨 기술적 요소들이 또다시 권력에 의해 인권과 민주주의에 대한 중대한 위협으로 전환되고 있음을 심각하게 인식할 필요가 있다. 새로운 감시기술이 우리의 일터와 조직에서 어떠한 방식으로 오용될 수 있는가를 제대로 인식하고, 이러한 오용이 미칠 수 있는 인간 억압의 가능성을 판별하여, 이에 대한 사회의 민주적 개임의 가능성을 열어 놓는 것은 탈근대 시대의 민주적 사회 세력이 추구해야 할 중요한 과제이다.

## 2. 유토피아와 디스토피아

종교, 과학, 정치 등 인간에 의해 수행되는 행위 영역들이 다른 영역들과는 구분되는 자체의 합리성과 내재적 발전의 논리를 지니고 있는 것처럼 기술도 사회의 영역과 구분되는 자체의 논리가 존재하고 있는 것으로 볼 수 있다. 극단적 사회 결정론의 관점에서 본다면 이러한 기술의 자율성마저 사회경제, 혹은 정치적

논리에 의해 지배되는 것으로 볼 수 있지만, 우리는 기술이 지니는 고유한 자기 논리를 부인할 수는 없을 것이다. 문제는 기술적 합리성도 사회적 맥락과 독립적으로 존재하는 것은 불가능하다는 데 있다. 기술이 어떠한 사회적 논리, 특히 어떠한 권력의 논리에 의해 활용되는가에 따라 기술의 얼굴은 두 가지 이념형으로 극단화될 수 있는 가능성이 언제나 존재한다.

기술합리성의 논리가 극단적으로 전개될 때 우리는 전자감시 체제를 '유토피아'로 미화시키는 논리에 접하게 된다. 기술은 권력과 사회의 맥락에 관계없이 독립적인 것이며, 결국 부족한 인간의 욕망을 충족하고, 삶의 질을 높이는 수단이 된다는 것이다. 이러한 논리로 본다면 기술과 권력은 아무런 상관성이 없다. 반대로 기술이 권력에 의해 완벽히 종속되는 '디스토피아'의 상황을 가정할 수 있다. 이 경우 기술은 권력의 완벽한 종속변수로 인간 통제의 더욱 고도화된 수단이 될 수밖에 없는 것이다.

우리가 경험하는 현실의 세계는 이 두 극단적 세계의 중간 어디엔가 위치할 것이다. 문제는 전자감시기술이 이 두 세계 가운데에서 차지하는 위상이다. 전자감시기술은 그 개념에서 드러나고 있듯이 인간의 신체와 정신 활동에 대한 모든 정보를 실시간으로 획득하고, 기록하며, 보관하여 권력의 통제 의지에 이를 제공하는 데 주된 목적을 두고 개발, 설치, 활용된다. 이렇게 볼 때 감시기술은 '권력'에 의해 도입되고, 조직되며, 활용되는 기술적 시스템으로 볼 수 있을 것이다.

고전적 권력의 개념은 상대방의 의지에 관계없이 권력자의 의지를 상대방에게 강제한다는 의미를 포함하고 있다. 그러나 보다 확장된 의미의 권력은 단순한 강제력 이상의 의식 및 무의식적 과정을 포괄하며, 권력의 네트워크에 의해 지탱되는 순응의 기제 전반을 지칭할 수 있다. 전자감시기술은 기본적으로 권력의 의지를 강제하기 위한 수단이지만, 단순한 강제력 이상의 강력한 의미를 지닌다. 전자감시기술이 포괄하는 범위는 우리 눈앞에 존재하는 명시적 행위 뿐 아니라, 우리가 느끼지 못하는 가운데 은밀하게 작동되는 훨씬 교묘한 정보감시와 수집에 관련된 기술적 요소들, 소프트웨어들, 그리고 이들이 결합된 네트워크 전반을 포함하는 훨씬 넓은 의미를 내포하고 있다. 문제는 이러한 기술적 요소들은 급속도로 고도화되어, 네트워크의 통제력을 엄청난 속도로 확장해가고 있는 반면, 네트

워크에 대한 사회의 민주적 참여, 윤리적 기준, 투명한 감시, 합리적 통제의 수단들은 거의 찾을 수 없는 불균형의 상황, 기술과 사회의 '짝 풀림'(decoupling)이 가속화되고 있다는 데 있다.

오늘날 우리들은 일터에서 고도의 전자감시 기술과 통제없는 권력이 결합되어 자유와 인권을 침해하는 사례들을 수없이 경험하고 있다. 탈현대의 작업장은 사실상 거대한 전자감시의 공간으로 변모할 기술적 가능성을 이미 거의 완성시켜 가고 있는 것으로 판단된다. 전자감시의 영역은 권력의 감시가 필요한 부분에 대해서는 시간과 장소를 구분할 필요가 없을 정도의 포괄적인 범위로 확장되었다. 일터를 중심으로 일상생활의 전 영역에 걸쳐 확장되어가는 정보네트워크는 그 자체가 거대한 시스템이며, 우리가 접하는 구체적인 정보기술의 하드웨어와 소프트웨어는 언제든지 그 시스템의 촉수이자 단말장치로 전환된 수 있게 되었다. 우리가 일하는 시간과 공간이 확장되고, 전자정보기기 사이의 의사소통이 전면화 되면서 감시 시스템도 인간의 모든 시간과 공간을 포괄할 수 있게 된 것이다.

이러한 상황에서 전자감기시술에 대한 민주적 통제와 개입이 이루어질 수 없다면, 사업장 감시 체제 속에서 일하는 노동자들의 인권을 보호하기 위한 적극적 대책이 이루어지지 않는다면, 전자감시 네트워크를 통해 이루어지는 권력의 개입을 통제할 수 있는 방법은 거의 없는 것으로 보아야 할 것이다. 민주적 통제를 결여한 기술적 합리성이 지향해 온 기술 유토피아의 세계는 이른바 '일렉트로닉 판옵티콘'(electronic panopticon)을 통해 권력에 대해 무한 통제권을 허용하는 디스토피아로 전락하게 될 가능성을 배제할 수 없다.

물론 전자감시기술의 도입을 적극적으로 몰아붙이는 세력의 입장도 그 나름대로 '도입의 합리성'을 보유하고 있다. 가장 강력한 도입의 논거는 경쟁을 위한 '효율성'(efficiency)의 논리일 것이다. 정보기술의 도입이 개인, 조직, 국가의 효율성과 경쟁력을 결정적으로 좌우하는 상황에서 이러한 기술을 적극적으로 도입하지 않는 것은 합리성을 추구하는 자본의 입장에서 볼 때 '자살행위'에 다름 아닐 것이기 때문이다. 경쟁을 위한 효율성 향상의 합리성의 논리에 대한 전면적 부정은 사실상 어려운 것이 사실이다. 문제는 합리성의 논리가 원래의 의도와는 다른 방향으로 전환되도록 만드는 권력의 문제로 볼 수 있으며, 우리가 정보기술과 권

력의 문제를 주목해야 하는 이유는 여기에 있다.

오늘날의 정보감시기술은 단순히 한두 가지 기술적 요소들에 국한되지 않는 시스템의 영역으로 확장되고 있다. 민주적 통제나 인권적 관심이 결여된 기술 시스템은 권력에 대해 영혼을 상실한 기술적 합리성의 지배를 허용할 위험성이 매우 높다. 감시 시스템이 프라이버시와 인권의 영역까지 확장되는 상황에서 인권적 차원의 접근이 본격화되어야 하는 이유는 여기에 있다.

## 3. 전자감시의 확장과 노동인권

### 1) 감시기술의 확장

전자감시가 작업장에 미치는 영향은 그 영역과 정도에 따라 다양한 차원으로 접근할 수 있다. 전자감시의 영향은 '작업장 내 시·공간'과 '작업장 외 시·공간'의 두 영역으로 나누어 볼 수 있을 것이다. 여기에서 작업장 내에서의 시·공간은 일상적 작업의 시간과 공간이라는 범주를 의미하며, 작업장 외 시·공간은 작업의 시간과 공간의 범주를 넘어서 일상생활이 이루어지는 시·공간의 범위를 포함할 수 있다.

사업장 감시는 또한 그 밀도에 따라 상단한 편차를 보일 수 있다. 공장, 작업현장, 사무실 등 일하는 공간을 의미하는 작업장은 전자감시가 가장 조밀하게 이루어지는 영역으로 볼 수 있다. 이 영역에서는 노동자들의 모든 신체 및 정신적 행위가 감시와 통제의 대상이 된다. 작업장 통제의 거의 대부분은 고용주와 노동자 간에 이루어지는 '노동 계약'에 의해 합법적으로 이루어지는 것으로 가정된다. 고용주는 노동계약을 근거로 노동자들의 정신과 육체적 활동 전반에 걸쳐 합법적으로 감시하고, 통제하며, 자료를 수집한다. 고용계약을 통해 고용주와 주어진 시간 동안 노동력 판매에 동의한 노동자들은 작업장통제의 기제 속에서 움직일 수 밖에 없다.

작업장에서 전자정보기술의 도입은 작업장의 노동시간에 존재하는 '틈새'(porosity) 영역들을 체계적으로 제거하고 노동과정에 대한 통제를 보다 촘촘히 엮는 데 결정적으로 기여한다. 노동과정에서 정보기술의 도입은 단순히 작업의 상황에 대한 관찰과 기록이라는 소극적 감시의 차원에 국한되지 않는다. 정보 시스템의 활동은 노동과정에 대한 적극적인 정보 수집을 통해 노동자들이 보유한 다양한 형태의 지식과 정보를 감시 노동자들의 몸으로부터 정보 시스템으로 체계적으로 이전시키는 '정보 회로'의 역할을 수행할 수 있다. 노동자들이 보유하는 기록되지 않는 '암묵지'(tacit knowledge)는 조직 과정을 통해 끊임없이 노출되며, 노출된 정보는 표준화 된 데이터베이스 시스템의 기계적 처리 과정을 거쳐 정보 시스템에 내장된다. 이렇게 내장된 정보는 노동과정을 보다 효과적으로 조직하는 유용한 자료로 활용되며, 이 과정은 노동과정 전반을 통해 끊임없이 반복되면서 진화한다.

조직의 규모와 분화 정도가 초보적이고 통제 기술이 발전되지 않았던 상황에서 조직의 통제는 고용주나 그를 대리하는 관리자와 노동자 간에 이루어지는 직접적, 인격적 통제가 주로 이루어지지만, 조직의 규모가 성장하고 복잡성이 증가하면서 인격적 통제는 한계에 도달한다. 이 단계에 이르면 통제는 복잡한 절차와 규칙이 중시되는 '관료적 통제'에 의존하는 상황을 맞이한다. 오늘날 현대적 조직의 통제는 이제 관료적 통제에 더하여 정보기술의 광범위한 도입과 더불어 관료제와 정보감시기술이 결합되는 '시스템적 통제'의 수준으로 발달한다. 시스템적 통제가 관료적 통제와 구분되는 것은 이것이 고도의 정보기술 네트워크와 불가분의 관련성을 맺고 있는 것이다.

시스템적 통제의 네트워크는 수많은 정보수집 센서들, 모니터 장치들, 프로세스 통제 소프트웨어 등이 네트워크로 연결되어 언제 어디서나 노동자들의 행동을 시간적 순서에 따라 정밀하게 모니터하고, 평가하는 자료를 생산하고, 이를 가공하여 조직 관리 정보로 전환시킨다. 관리 조직과 고용주는 이렇게 생산된 자료에 독점적으로 접근하여, 이를 가공하고 조직의 목적을 위해 활용할 수 있는 권한을 보유한다. 반면 노동자들은 자신에 대한 정보가 어떠한 방식으로 수집, 가공, 활용되는지에 대해 제대로 알 수 없으며, 극히 일부의 내용을 제외하면 자신을 포함한

타인의 정보에 대해 접근할 수도 알 수도 없다. 정보의 불균형 상황이 전개되는 것이다.

노동자와 관리자 사이의 정보 비대칭은 권력의 비대칭성을 전제로 한다. 권력의 비대칭성이 심화될수록 정보의 비대칭성도 증가할 가능성이 높으며, 그 역방향의 피드백 고리도 동시에 작동한다. 노동자들에 관한 정보가 독점적으로 활용되고, 일상적 감시의 폭과 밀도가 증가하게 될 수록 권력의 불균형이 심화되는 것이다. 정보감시기술은 정보의 극단적 비대칭성에 가속페달을 제공한다. 노동자들은 작업장의 모든 과정에서 감시 시스템의 영향을 벗어나기 힘들어지고, 이렇게 확대되는 일상적 감시는 인간의 정신과 육체 활동 전반을 시스템의 감시 하에 위치시키게 되는 것이다.

노동자들의 일거수 일투족이 정보시스템의 관리 하에 놓여감에 따라 시스템의 통제를 받는 노동자들은 육체적, 정신적 압박 하에서 노동생활을 수행할 수밖에 없는 상황에 처하게 된다. 공장제 자본주의 생산체제 하에서 작업장의 감시는 특정한 물리적 공간에 한정되어 있었다. 작업장의 시간 및 공간적 범위가 특정한 장소에 한정되지 않는 노동자들은 작업장의 통제로부터 상대적으로 자유로울 수 있었다. 그러나 이러한 상황은 정보감시기술의 외연이 확장되면서 크게 변화하였다. 정보감시기술은 특정한 작업 공간을 넘어서는 광범위한 시간 및 공간적 범위에 걸친 모니터링이 가능한 기술적 수단을 제공하였고, 이제 감시시스템의 범위는 특정한 작업장의 한정된 영역을 넘어서 삶의 모든 이동 공간, 심지어 개인적 삶의 영역까지 거침없이 확장될 수 있게 된 것이다. 시스템의 확장과 더불어 노동자들은 훨씬 더 빈 틈 없이 촘촘하게 짜인 통제의 망 속에서 육체적, 정신적 스트레스를 받지 않을 수 없는 상황에 처하게 된 것이다.

### 2) 감시기술과 노동인권

전자감시 시스템에 의해 통제되는 노동자들은 이에 대한 효과적인 법제도적 보호 수단이 없는 한 시스템의 통제로부터 그들의 자유와 인권을 지키기 힘들어

지게 된다. 모든 노동 과정이 시스템에 의해 완벽히 통제될 때 노동자들은 '투명 감시'의 상황에 직면한다. 그러나 이 투명감시는 권력의 입장만을 반영하는 것일 뿐, 감시의 대상인 노동자들의 입장에서는 보이지 않는 적의 통제 하에서 완전히 노출된 삶의 스트레스를 감내해야 한다는 것을 의미할 뿐이다.

노동감시 시스템의 영역이 대폭적으로 확장되어 인권과 프라이버시의 침해 가능성이 크게 증가했음에도 노동자들은 이에 대해 별다른 대응 수단을 확보하지 못하고 있다. 특히 작업장의 감시가 단순한 정보 수집의 영역을 넘어 수집된 정보의 가공과, 동의 없는 활용으로 나아갈 때 그것이 미치는 영향은 엄청나게 클 수 있음에도 불구하고 현재까지 이러한 문제들에 대해 사회적, 법제적 차원의 대응 노력은 거의 불모에 가까울 정도로 취약했던 것이 사실이다.

작업장의 어디에서나 존재할 수 있고, 감시의 목적으로 활용될 수 있는 기술적 수단에 대해 노동인권 차원에서 합리적 평가나, 잠재적 감시 대상인 노동자들의 적절한 참여, 혹은 동의 절차가 마련되지 못할 경우 사업장의 감시는 노동인권을 심각하게 침해할 가능성을 충분히 내장하고 있다. 사업장의 권력관계가 극단적인 비대칭의 상황은 정보기술을 감시기술로 전환시킬 유혹을 더욱 증폭시킨다. 정보기술이 감시기술로 활용되는 것은 인간의 의지의 문제일 뿐 더 이상 기술적 가능성의 문제가 아닌 상황이 되었기 때문이다. 감시 기술의 인권 침해 가능성에 대한 명확한 법제도적 규제가 미비한 상황에서 정보감시기술이 노동인권을 침해하는 사례들이 계속 증가할 수 있을 뿐 아니라 새로운 형태의 정보감시기술들이 끊임없이 개발될 수 있다는 것을 시사하고 있다.

사업장 감시기술의 발달이 급진전되는 상황과는 달리 이 문제에 대한 사회적, 법제도적 대응은 답답할 정도로 진전이 이루어지지 않고 있다. 선진국들의 경우 이미 20여 년 전부터 사업장 감시 실태에 대한 체계적인 조사에 기초하여 이에 대한 윤리적, 인권적, 법제적 차원의 대응 방안들을 구체적으로 모색해 왔으나, 우리의 경우에는 이제 막 사건화 된 사례나 조사들을 중심으로 문제제기 차원의 초보적 대응 수준에 머물고 있다. 기술에 대한 시민의 참여와 사회적 평가가 제대로 이루어지지 못할 경우 기술이 권력과 자본에 의한 통제의 수단으로 전락하는 사례들은 얼마든지 찾아볼 수 있다.

전자감시에 대한 사회적 규제의 수단이 제대로 마련되지 않을 경우 관리자들은 그들이 합법적으로 보유한 '감시권'(monitoring right)을 얼마든지 확장할 수 있다. 게다가 작업장에서 이루어지는 감시의 대부분은 합법적 경영권의 일부로 간주될 수 있는 여지가 매우 크기 때문에 전자감시에 대한 노동자들의 저항이 법의 보호를 받을 수 있는 가능성은 매우 낮으며, 개인의 프라이버시가 중시되는 외국의 경우에도 명확한 기준이 설정되지 못할 경우 경영권에 대응하여 프라이버시를 보호하는 것은 쉬운 일이 아닌 것으로 드러나고 있다.

감시기술에 대한 윤리·사회적, 법제적 대응 수단이 마련되지 않은 상황에서 급속히 발전하는 전자감시기술은 고용주의 감시권을 효과적으로 실현하는 신무기를 제공하는 것에 다름 아닌 것이다. 통제되지 않은 감시기술은 권력의 힘을 강화하고, 이를 더욱 위험한 물건으로 키우는 결과를 초래하게 될 것이다.

정보감시기술의 확장으로 인한 프라이버시와 노동인권 침해는 많은 작업장에서 노동자들의 저항을 불러일으키고 있으며, 이미 국내외의 많은 사업장들에서 이러한 문제들이 중요한 노동현안의 영역으로 들어와 있다. 문제는 프라이버시가 중시되는 외국의 경우에도 사업장 감시에 대응하여 프라이버시와 인권을 보호하기 위한 명확한 기준의 마련이 결코 쉬운 일이 아니라는 데 있다. 그러나 감시기술의 무차별적 도입에 대한 사회적 차원의 문제 제기가 본격적으로 이루어지지 못할 경우 작업장의 노동인권과 프라이버시는 더 이상 보호받지 못하는 상황에 이를 가능성이 높다. 감시기술에 대한 노동인권적 차원의 문제의식이 사회적으로 조직화되고, 이에 대한 복합적 차원의 사회적 대응 방안이 모색되어야 할 필요성은 감시기술의 급속한 발전과 더불어 더욱 절실한 과제로 등장하고 있는 것이다.

## 4. 연구의 내용과 방법

한국 사회의 경우 90년대 이후 다른 어느 나라 보다 빠른 속도로 발전, 확산된 정보통신기술이 생활의 편리와 생산성의 향상을 가져왔지만, 그 부작용도 꾸준

히 지적되어 왔다. 특히 정보통신 기술이 사업주에 의해 CCTV나 이메일 체킹 등의 방법으로 노동자 감시 및 통제의 수단으로 이용되면서 이에 대한 우려와 반발도 높아지고 있는 상황이다.

그러나 사업장 내외의 감시 시스템이 노동인권과 노동자의 건강권에 미치는 영향을 조사·평가하는 작업은 아직 미진하며, 그 부작용을 방지할 법제도적 장치도 미비하여 사용자는 감시 시스템을 남용하는 상황이다. 또한 노동법의 조항과 단체협약을 통해 감시시스템의 설치와 운용을 부분적으로 제어할 수 있음에도 이에 대한 인식은 사용자와 노동자 양자에게서 모두 낮은 형편이다.

국내 사업장의 감시 시스템 실태 파악에 기반하여 이의 문제점을 실질적으로 개선하기 위하여 노동관련 인권보호 정책 및 법제 개선 방안을 마련하는 작업이 시급한 때이다.

이와 관련한 선행연구를 간단히 살펴보면, 1990년대 말부터 전자 감시와 노동통제에 관한 이론적 논의가 시작되었으며 노동운동 진영에서 수 차례의 토론회를 개최하여 호응을 얻었다. 특히 민주노총, 진보네트워크센터 등이 함께 구성한 '노동자감시근절을 위한 연대모임'은 사업장 감시 시스템과 관련하여 발생한 분쟁을 중심으로 일련의 현장 연구를 진행하였고, 이 연구팀에서 2002년에 주최한 "첨단기술에 의한 노동자감시, 어떻게 대응할 것인가" 토론회와 일련의 발간 보고서가 주목 받았다.

2005년 경실련 노동위원회에서 이병훈 등이 연구를 진행하여 펴낸 "전자 노동감시의 실태와 개선과제"는 가장 최근의 작업이며, 국내의 실태뿐 아니라 해외의 사업장 감시시스템 사례와 이에 기준과 입법례를 수록하고 있다.

그 동안의 연구들로 인해 사업장 감시시스템이 갖는 문제점에 대한 인식이 상당히 제고되었고, 일반 언론에서도 관심을 갖고 다루게 되었다. 2000년 이후 노동과정의 고도화와 일망통제 감시망은 더욱 급속히 보편화되었지만, 이를 노동자의 기본적 인권 침해라는 시각에서 조망하고 논의를 전개하는 작업은 현실을 따르지 못하고 있다. 노동계와 정치권에서도 이러한 상황에 주목하고 문제점을 최소화할 수 있는 입법을 논의하고 있는 즈음, 국내 사업장 감시 시스템의 전반적인 실태를 분석하고 노동권을 보호할 수 있는 구체적 대안을 마련하기 위한 연구가

절실한 시점이다.

특히, 2000년 이후 새로 도입된 다양한 기술 방식의 감시시스템의 현황, 그것이 노동자의 신체와 심리 및 조직 활동에 미치는 영향, 외국의 유사 사례와 법제도를 분석하는 연구는 향후 연구에서 반드시 채워져야 할 부분이라 할 것이다.

본 연구는 우선 문헌을 통해 사업장 감시시스템에 관한 기존 연구 및 실태조사 결과를 정리하고, 새로운 기술과 감시 방식의 도입이나 분쟁의 발생으로 인해 연구가 필요한 영역이나 사례를 문헌과 현장조사 및 설문조사로 보완하는 방식으로 진행되었다.

2장에서는 노동자 전자감시의 개념을 정의하고 감시 기술 및 활용의 현황과 효과를 개괄한다. 감시시스템에 사용되는 기술과 영역, 목적에 따라 현재 이용되고 있는 감시시스템의 세부 현황을 파악하고, 그 효과 또는 역효과의 생산성 증진, 보안 강화, 통제 강화 등의 측면에서 살펴본다.

3장은 사업장 실태조사로, 먼저 실지조사는 감시시스템이 채용되어 있는 사업장 중 직종 및 업종별 대표 사업장을 방문하여 시스템 담당자 및 노동자 대표와 면접을 실시하고 관련 자료를 획득하여 사례를 정리한다. 4장에서는 감시시스템이 채용되어 있는 사업장의 노동자를 대상으로 우편설문조사를 실시하여 감시시스템의 인지도 및 영향, 감시 시스템에 대한 의견을 파악한다.

5장에서 감시시스템 관련 외국 사례와 국제 기준 및 입법례 분석을 위해 외국의 감시시스템 조사사례를 정리하고, 이에 관한 논쟁 및 판례 등을 수집한다. 이를 기반으로 감시시스템의 채용과 운용에 관한 국제기준과 각국의 관련 이행 입법례를 비교 분석한다.

6장에서는 이를 바탕으로 국내 법제, 정책의 문제점을 분석하고 개선방안을 제시한다. 헌법, 노동조합 및 노동쟁의조정법, 정보통신망이용촉진및정보보호에관한법률이 사업장 감시시스템의 운용에 개입할 여지가 제한적임을 분석하고, 이를 기존 법률의 개선 및 새로운 법률의 제정, 단체협약 상의 개선을 통해 해결할 수 있는 방안을 도출하고자 하였다.

결론적으로 7장에서 감시시스템의 남용을 막고, 노동자의 기본적 인권을 보장하면서 부작용을 최소화하기 위해 정부, 사업주, 노동자가 해야 할 노력을 제시하

고자 한다.

본 연구의 주안점은 다음과 같다. 첫째, 기존 연구 성과 위에 변화된 감시환경(인터넷 원격감시 등)을 포함시킨다. 둘째, 감시시스템과 관련한 노동인권, 건강권 개념과 기준을 정리하고 일정한 가이드라인을 제시하는 것을 주된 목적으로 한다. 셋째, 감시와 분쟁 사례의 나열만이 아니라 감시의 기술적, 정치적 측면을 총괄적으로 재정리할 수 있도록 한다. 넷째, 조사 연구는 실지조사 중심으로 노동현장의 인권 침해 사례를 구체적으로 드러내는 것에 집중하고, 설문조사는 감시시스템의 전반적 확산과 그에 대한 인식 및 대응 정도를 파악하는 것으로 한다. 다섯째, 해외 사례, 입법례 등 최근의 사례를 폭넓게 수집하여 실효성 있는 제언이 나올 수 있도록 한다. 여섯째, 법제도, 정책 및 행정 측면의 개선방안에 더하여 (시민사회 차원의) 규범 및 사회문화적 액션 필요성을 도출하도록 한다.

# 2장. 사업장 감시시스템의 일반적 현황

## 1. 전자 노동감시의 개념

자본주의적 생산체제에 있어 노동력의 거래를 둘러싼 노동자와 자본가(또는 사용자)간의 상호관계는 '각축적 교환관계(contested exchange)'로 성격지어지고 있다. 따라서 사용자는 생산과정에 있어 잉여노동의 극대화를 위해서 뿐 아니라, 노동자들의 집단적인 저항을 억제하기 위해 노동통제의 수단을 적극적으로 도입·활용하게 된다.

과거 산업화시대에 있어 작업현장에서의 감독·감시는 주로 관리자 또는 현장감독자(supervisor)들에 의해 가시적인 방식으로 수행되었던 반면, 정보통신기술의 발전을 통해 작업현장에 '전자 노동감시(electronic labor surveillance)'가 새롭게 등장·확산되고 있다. 전자 노동감시에 대해서는 선행 연구에 의해 다양한 개념정의가 다음과 같이 제시되고 있다. 주요한 것들을 추려보면 다음과 같다.

- "노동자들의 생산활동 및 직장 내의 생활에 관한 정보를 컴퓨터 등의 정보통신기술을 활용하여 수집·저장·분석·기록하는 행위" (권순원, 1998)

- "정보통신장비를 이용하여 노동자의 근로휴게시간, 퇴근후 일상생활에서의 모든 행위를 사전 동의나 합의 없이 개인이나 집단의 정보를 취득·송신·수신·저장·관리·가공·자원화하여 인간의 존엄성, 사상·행동·신체·양심의 자유를 억압하는 행위" (김세곤, 2003)

- "노동자의 행동과 의식, 태도와 직무성과 등이 디지털신호체계로 포착

되어 정리·분류·비교·평가되는 일련의 감독체제" (김영권, 2004)

요컨대, 전자 노동감시란 "사용자의 재산권 보호과 노동력 통제력 강화를 위해 정보통신기술에 의존하여 작업장 안팎에서 노동자들의 작업활동, 생활태도 그리고 의식성향에 대한 음성·영상·(컴퓨터)데이터정보를 취득·수집·전송·저장·가공·분석하는 일체의 사용자 행위"를 지칭하는 것으로 정의할 수 있다.(이병훈, 2004)

그런데 전자 노동감시는 단지 노동 통제에 전자적 장치를 덧붙인 것만이 아니라는 점에 유의해야 한다. 기존 노동 통제가 신체상의 소극적, 가시적 제약이었다면, 전자 노동감시는 정보통신기술의 이용을 통해 노동/직무 정보 제공-활용함으로써 업무수행에 대한 능동적 통제를 가능케 한다는 점에서 큰 차이가 있다.

<표 2-1> 노동 통제방식의 비교

| 전통적 통제 | 전자감시통제 |
|---|---|
| - 제한적 근접감시-인격적 통제 | - 고밀도감시-간접통제 |
| - 현장관리/감독자 중심의 통제행위 | - 경영자의 통제행위 가능 |
| - 주관적 통제 | - 객관적 통제: 비교평가 용이 |
| - 가시적 통제 | - 비가시적 통제 (Panopticon 효과) |
| - 제한적 공간대상 | - 일상생활 포함의 감시대상 광범위 |

* 이병훈, 2004

한편 기존 연구문헌에서는 노동자들에 대한 사용자의 감시행위의 영문 표기로 'monitoring'과 'surveillance'가 혼재되어 사용되고 있다, ILO(1993)는 monitoring을 직무수행 및 결과에 대한 협의의 감시로 정의한 한편, surveillance를 작업장 내에 노동자들의 전반적 근로활동 및 직장생활에 대한 포괄적인 감시활동으로 대비하고 있다. 또한, 이 ILO보고서에는 감시행위의 공개성 여부에 따라

공개적인 감시활동에 대해 monitoring의 개념을 사용하고, 비밀스런 감시활동에 대해서는 surveillance의 표현을 적용하기도 한다.

## 2. 노동자 전자감시의 유형

노동자 전자감시는 감시의 목적, 감시의 대상, 감시의 수단과 같은 기준에 따라 몇 가지 유형으로 분류해 볼 수 있다. 본 연구에서도 이러한 유형에 따라 사례를 살펴보도록 할 것이다.

### (1) 감시의 목적 (Why)

전자 노동감시를 시행하게 된 사용자들의 의도하는 목적은 다음의 7가지 측면에서 정리될 수 있다: ① 업무생산성을 제고하기 위한 작업공정의 통제 강화, ② 생산설비 및 자재의 도난방지와 기업정보의 유출방지, ③ 사업장내 안전사고의 사전 예방과 사후 신속대처, ④ 기업내 컴퓨터시스템 및 생산설비에 대한 개인적 유용 방지 및 장애발생 행위 차단, ⑤ 노동자의 개인적 또는 집단적 반기업활동 및 불법행위 (조직규율 위반행동)에 대한 규제, ⑥ 업무성과의 객관적 측정 및 보상연계, ⑦ 대고객 서비스 품질 개선. 이같은 전자감시의 다양한 추구 목적을 간추리면 사용자의 재산권 보호 및 노동인력에 대한 통제력 강화로 요약될 수 있을 것이다.

### (2) 감시의 대상 (What)

전자 노동감시의 대상은 감시영역과 감시대상범주 그리고 구체적인 대상물로 나누어 살펴볼 수 있다. 감시영역은 주로 작업현장 및 주변 사업장 부대공간이 되겠지만, 노조활동과 관련하여 작업일과 이후 노동자들의 활동 및 생활공간에 대해

감시활동이 전개될 수 있다. 감시대상범주로는 노동자들의 작업활동 및 그 직무성과, 직무태도 및 생활방식 그리고 의식성향과 가치관 등이 포괄될 수 있을 것이다. 끝으로, 감시대상물로는 노동자들로부터 의식적으로 수집될 수 있는 음성, 영상, (컴퓨터) 데이터 정보들이 모두 포함될 수 있는 바, 구체적인 예로는 전화통화기록, 음성녹취록, E-mail 메시지, 컴퓨터파일, 폐쇄회로 감시영상, 인터넷접속기록, 근태 및 생산활동관리 컴퓨터데이터, 그리고 위성위치추적 데이터 등을 열거할 수 있을 것이다.

### (3) 감시의 수단 (How)

전자 노동감시는 개념 정의에서 공통적으로 지적하듯이 정보통신기술이 핵심수단으로 활용되고 있다. 조돈문(1996)은 전자감시기술을 크게 3개 요소로 구성하고 있는 것으로 논의하는 바, 그 첫째로 관찰·감시자의 노출 없이 감시대상의 개인정보를 다량 수집할 수 있는 기술 요소, 둘째로는 통신네트워크를 통해 정보전송을 통해 공간을 초월한 정보 공유를 가능케 하는 기술 요소, 셋째로 분산된 개인신상정보를 연결-통합하여 관리하는 체계적인 DB을 구축할 수 있는 기술요소가 이에 해당된다. 이러한 기술요소들이 투영된 현실적인 전자감시기제로는 폐쇄회로(Closed Circuit, CC)TV, 전자ID카드, RF카드, Active Badge, 인터넷 및 이메일 이용통제 관리시스템, 전화 및 특정 공간의 감청설비, 전화모니터링시스템, 위성위치추적장치(Global Positioning System, GPS), 생체인식기(예: 정맥, 지문, 홍체, 얼굴, 음성, 서명, 유전자감식), 그리고 생산라인관리시스템(예: Data Acquisition System, Enterprise Resource Planning) 등을 꼽을 수 있다.

그 외에 감시 방식에 따른 유형 분류로 ▲시청, 도청 통한 행동 통제 (판옵티콘 효과), ▲(기업주나 생산성에 반하는) 증거물 수집, ▲종업원 및 장비, 부품의 경로, 위치, 출납, 수량 파악, ▲(노조 등) 노동자 조직 활동 방해, ▲특정인에 대한 미행 및 감시 등으로 나눌 수 있다.

<표 2-2> 전자 노동감시의 유형별 분류

| 분류 기준 | 주요 내용 |
|---|---|
| 목적에 따른 유형 | - 작업조직 통제 강화 => 직무생산성 제고<br>- 기업/조직 정보유출 차단 및 기업재산 보호 (도난사고 방지)<br>- 작업장내 사고/산재 발생 예방<br>- ICT 설비의 사적 이용 방지<br>- 해적판 S/W와 바이러스 및 시스템 기능 저하 억제/차단<br>- 개별/집단적 저항행위 및 불법행위 규제<br>- 모니터링-보상/고객서비스/규칙준수/안전 연계 |
| 사용 기술에 따른 유형 | - CCTV (폐쇄회로 TV) 및 몰래카메라<br>- 전자신분증, 바코드, RFid, 액티브 배지<br>- GPS (핸드폰, 택시 등) 위치추적<br>- 인터넷 이메일, 메신저, 하드드라이브 체킹<br>- 도감청<br>- 전화 통화 모니터링 (콜센터)<br>- 인터넷 사이트 접속 차단<br>- ERP<br>- DAS<br>- 생체인식 |
| 감시 대상에 따른 유형 | - 노동자 (전체/타겟)<br>- 작업과정 (작업장 내외부)<br>- 부품 및 장비<br>- 생산물, 실적 |

# 3. 감시시스템 기술과 현황

## 1) 국내의 기술 동향

현재 국내에서 사용되고 있는 주요 감시시스템을 기술별로 살펴보면 영상시스템(CCTV 몰래카메라), 위치추적시스템(GPS, 핸드폰 위치추적 등), 전자카드(IC칩 카드, 액티브 배지), 생체인식기 등이 있으며, 최근에는 업무용 개인 컴퓨터,

전화 등에 대한 무단 열람, 도감청도 증가하고 있고, 생산자동화 시스템(ERP, DAS 등)도 노동자 감시 시스템으로 활용되고 있다. 그 중 대표적인 기술들의 현황과 변화 추세를 일별해 보면 다음과 같다.

### (1) CCTV

전자 노동감시에서 가장 대표적으로, 폭넓게 이용되고 있는 것이 폐쇄회로 카메라(CCTV)이며 그에 따른 분쟁 사례도 가장 많은 편이다.

CCTV는 단순 촬영, 녹화에서 통합 출입관리 시스템으로 이동하고 있는 추세이다. 또한 기록 장치도 아날로그 테이프에서 DVR(Digital Video Recorder)로 변화하고 있다. DVR의 경우 테이프를 바꾸어 끼울 필요도 없고 방대한 용량 녹화가 가능하며, 자유로이 편집하여 활용할 수 있기 때문에 더욱 선호도가 높다.

<표 2-3> 아날로그 녹화방식과 디지털 녹화방식의 비교

| | 아날로그 방식 | 디지털 방식 |
|---|---|---|
| 녹화방식 | 아날로그 화상 | 디지털 고해상도 화상 |
| 저장매체 | VTR 테이프 (수시 교체) | HDD, DAT, MOD, DVD |
| 자장매체 사용시간 | 3-5회 사용 후 폐기 | 반영구적 |
| 재생시 검색방법 | 계속 재생 (리니어) | 특정시간 지정, 즉시 재생 (넌리니어) |
| 감시범위 | 근거리 | 근거리 및 원격감시 |
| 녹화방식 | 계속 녹화 | 움직임 감지 녹화, 연속녹화, 센서 연동 녹화 등 |
| 재생 화질 | 저화질 (반복 재생시 화질 급격히 저하됨) | 고화질 (반복 재생에도 화질 저하 거의 없음) |
| 편집기능 | 확대기능 없음 | 특정화면 프린터 출력 및 영상 확대 |
| 화면 전송기능 | 없음 | 가능 |
| 유지관리 | 테이프 교체 및 보관 직[illegible] | 24시간 관리 불필요 |

* 전자부품연구원, 디지털 영상 감시 및 녹화장비

컬러 CCTV 카메라 4대에 모니터 1대, DVR 1대 정도의 기본 시스템의 경우 200여 만원으로 구축이 가능하고 임대로 할 때 월 10만원 이내에서 이용할 수 있으므로, 관리자 측이 저렴한 비용으로 감시 효과를 거둘 수 있다는 점 역시 이용도를 높이고 있다.

### (2) RFiD 카드

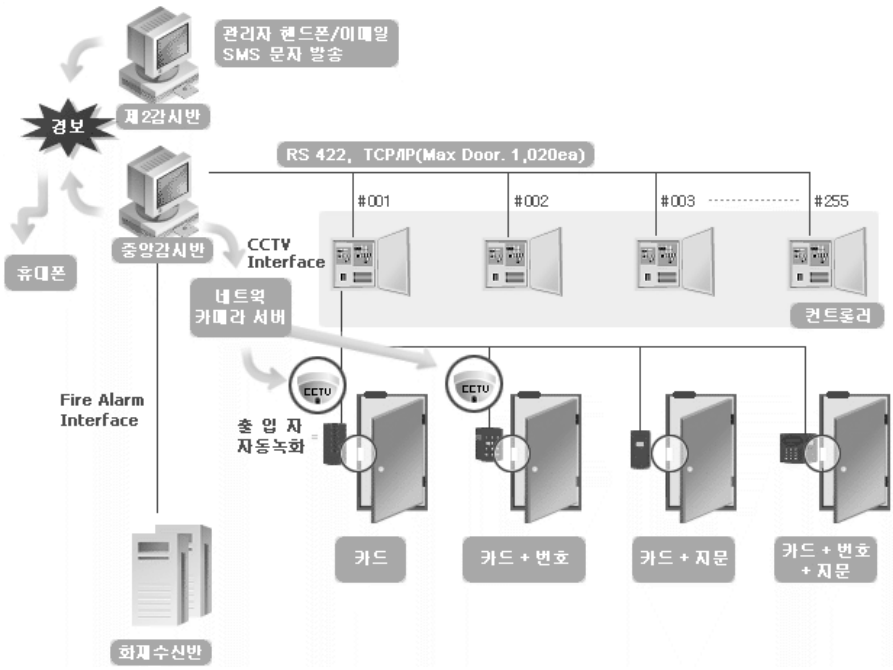
단순한 출입 카드를 넘어, 개인의 신상정보를 내장한 RF(Remote frequency) ID 카드는 다기능 학생증 / 교통카드, 유통업계(RFID), 출입통제 / 근태관리 / 식수관리 시스템 등으로 갈수록 그 사용 범위를 넓혀가고 있다. RF의 주파수 대역으로는 125 KHz, 13.56 MHz, 311 MHz, 2.45 GHz 등이 많이 사용되는데, 그 성능과 이용범위는 아래의 <표>와 같다.

ID카드는 그 사양에 따라 다양한 시스템이 구축된다. 가장 단순한 독립형 시스템의 경우 최저가형으로 단순히 출입통제의 목적으로만 사용하며, 제품에 따라 비밀번호 혹은 카드를 이용하여 출입할 수 있다. 가장 단순한 것도 기본 128개의 각기 다른 비밀번호 또는 카드를 사용할 수 있으며, 확장 시 512개까지 사용할 수 있다. RS-232C 통신 Port를 이용하여 Computer에 연결 사용할 수도 있다.

<표 2-4> RF의 성능과 이용범위

| 13.56 MHz | 2.45GHz |
|---|---|
| 1. 1Kbyte Read/Write, 비접촉식<br>2. 한장의 카드에 다양한 어플리케이션(신분증,신용카드,교통카드,출입통제..) 수용<br>3. 최대 10cm 인식거리<br>4. 기존의 바코드 시스템을 대체함<br>5. 다양한 모양의 카드와 태그 제공<br>6. 영구적 사용<br>7. 고도의 보안 알고리즘 내장 | 1. 인식거리 : 5~10M<br>2. 외부환경에 영향을 거의 받지않음<br>3. 움직이는 태그 인식가능(동적인식)<br>4. 강력한 Error 감지 |

<그림 2-1> 통합 감시시스템의 운용




* 출처: http://kor.idteck.com/product/

중대규모 시스템의 경우 분산 제어 방식으로서 출입자의 출입 레벨을 정하여 출입지역, 출입시간 등을 설정하여 운영할 수 있으며, 각종 시스템에 연계 사용할 수 있고 (센서, 화재, CCTV 등등) 각 출입문의 원격제어 및 출입자의 모든 현황을 중앙에서 감시할 수 있도록 설계되기도 한다.

RFiD와 CCTV 등 감시 시스템은 더욱 통합되어 유기적으로 활용되고 있는 추세다. 위의 <그림>은 한 감시시스템 업체가 자신의 상품을 소개하는 내용으로, CCTV와 출입카드를 통합하여 운영하는 메커니즘과 구조를 잘 알 수 있다.

### (3) ERP

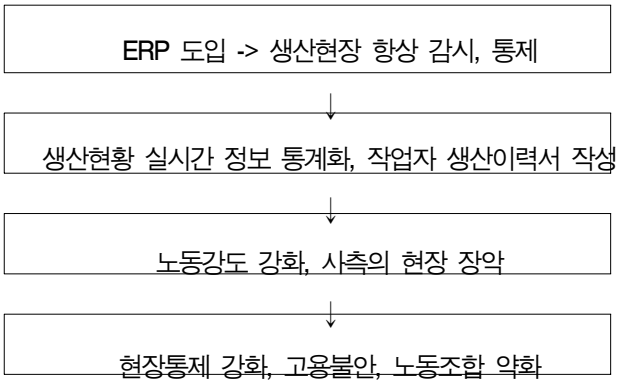
ERP는 전사적 자원관리(Enterprise Resource Planning)의 약자로, 기업활동을 위해 쓰이는 기업 내의 모든 인적, 물적 자원을 효율적으로 관리하여 궁극적으로 기업경쟁력을 강화시켜주는 역할을 하게 되는 통합정보시스템(고기능성 기업용 소프트웨어)을 말한다.

ERP 시스템 도입의 주된 목적은 다음과 같다. 영업, 생산, 구매, 자재, 회계, 인사 등 회사 내 모든 업무를 IT 자원을 활용하여 동시에 통합 처리되고 정보를 실시간으로 주고받을 수 있으며 비즈니스 프로세스(Business Process: 업무절차) 역시 ERP가 선진 프로세스를 내장하고 있기 때문에 기업체들은 별도의 첨단경영기법이나 경영컨설팅 또는 BPR(Business Process Re-engineering: 업무흐름 재설계)을 하지 않고도 ERP 도입을 통해 자동적으로 경영혁신이 되는 효과가 있다. 따라서 급변하는 경영환경 변화와 정보기술의 발전에 필사적으로 대응하려는 경영자들의 고민을 해결시켜주는 최상의 솔루션이라 일컬어진다.

이러한 ERP가 노동자 전자감시 시스템으로 이해되고 우려를 자아내는 이유는 다음과 같다. 제조업의 경우 정확한 판매예측에 입각한 수요계획이 생산작업계획과 오차 없이 연동되기 위해서는 재고가 없어야 하며 또는 적정재고 수준이어야 한다. 따라서 이전보다 ① 생산계획 수립이 시장변화에 더욱 민감해지면서 ② 생산작업계획에 따른 인원, 설비가동력 등이 철저히 계산되고 표준화된다. 그렇기 때문에 ③ 모델별, 공정별 투입공수를 고려한 공정관리가 더욱 강화되고, ④ 공정관리는 품질관리와 직접적으로 연동되어 실시간 품질정보를 코드화하여 품질증명, 품질실명 따위의 것들을 정착시키게 된다. 이것은 결국 ⑤ 납기를 100% 충족하는 것으로, 낭비(인원공수, 재고량, 자재 결품율 등)를 최소화하는 것으로 귀결될 것이다.

ERP 시스템 구축 과정에서 모든 불합리한 요소들을 배제한다면(ERP 도입 목적 자체가 정보기술시스템에 의한 인적, 물적 자원의 효율적 관리이므로) 자본이 추구하는 생산성은 높아질 것이나, 이는 곧 노동자들에게 그만큼 노동강도가 강화되는 과정으로 현장의 관리통제시스템이 강화되는 것으로 다가온다는 것이다.

<그림 2-2> ERP가 노동에 미치는 영향




### (4) 생체인식

생체인식 기술은 사람의 신체를 신분 식별 수단으로 활용한다. 그 수단에는 유전 정보를 담은 디엔에이(DNA)부터, 얼굴과 홍채, 망막, 지문, 손등혈관, 손금은 물론 귀와 혀까지 다양하다.

가장 정확한 정보는 물론 디엔에이다. 하지만 신원을 그 자리에서 증명하는 데에는 홍채가 빠르고도 정확하다. 홍채 주름의 모양은 생후 18개월쯤 완성된 이후엔 거의 변하지 않으며 지문보다 식별력도 더 뛰어나기 때문이다. 국내에선 홍채인식기에서 1m 가량 떨어진 사람도 식별할 정도의 인식 기술이 개발돼 있다.

3차원 얼굴 인식 기술은 최근 들어 새롭게 주목받고 있다. 사람 얼굴이 비치는 각도와 얼굴 표정이 달라도 같은 사람이라는 것을 인식할 수 있어야 하기 때문에 매우 까다로운 기술로 통한다. 사람의 눈 끝, 입 끝, 콧구멍 등 여러 얼굴 부위의 위치를 좌표로 인식한 뒤에 그 각도와 거리 등을 계산해 사람을 식별하는 방식이다.

하지만 생체 정보는 유출되면 복구가 힘들기 때문에 개인정보들 가운데에서도 가장 중요하고도 민감한 정보다.

생체인식 기술 역시 RFiD나 CCTV와 결합되어 사용되는 경우가 많은데, 기

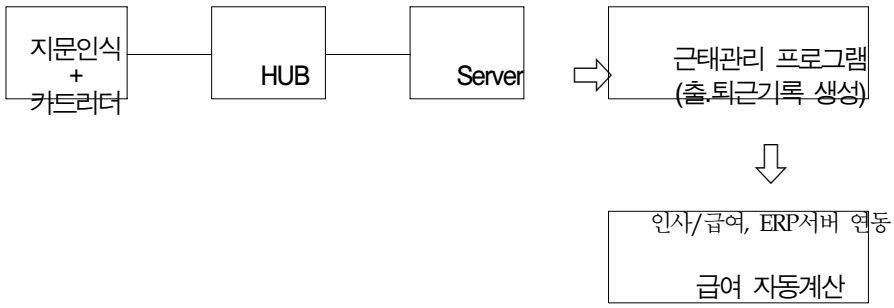
본은 출입통제와 근태관리를 위한 이중기능이다. 국내에 많이 보급되어 있는 지문 인식기의 한 모델(FINGER007/P)을 살펴 보면, 1,000개의 사용자 지문등록/26,000건의 이벤트가 내장(2,000/4,000개의 지문 확장 가능)되어 있고, 독립형 또는 RS232/RS422(최대 32개 연결 가능)를 통한 네트워크 통신도 가능하다. 한 사람이 두개의 지문등록 가능(선택)하며, 지문만을 이용한 자동 인증 기능도 있다.

<표 2-5> 생체인식 기술들의 특징

| 종류 | 특징 |
|---|---|
| 정맥인식 | 손등이나 손목 혈관의 형태를 인식하는 방법으로, 적외선을 혈관에 투시하여 혈관의 형태에 따라 신원을 확인<br>복제가 거의 불가능하여 높은 보안성을 갖지만 하드웨어 구성이 복잡하고 전체 시스템 비용이 많이 들어 활용할 수 있는 범위가 제한 |
| 손바닥 인식 | 사람의 손바닥에 분포되어 있는 손금을 이용하는 것으로 개개인의 손금은 모두 독특한 패턴을 가지고 있다는 점에서 착안 |
| 음성인식 | 사람의 억양과 음의 높낮이가 서로 다르다는 특성에 기인한 방식으로 마이크 등을 통해 전달된 음성의 특징을 분석한 후 가장 근접한 것을 찾아내는 방식<br>다른 생체인식과 달리 멀리 떨어진 곳에서도 전화를 이용하여 신분을 확인할 수 있고, 사용하기 위한 별도의 교육이 필요하지 않으며 시스템 가격이 저렴.<br>감기나 기타 요인에 의해 목이 쉬었을 때나, 의도적으로 타인의 목소리를 흉내내거나 주변환경에 큰 소음이 있을 경우에는 오인식을 할 수 있다는 단점 |
| 얼굴인식 | 기계에 접촉하지 않고 카메라를 입력된 얼굴 형상을 데이터베이스와 비교하는 방식으로 사용자의 표정이 바뀌거나 주위 조명의 영향을 많이 받는다는 단점 |
| 홍채인식 | 사람마다 고유한 특성을 가진 눈동자 바깥의 홍채 패턴을 이용한 것으로 데이터의 정확성, 안정성, 사용 편리성, 처리속도면에서 지문 또는 망막인식에 비해 가장 발전한 보안시스템<br>홍채는 통상 생후 1~2년 내에 고유한 패턴이 형성된 후 평생 변하지 않으며, 어느 정도 떨어진 상태에서 홍채패턴을 인식하는 비접촉 방식으로 거부감이 덜하다는 점 |
| 지문인식 | 진피부분이 손상되지 않는 한 평생 변하지 않는 특성을 갖기 때문에 오래 전부터 보편적으로 사용<br>지문의 융선과 골, 단점 등 지문이미지의 특징점을 파악하여 저장된 원본데이터와 일치하는지를 비교 |

한편 CCTV, RFiD, 생체 인식 등의 감시 시스템은 인사, 급여, ERP 시스템에 자동으로 연계, 반영되게 된다. 아래는 단독사용 근태관리(Stand-Alone Type)의 간단한 개념도이다. 이는 중대규모 기업 내 혹은 지사 간 네트워크로 많지 않은 투자비용으로도 얼마든지 확장될 수 있다.

<그림 2-3> 전자 노동감시 시스템과 인사관리의 연계




### (5) 인터넷 이용 모니터링 및 체킹

노동조합 활동과 관련된 특정한 사이트의 접속을 차단하거나 인터넷 서핑을 아예 못하게 하여 노동자들의 조직 활동을 방해하는 것은 기본적이고도 여전히 이용되는 노동통제 방식 중 하나다. 하지만 여기서 한발 더 나아가서 어지간한 규모의 회사에서 직원들의 인터넷 사용을 감시, 체킹한다는 것은 이미 상당히 알려진 사실이다. 여기에는 인터넷 사이트 서핑 내역은 물론, 이메일로 주고받는 내용, 메신저로 주고받는 내용까지 모두 포함된다. 이는 인터넷으로 전송되는 파일이 패킷(packet)이라는 단위로 나뉘어져 네트워크 전체에 나뉘어져 오고 간다는 인터넷 자체의 특성에서 기인하는 것이다.

이론적으로, 스탠드얼론(stand alone) 컴퓨터가 아니라 네트워크에 접속되어 있는 컴퓨터라면 패킷의 전송 사실은 물론 내용까지 파악이 가능하며, 이러한 기

술을 패킷 스니핑(Packet sniffing)이라 한다. 여기서 스니핑(Sniffing)은 사전적으로는 “코를 킁킁거리다”, “냄새를 맡다”라는 뜻으로, IT적인 의미로는 불법적인 행위를 뜻하는 네트워크 기법 중 하나이다.[1)]

네트워크상에서 스니핑 도구를 설치하면 네트워크상에서 지나다니는 모든 패킷을 포획하여 정보를 추출할 수 있다. 이것은 사용자가 현재 자신이 전달하는 트래픽이 스니핑 당하고 있다는 것을 인지할 수 없기 때문에 문제가 된다. 이러한 기법을 적용한 솔루션이 메일 모니터링(Mail monitoring) 도구다.

직원이 회사에서 사용하는 이메일의 메시지 내용을 스니핑을 통하여 네트워크상에서 가로챌 수 있는 기법이다. 이러한 도구를 합법적으로 사용하기 위해서는 직원들에게 충분한 공지를 통해 현재 스니핑이 진행되고 있음을 충분히 알려야 하지만 그렇게 공식적으로 고지하는 경우는 별로 없다.

물론 오래전부터 많은 회사는 직원들의 이메일 박스와 하드 디스크, 그리고 컴퓨터의 사용에 대해 감시와 제어를 해 왔다. 실제로 이런 프로그램 혹은 서비스를 제공하는 업체는 다수 존재한다. 그러나 그것을 제작하는 회사나 사용하는 회사는 이런 사실을 공식적으로 부정한다. 왜냐면 그것이 현행 법률에도 문제가 되고 분쟁의 소지가 분명함을 잘 알고 있기 때문이다.

하지만 이미 많은 사람들이 이런 프로그램의 존재와 스니핑 프로그램을 이용하여 제작된 수많은 도구를 알고 있다. 스니핑 기술을 이용하면 네트워크의 문제점을 해결하고 애플리케이션의 버그를 잡아 낼 수도 있다. 그러나 악용하면 누군가의 개인정보를 훔쳐내고 감시하는 도구로 사용될 수 있다

실제로 전문업체가 제작하는 스니핑 솔루션 뿐만 아니라 무료 다운로드가 가

1) 패킷 스니핑은 해킹 기술로 알려져 있지만 꼭 그런 것은 아니다. 피싱(Pishing)은 이와 구별된다. 피싱은 개인정보(Private Data)와 낚시(Fishing)의 합성어로, 1996년 American Online(AOL)을 사용하던 10대들이 타 사용자에게 AOL에서 보내는 E-Mail인 것처럼 속여 그들의 계정 정보를 훔치는 것에서 유래된 것으로 악의적인 사용자가 특정 웹 서비스 이용자에게 이메일을 보내 자신의 계좌정보를 확인하도록 하거나, 이벤트 당첨 사은품을 받기 위해서는 계좌정보를 확인해야 한다고 속여 고객의 개인금융정보를 빼내서 범죄에 사용하는 수법으로 다수의 일반인에게 은행이나 유명 쇼핑몰 사이트의 로고 등을 포함한 e-mail을 보내 로고 등을 클릭하면 자신들이 작성한 가짜 웹사이트(은행이나 쇼핑몰처럼 꾸며진 가짜 웹사이트)로 연결이 되도록 하여 고객이 아이디, 패스워드, 계좌번호, 신용카드번호, 주민번호 등을 입력하도록 유도하는 방식으로 신상 정보를 빼내는 기술적인 기법이다.

능한 제품들도 어렵지 않게 구하여 이용할 수 있는 실정이다. 특히 유비쿼터스 환경에서 무선 랜은 패킷 스니핑을 더욱 용이하게 만들고 있다. '에어XXX', '이더XX', '에어XX' 등 무선랜 전용 스니핑 프로그램들은 인터넷 자료실에서 유무료로 누구나 쉽게 다운받을 수 있다.

직원들의 컴퓨터 작업 화면을 그대로 모니터링 하거나, 메신저 대화내용을 체킹하는 프로그램을 그룹 차원에서 설치한 회사들도 많이 있다. 스니핑을 방지하는 툴도 함께 보급되지만, 회사 차원에서 모니터링 툴을 가동할 경우 직원들은 이를 피하기 어렵다.

### (6) GPS

최근 국민의 1/3이 휴대폰을 가지고 있다는 통계가 나온 가운데 정부에서 '위치정보보호 및 이용 등에 관한 법률'을 만들려는 움직임이 분주하다. GPS는 "global positioning system"의 약자로 지구상 모든 곳의 위치정보를 제공하는 장치다. 즉 비행기, 선박, 자동차뿐만 아니라 세계 어느 곳에서든지 인공위성을 이용하여 자신의 위치를 정확히 알 수 있는 시스템이다. 세계적으로 24개의 위성이 지구상 2만200km 지점에서 아주 정확한 시간정보를 지상으로 쏘아준다. 지상에서는 대부분의 지점에서 동시에 4개의 위성을 관찰할 수 있는데, 이들로부터 수신한 시간정보와 지피에스 수신기 내 시간과의 차이를 통해 현재의 지점에서 위성까지의 정확한 거리를 계산하게 된다. 휴대폰 전화기술의 발달로 휴대폰을 이용한 위치추적 프로그램이 더욱 정교해지면서 이용자의 사생활 노출 가능성도 더욱 높아지고 있다. 인공위성기술과 결합하여 위치추적 정확성은 매우 높아질 것이다.

이동 통신 전파환경 측정 시스템(PROMAS)은 자동위치추적 기능을 수행하는 위성위치 확인 시스템(GPS)이 있는데, 이 GPS를 이용하면 지구상공 약2만 km에 위치한 6개 궤도를 회전하는 24개의 인공위성으로부터 전파를 직접 수신하여 지구상의 어떤 위치에도 24시간 실시간으로 정확한 위치, 이동 방향, 속도를 알 수 있다.

이러한 위치추적시스템은 개인이나 사물의 위치를 파악할 경우에는 이를 통해서 그 개인의 활동영역과 활동내역을 파악하거나 추측할 수 있다. 이처럼 개인의 활동영역과 활동내역이 파악되는 경우에는 그 정도에 따라 개인의 행동의 자유와 양심의 자유가 심각하게 침해될 가능성이 있다. 예컨대 이동전화나 PDA 등을 이용하여 위치정보를 파악하는 경우를 들 수 있다. 그리고 기업에서 개인의 위치정보를 영리적으로 활용하기 위하여 개인의 위치정보를 수집·분석하는 경우 노동자의 성향을 파악할 수 있다. 또한 고객서비스의 강화나 서비스 품질의 개선이라는 명목으로 개인의 위치정보가 직장에서 활용될 가능성이 높다. 이 경우 개인의 "위치를 실시간으로 파악"하게 되면 노동자의 인권이 침해될 것이며, 이는 부당한 노동통제와 위치정보를 근무평정에 활용할 경우 노동의 강도가 높아지게 된다. 현재 상당수의 영업용 택시에 부착된 GPS 시스템이나 학습지 교사 노동자나 택배 노동자들에게 지급된 PDA, 휴대폰 등은 유비쿼터스 환경과 결합되어 가장 강력한 노동감시 장치로 이용될 잠재력을 가지고 있다.

### 2) 감시시스템 시장

전자 노동감시 시스템은 불황기의 IT산업에서도 황금알을 낳는 시장으로 자리매김되어 규모를 키워가고 있으며, 정부에서도 이를 적극 지원하고 있는 상황이다. 그러나 시장 활성화에만 관심을 기울일 뿐, 그 사회적, 인권적 측면에 대한 제도적 견제장치 보완은 따라주지 못하여 염려를 낳는다.

CCTV의 국내 시장 규모는 2002년 통계로도 2520억원 대에 이른다. 최근 더욱 각광받는 것은 생체인식 시장이다. 구체적으로 2005년 국내 생체인식 시장은 처음으로 1000억원대를 돌파할 것으로 예상되고 있다. 전자산업진흥회와 한국정보보호진흥원에 따르면 2000년 210억원에 불과했던 국내 생체인식업체들의 매출은 매년 50~100%씩 고성장을 지속해 올해 처음 1000억원대를 넘어설 것이라고 밝혔다.

부문별로는 2004년 현재 지문 인식기술이 시장의 50% 이상을 차지하고 있으

며 얼굴인식(14%), 정맥인식(13%), 홍채인식(10%) 등의 순인 것으로 나타났다. 생체인식 시장은 도어록·출입 통제시스템 등 물리적 접근제어 분야가 가장 큰 수요처로 향후 컴퓨터, 금융권 등으로 빠르게 확산될 것으로 전망됐다.

지난 2000년 말 정부가 생체인식산업을 전략산업으로 집중 육성하겠다는 의지를 표명함에 따라 생체인식 시장은 더욱 주목받고 있다. 현재 생체인식 기술 및 응용제품을 개발하는 업체는 40여개사에 이르나, 독자적인 암호 알고리즘이나 기술을 개발하거나 보유하고 있는 업체수는 적은 편이다. 상용화되어 있는 분야는 지문인식, 음성, 홍채, 정맥인식 등이며, 향후 여러 기술들이 복합적으로 결합되어 있는 다중 생체인식 기술개발이 활발히 이루어질 전망이다. 특히, 스마트카드나 공개키기반구조(PKI) 인증기법의 상호운용을 통한 기술도 개발될 것으로 보인다.

<표 2-6> CCTV 국내 시장규모 (2002년)

| 품목 | 추정금액 (억원) |
|---|---|
| 카메라용 렌즈 | 120 |
| 카메라 | 430 |
| 모니터 | 100 |
| 네트워크 카메라 | 200 |
| 타임랩스 VCR | 140 |
| DVR | 880 |
| 멀티플렉서, 스위치 등 제어기기 | 380 |
| 기타 주변기기 및 액세서리 | 270 |
| 합계 | 2,520 |

### 3) 노동자 감시시스템 보급 현황

노동자감시근절연」 곤임이 2003년 조사, 발표한 노동자 감시 시스템 실태 및 노동자 인식 조사 결과 는 한국 노동현장에서 노동자감시 시스템이 얼마나 많이

보급되고 인식이 이루어지고 있는지를 전반적으로 보여주었다.

당시 조사는 성별, 연령별, 업종별, 직무별, 사업장규모별, 근속년수 별, 조합원여부별로 표집되어 이루어졌는데, 90% 가까이의 사업장에서 어떤 종류이든 전자 감시시스템이 설치되어있다고 나타난 바 있다.

이 조사는 노동조합 간부 또는 시스템 관련 직원을 대상으로 조사한 것으로서, 조사 결과에 나타난 설치 비율이 실제보다 적을 가능성이 있지만, 90%라는 수치는 이미 감시시스템이 '일반적'으로 이용되고 있음을 의미한다.

<표 2-7> 노동자 감시시스템 실태

| | 인터넷 | 하드디스크 | 전화 | CCTV | 전자신분증 | ERP | 비설치 | 설치 |
|---|---|---|---|---|---|---|---|---|
| ■ 전 체 | 41.5 | 44.0 | 24.2 | 57.0 | 56.5 | 29.5 | 10.1 | 89.9 |
| □ 업 종 별 | | | | | | | | |
| 기계/금속(N=61) | 47.5 | 47.5 | 31.1 | 45.9 | 70.5 | 50.8 | 6.6 | 93.4 |
| 화학/섬유(N=24) | 45.8 | 41.7 | 12.5 | 37.5 | 41.7 | 45.8 | 20.8 | 79.2 |
| 유통/숙박(N=22) | 31.8 | 27.3 | 27.3 | 68.2 | 59.1 | 18.2 | 18.2 | 81.8 |
| 운 수(N=19) | 36.8 | 42.1 | 15.8 | 52.6 | 36.8 | 15.8 | 21.1 | 78.9 |
| 금융서비스(N=30) | 36.7 | 40.0 | 20.0 | 80.0 | 63.3 | 13.3 | 3.3 | 96.7 |
| 보건 의료(N=21) | 38.1 | 52.4 | 57.1 | 81.0 | 57.1 | 4.8 | 0.0 | 100.0 |
| 공 공(N=30) | 43.3 | 50.0 | 3.3 | 50.0 | 43.3 | 23.3 | 10.0 | 90.0 |
| □ 직 종 별 | | | | | | | | |
| 생산기능직(N=79) | 48.1 | 45.6 | 22.8 | 45.6 | 62.0 | 48.1 | 10.1 | 89.9 |
| 사무영업직(N=38) | 39.5 | 39.5 | 26.3 | 71.1 | 65.8 | 23.7 | 5.3 | 94.7 |
| 판매서비스직(N=20) | 25.0 | 30.0 | 30.0 | 65.0 | 55.0 | 15.0 | 20.0 | 80.0 |
| □ 사업장규모별 | | | | | | | | |
| 1- 99인(N=25) | 16.0 | 40.0 | 12.0 | 52.0 | 36.0 | 12.0 | 20.0 | 80.0 |
| 100-499인(N=91) | 31.9 | 38.5 | 20.9 | 50.5 | 50.5 | 27.5 | 16.5 | 83.5 |
| 500-999인(N=35) | 51.4 | 51.4 | 34.3 | 45.7 | 60.0 | 31.4 | 2.9 | 97.1 |
| 1000인이상(N=56) | 62.5 | 50.0 | 28.6 | 76.8 | 73.2 | 39.3 | 0.0 | 100.0 |

* 노동자감시근절연대모임, 2003

또 감시 시스템을 도입한 사업장의 경우 평균 2.57 가지의 감시 시스템을 운영하는 것으로 나타났다. 조사에 따르면 △인터넷 이용감시 △하드디스크 내용검사 △전화 송수신 기록 △CCTV카메라 설치 △전자신분증 사용 △ERP(전사적 자원관리시스템) 설치 중 적어도 한 가지 이상을 설치한 사업장이 89.9%인 반면, 한 가지도 설치하지 않았다는 사업장은 10.1%에 불과했다. 특히 보건의료업종과 1000명 이상 사업장의 경우는 조사대상 사업장 전체(100%)에 보안관리시스템이 설치된 것으로 나타났다.

보안관리시스템의 개별설치 실태를 보면, CCTV 카메라 설치(57%)와 전자신분증 사용(56.5%) 비율이 가장 높았고, 그 다음은 하드디스크 내용 검사(44%), 인터넷 이용감시(41.5%) 순이었으며, ERP 설치(29.5%), 전화송수신 기록(24.2%)은 상대적으로 낮게 나타났다.

하지만 이 역시 최근 도입되고 있는 위치추적시스템(GPS, 핸드폰 위치추적 등)과 생체인식기(지문, 홍채, 정맥 인식기 등)를 포함하고 있지 않아, 전체 감시 시스템 도입 비율 또는 감시 시스템 평균 운영 수는 조사 결과보다 상회할 수 있음을 감안해야 한다.

한편 회사 측이 밝힌 감시 시스템의 도입 근거는 ▲문제발생시 객관적 근거마련, ▲생산과정 모니터링과 경영혁신, ▲노동자 기물파손 및 절도방지, ▲불법소프트웨어 문제 방지 등의 순으로 나타났다.

<표 2-8> 회사 측 감시 시스템 도입 근거

| 도입 근거 | 문제발생시 객관적 근거마련 | 생산과정 모니터링 경영혁신 | 노동자 기물파손 절도방지 | 불법소프트웨어 문제방지 | 근무시간 사적활동 방지 | 노동자 건강안전 | 기타 | 잘모름 |
|---|---|---|---|---|---|---|---|---|
| 비율 | 30.6 | 27.4 | 16.7 | 8.1 | 7.5 | 5.9 | 12.9 | 27.4 |

* 노동자감시근절연대모임, 2003

같은 조사의 결과에서 인터넷 감시 중 차단되는 사이트가 노동조합 9.6%, 정당시민단체 1.4%인 것은, 회사가 노동자의 권리인 자주적인 노동조합 활동을 의

도적으로 방해하고, 공민권을 제한하는 등 노동자의 기본 권리를 제약하는 비율이 적지 않음을 보여주었다. 또 홈페이지 게시판 작성이나 이메일 작성 내용까지 기록하는 경우가 18.8%에 이르며, 전화 통화내용까지 기록하는 경우도 6.0%에 이르는 것으로 나타났다.

감시 기록에 대해서 당사자나 노동조합이 기록·저장 내용 열람 및 소명을 할 수 있는 비율이 40.9% 밖에 되지 않아 절반 이상의 노동자가 무엇이 기록되고 있는지 알 수 없으며, 잘못된 기록을 수정할 수 있는 기회를 갖지 못하는 것도 문제로 드러났다.

또 감시 시스템 설치 시 노동조합과 회사 간 마찰 비율은 26.3%, 노동자와 회사 간 마찰 비율은 12.9%로, 감시 시스템 설치로 인한 마찰이 적지 않음을 보여 주었고, 감시 시스템 설치에 대한 문제제기 내용으로 프라이버시 문제, 노조활동 위축탄압, 부당노동 행위, 노동 강도의 비율이 높게 나타났다. 특히, 1/4 가량에서는 회사 측이 단체협약을 위반하면서까지 감시 시스템을 설치하여 마찰을 빚은 것으로 조사되었다.

<표 2-9> 감시 시스템 설치 시 노동조합/현장노동자와 회사의 마찰

| | 마찰 비율 | 프라이버시 문제 | 노조활동 위축탄압 | 부당노동행위 | 노동강도 | 작업방식 태도변화 | 인사관리 | 단협위반 | 고용불안 | 임금 | 문제제기 내용 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 노동조합 | 26.3 | 55.1 | 51.0 | 44.9 | 40.8 | 28.6 | 24.5 | 24.5 | 20.4 | 14.3 | 노동조합 |
| 노동자 | 12.9 | 66.7 | - | - | 54.2 | 37.5 | 29.2 | - | 25.0 | 16.7 | 노동자 |

* 노동자감시근절연대모임, 2003

감시 시스템을 회사가 도입할 때, 사전협의(또는 합의) 24.2%, 사후협의(또는 합의) 6.5%에 비해 노동자나 노동조합에 통보 없이 도입하는 경우가 46.2%로, 노동자나 노동조합에 영향을 미치는 감시 시스템이 회사에 의해 일방적으로 도입되

는 경우가 월등했다. 단체협약에 새로운 생산방식이나 장비도입과 관련된 협의나 합의를 하도록 하는 조항이 있는 경우가 26.9% 밖에 되지 않아, 새로운 시스템 도입이 노동자나 노동조합에 부정적인 영향을 미치지 않도록 하는 사전 장치가 상당한 수의 사업장에 부재함을 보여주었다.

# 3장. 사업장 실지조사

## 1. 조사의 개요

본 연구의 실지조사는 △업종과 부문, △기술적 특성, △갈등상황 순으로 대상 업체를 선정하여 15개 사업장에 대하여 진행하였다. 이는 감시시스템과 관련하여 분쟁이 발생하거나 내용이 잘 알려진 사업장에만 집중하는 결과를 방지하기 위함이었다.

사전 조사로 기존 연구결과 및 기술적 검토를 선행했고, 질문지를 배포하고 그 순서에 따라 면접을 하는 방식을 취했다. 피조사자는 노동자 측과 관리자 측 양측을 모두 포함하는 것을 기본으로 하였으나, 관리자 측에 대한 접근성이 어려움으로 인해 사측의 입장에 대한 충분한 조사는 이루어지지 못했다. 이 외에 감시시스템과 관련하여 입수 가능한 문서자료와 사진자료를 활용하였다. 조사 결과를 공통성이 강한 사례들을 중심으로 몇 개의 범주로 묶어서 정리하였다. 이미 잘 알려진 일부 사례의 경우 문헌자료 취합 및 보충 인터뷰로 보완하였다.

<표 3-1> 실지조사 사업장 개요[2)]

| 구분 | 사업장명 | 업종 | 감시시스템 종류 |
|---|---|---|---|
| 노조탄압과 감시시스템 | KT 상품판매팀 | 민간서비스 | 도청, 미행, GPS |
| | 삼성 SDI | 제조업 | 핸드폰 복제 추적 |
| | 하이텍 RCD | 제조업 | CCTV, 전자카드 |
| CCTV의 과다한 사용 | 성진애드컴 | 제조업 | CCTV |
| | A운수 | 운수업 | CCTV |
| | B버스 | 운수업 | CCTV |

| | | | |
|---|---|---|---|
| IT업종과 인터넷 체킹 | C사 | 제조업(IT) | 인터넷 원격감시, 이메일,메신저 체킹 |
| | D시스템 | 제조업(IT) | 인터넷 원격감시 |
| ERP의 영향 | E사 | 판매서비스 | 스캐너 |
| | F교육 | 민간교육 | PDA |
| | 전북대병원 | 보건의료 | ERP |
| | 광명성애병원 | 보건의료 | ERP, CCTV |
| 기타 | G사 | 공공서비스 | 전자출입통제 시스템 |
| | H은행 콜센터 | 금융업 | 통화내용 녹취 |
| | I구청 | 정부부문 | 생체인식 출입기록 |

## 2. 조사 결과

### 1) 노조 탄압과 감시시스템

여기에서 살펴보는 세 개의 사업장은 노조 결성 움직임에 대한 사용자의 극단적 탄압과 노조 활동 방해가 감시시스템을 통해 이루어지고, 이와 관련하여 노사 간의 첨예한 충돌이 빚어진 사례들이다. 비단 전자 감시시스템만이 아니라 미행, 협박 등 전통적인 감시, 통제 방식 등이 다양하게 이용되었으나 핸드폰 복제와 위치추적 등 새로운 기술을 이용한 감시가 극단적인 인권 침해 사례를 만들었고, 그것이 매우 격렬한 갈등을 낳는다는 점에서 특별한 관심을 요한다.

#### (1) KT 상품판매팀

KT는 전기통신사업의 효율적 경영을 위해 체신부에서 통신부문을 분리하는 공사화 전환 계획에 따라 1981년 '한국통신'으로 설립되었고, 민영화를 거치면서

2) 언론 등을 통해 이미 알려진 사업장이 아닌 경우 본문에서 알파벳으로 표기하였다.

2001년 12월 사명을 'KT'로 바꾸었다. 국내 일반전화 사업을 독과점하고 있을뿐 아니라, 초고속인터넷 시장의 후발 사업자로서 사업개시 1년 만인 2000년 6월 국내 초고속인터넷 시장 1위 달성한데 이어 2003년 1월, 500만 가입자를 확보할 정도로 국내 초고속인터넷 시장에서 독보적인 자리를 굳히고 있다.

KT 노조는 2005년 4월 현재 전국 473개지부에 30,868명의 조합원을 확보하고 있고, 민주노총 IT연맹 소속이다. 하지만 노조의 노선을 둘러싸고 노동조합 내의 갈등이 몇 년째 지속되고 있다.

KT 상품판매팀의 사례는 노동조합과 관련된 특정 노동자 집단을 배제하고 탄압하기 위하여 매우 다양한 감시통제 기법을 사용한 경우로 꼽힌다. 특히 이로 인해 해당 노동자들이 정신적 질환을 겪고 있다는 결과가 발표돼 충격을 주기도 했다.

이는 KT가 2004년 9월 대대적인 명예퇴직을 단행하면서 이에 응하지 않는 500여명의 노동자들을 '상품판매전담팀'(상판팀)으로 강제 발령하고, 이들에 대해 수시로 감시·미행함으로써 해당 노동자 상당수가 정신적 스트레스로 인한 우울, 불안, 긴장, 공포, 신경과민 등의 증세에 시달리고 있다고 언론에 보도되면서 알려졌다. 이러한 결과는 인권단체연석회의가 지난 2004년 9월부터 두 달에 걸쳐 KT 전국상판인모임을 순회하며 집단 설문을 벌이고, 보건의료단체의 도움을 받아 이들 상판노동자들에 대해 정신질환검사를 진행한 결과에 따른 것이었다.

<표 3-2> 상판팀에 대한 감시 유형

| 감시유형 | 개수 | 비율 |
|---|---|---|
| 특정인의 미행을 통한 감시 | 43 | 28.1 |
| 사진 또는 동영상 촬영 | 8 | 5.2 |
| 음성기록장치를 통한 녹음 | 6 | 3.9 |
| 핸드폰, PDA 공중전화를 통한 위치 파악 | 19 | 12.4 |
| 「기타」 | 20 | 13.1 |

* 인권단체 연석회의, KT 상품판매 전담팀 인권백서

인권단체연석회의는 “KT가 단일 기업으로는 최대규모의 명예퇴직을 단행하면서 이에 응하지 않는 노동자가 늘어나자 ‘상판팀’ 개설이라는 특단의 조치를 취하기에 이르렀으며, 이렇듯 명예퇴직 거부에 따른 인력퇴출 프로그램의 일환으로 구성된 상판팀은 일반 영업직원들과는 전혀 다른 갖가지 감시와 차별에 시달려야 했다”고 밝혔다.

상판팀 노동자들은 특히 △업무지역 미배정 △판촉상품과 기업카드 미지급 △개인별 매출목표 제출 △일일 활동실적 제출 △각종 교육 및 회의 참석 불허 △영업활동에 따른 휴대폰 보조금 차별 등을 경험했고, 이로 인해 상당수가 심각한 스트레스에 시달렸다. 실제로 인도주의실천의사협회가 KT 상판팀 노동자 188명을 대상으로 기초적인 정신질환검사(MMPI 다면성 인성검사)를 실시한 결과, 검사에 응한 노동자 중 84명(45%)에게서 정신병적 상태가 발견되기도 했다.

감시는 미행과 위치추적 감시가 가장 주된 형태였다. 특히 정신건강 악화로 인해 산재판결을 받은 박아무개씨는 “나도 모르는 사이 회사 관계자들이 나를 미행하고 있었다”며 “휴대폰 영업을 위해 사람이 많이 모인 시장에 갈 때도, 심지어 목욕탕에 갈 때도 미행하고 있었다”고 주장했다. 또한 “회사는 상판팀 노동자들의 이동경로를 감시하면서, 매일 회사에 제출하게 돼 있는 ‘일일활동계획’에서 벗어난 곳으로 이동할 경우 ‘직무태만’임을 들어 퇴직을 종용했다”며 “지금도 누군가가 나를 지켜보고 있는 것 같은 불안감에 시달리고 있다”고 말했다.

결국 KT는 사회적 여론의 압박을 견디지 목하고 2005년 1월 상판팀을 해체하고 해당 노동자들을 일반 업무에 복귀시켰다.

### (2) 삼성 SDI

삼성 SDI는 ‘삼성전관’으로 출발하여 컴퓨터 모니터, TV브라운관으로부터 최근 디지털 TV용 PDP, 이동정보 통신기기 LCD, 2차 전지 및 인터넷 핵심부품까지 세계적 수준의 디스플레이 전문 생산업체이며, 설립된지 30년 정도 된 중견기업이다. 현재 전체 종업원 수는 18,500여 명이고, 매출액은 5조3천억 원에 이른다.

삼성 SDI는 삼성그룹에 공통적인 '무노조 경영' 노선을 따르고 있고, 이에 대한 평가도 엇갈린다. 사측은 노사협의회를 통해 고충이 해결되고, 또 기업 경쟁력의 원천을 신뢰와 믿음을 바탕으로 한 조직풍토에 두기 때문에 노조는 필요 없다는 입장이다. 하지만 노조가 필요하든 주장이나 결성 움직임은 심심치 않게 일어나 왔으며, 이에 대한 사측의 집요한 방해와 탄압이 사회문제화된 바도 적지 않았다. 여기서 살펴보는 사례도 그러한 맥락 속에서 이해할 수 있다는 경우다.

삼성 SDI는 2003년 이래 노조 결성을 막기 위해 사측에서 불법 복제 휴대폰을 만들어 노동자들의 감시에 사용했다는 의혹을 받았다. 이 사건 피해자들은 모두 삼성 SDI 수원공장과 울산공장의 직원과 근무 중 사망한 노동자의 배우자, 삼성일반노조 위원장이기 때문에 삼성의 연관성을 의심받았다. 또한 불법복제폰을 이용해서 발신을 할 때 기지국이 대부분 삼성 SDI 수원공장이 있는 지역이어서 불법복제 휴대폰을 소지한 사람은 삼성SDI 현재 직원일 가능성이 높다고 지적되었다.

2003년 8월, 삼성 SDI의 전 현직 노동자들, 삼성전자 해고자, SDI 부산공장 산재사망노동자 배우자 등 삼성과 '불편한 관계'에 있는 20여명이 누군가로부터 위치추적을 계속 당해왔다는 이야기가 알려졌다. 이들 피해자들은 삼성그룹 차원에서 노동자들을 감시·통제하면서 노동기본권을 침해하고 있다는 강한 의혹을 제기했다. '불법 위치추적'이 삼성이 행한 것이라는 의혹의 이유는 다음과 같다.

첫째, 피해자 대부분이 노조결성 추진과 관련한 전, 현직 삼성노동자들이거나 가족이라는 사실이다. 둘째, 누군가 동일한 핸드폰으로 삼성의 전, 현직 노동자 9명 혹은 10명씩 위치추적을 했는데 이는 개인적인 동기에 의해 이루어지기 힘들다는 점이다. 즉 2인 이상 누군가에 의해 조직적이며 계획적으로 이루어 졌다고 볼 수밖에 없다는 것이다. 셋째, 피해자들에 대한 위치추적이 장기간 반복적으로 진행됐는데 퇴근시간 후에 집중적으로 이뤄졌다. 삼성 SDI 부산공장 송OO씨의 경우 다른 노동자들과 모임이 있는 날 18시경부터 21시께까지 총28회 위치추적을 당한 것으로 드러났다. 넷째, 불법복제폰 발신시 기지국이 대부분 '수원시 영통구 신동'이다. 그런데 이곳은 삼성 SDI 수원공장이 있는 지역으로 불법복제 한 휴대폰을 소지한 사람이 삼성 SDI 직원일 가능성이 높다는 것이다. 다섯째, 위치추적

이 삼성 SDI 울산공장과 수원공장에서 동시에 이루어졌다는 점이다. 여섯째, 위치 추적이 집중적으로 진행되던 3개월 동안은 삼성수원공장에 대한 해외이전이 추진되면서 구조조정을 한창 진행하던 시기로서 그 어느 때보다 노동자들의 불만이 표면화 되었을 때라는 점이다.

게다가 위치 추적이 이뤄진 당일은 적극적으로 노조 결성을 추진했던 피해자들이 회합을 가진 날이어서 삼성이 노조결성과 관련한 움직임을 파악하기 위해 장기간에 걸쳐 조직적, 계획적으로 위치를 추적한 것으로 추정되고 있다. 특히 사망한 사람의 핸드폰 번호까지 이용해 위치추적을 해온 사실은, 전문가들까지 동원해 진행됐다는 점에서 더 큰 충격을 주었다.

이와 관련해 인권·시민단체들은 기자회견을 열어 "피해자 전원이 전·현직 삼성노동자라는 점에서 삼성그룹이 노조 결성을 막으려 불법으로 노동자들을 감시한 의혹이 짙다"며 이학수 삼성구조조정본부 부회장 등 삼성 관계자 7명을 통신비밀보호법 위반 등 혐의로 서울중앙지검에 고소했다.

하지만 2005년 2월 중순 경, 검찰은 7-8개월을 끈 삼성 SDI 전, 현직 노동자들에 대한 불법 휴대폰 복제를 통한 위치추적 수사에 대해 '휴대폰 복제는 맞으나 복제를 했다는 성명 불상자에 대해 신원확인이 되지 않아 기소 중지하고, 삼성 관계자들에 대해서는 참고인 중지를 결정하며 사실상 수사를 종결하겠다'고 밝혔다.

### (3) 하이텍 RCD 코리아

서울 금천구에 위치한 하이텍 RCD 코리아는 1973년에 설립된 제조업체로, 모형비행기 부품 등을 만드는 중소기업(회장 박승순)이다. 총 130여명의 사원 중 약 45명이 생산직에서 근무하고 있는데, 이중 노조 조합원은 15명(육아휴직 2명 포함)이다.

하이텍 RCD 코리아는 CCTV, 동료를 통한 사업장 감시, 녹음 등 여러 방식을 조합하여 노동조합 활동을 방해함으로써 사회 문제가 되었다. 하이텍 RCD 지회는 2002년 임단협 당시 김OO 지회장을 비롯한 5명의 조합원이 부당해고를 당

해 이들에 대한 원직복직을 비롯, 노조탄압 중단 등을 요구하며 올해로 4년째 투쟁을 진행하고 있다.

현재까지 지속되고 있는 노사갈등의 진원은 지난 2002년으로 거슬러 올라간다. 당시 회사는 천지 태광 노조와의 대각선 교섭을 문제 삼아 일체의 교섭에 응하지 않는 등 노조와 대립했고, 같은 해 6월부터 11월까지 6개월 동안 쟁의행위에 결합한 조합원들의 출입을 봉쇄하는 이른바 '공격적 직장폐쇄'를 단행해 물의를 빚은 바 있다.

이후 직장폐쇄를 풀고 조합원이 업무에 복귀한 후 다음해인 2003년 1월 회사는 다시 노조 지회장을 비롯한 5명의 조합원들을 일방적으로 해고하고, 감시카메라 등을 설치해 조합원에 대한 일상적인 감시에 나서 노조의 반발을 사왔다. 지난 2003년에는 회사의 CCTV를 통한 노동자 감시사례가 언론에 보도돼 사회 문제화되기도. 한편 서울지방노동위원회와 중앙노동위원회는 2003년 4월과 11월 해고자 5인에 대해 '부당해고'로 인정하고 '원직복직 시키라'고 판결을 내렸으나 회사는 현재까지 이를 이행하지 않고 있어 노조와의 마찰을 빚고 있다.

이 과정에서 조합원 다수가 회사의 일상적인 감시와 탄압, 노골적인 비조합원과의 차별 대우 등으로 인한 정신적 고통을 호소해 지난 해 한국노동안전보건연구소 연구원과 상담한 바 있다. 이어 연구소의 소개로 2004년 8월부터 신경정신과 의원의 진료를 받아온 조합원들은 2005년 4월 현재 13명 조합원 전원이 '우울증을 수반한 적응장애' 진단을 받고 치료 중이다.

조합원들에게 공통적으로 나타나는 증상은 두통, 안면근육마비, 불면증, 소화불량, 강박증 등. 일부 조합원은 "화를 참지 못하고 자주 통곡을 한다", "때때로 살인충동을 느끼고, 나도 모르게 욕설이 나오는 등 과격해졌다"며 성격이 과격해지는 변화를 겪었다고 증언하기도 했다.

조합원들은 이러한 증상의 원인이 지난 4년여 동안 일상적으로 이루어진 회사측의 노조 탄압 때문이라고 주장하고 있다. 특히 CCTV, 녹음기, 도청기를 동원한 전방위적 감시가 조합원들의 불안증, 강박증을 유발하는 일차적 원인이라는 지적이다.

노조는 회사를 노동부에 고발하며 "부당해고도 억울한데 CCTV 감시로 인권

침해를 받고 있다"고 말했다. 더욱이 CCTV의 설치시기가 노사간의 갈등이 첨예한 시기였고, 또 설치장소가 노조사무실 인근과 집회가 열리는 회사마당, 공장 출입구 등이어서 '노조감시용'이라는 의혹을 증폭시키고 있다.

실제로 회사가 조합원들을 상대로 작성한 고소 고발장에는 CCTV에 담긴 장면들이 근거자료로 다수 활용되고 있었다. 회사측은 "재산관리, 방범의 목적"과 동시에 "불법적 노조활동에 대한 방어조치의 측면도 있다"고 말해 노조에 대한 감시목적을 전면 부인하지는 않았다. 또한 지난 4월부터 도입한 직원카드에 대해서는 "근태관리와 급여관리의 기본자료로 사용되고 있다"고 덧붙였다.

### 2) CCTV의 과다한 사용

CCTV는 가장 광범위하게 사용되는 감시시스템이다. 점포, 아파트, 관공서, 어린이집에 이르기까지 평범한 사람들의 일상생활이 이루어지는 거의 모든 곳에서 이용되고 있는 시스템이지만, 강남구의 방범용 CCTV 논쟁에서 드러났듯이, 아직 그 이용의 제한이나 방식에 대한 제도화나 사회적 합의가 충분히 이루어지지 않고 있음이 여러 차례 제기되었다.

작업장에서의 CCTV는 노동과 자본 사이의 통제와 저항이라는 잠재적 대립구도 속에서 더욱 심각한 양상으로 갈등을 빚어내곤 한다. 그러나 관리비용의 절감이라는 이점과 사회적 견제 장치의 부재 속에서 사용자 측에서는 아무런 문제의식 없이 CCTV를 과용하는 경우가 많으며, 노동자 측에서도 그것을 당연한 것으로 생각하는 경향이 있다는 것이 문제로 지적된다. 대구 삼천리버스 등의 사례는 노사 간의 법적 다툼으로까지 문제가 비화되기도 했다.

노동 현장에서의 CCTV 문제는 (주)대용의 사례로부터 알려지기 시작했다. (주)대용의 노동조합은 전국 최초로 노동자의 인권을 침해하는 CCTV 철거를 외치며 2001년 8월 파업에 돌입하여 한 달만에 CCTV를 철거시켰다. 당시 전북지역 19개 사회단체가 모여 '공동대책위원회'를 결성하고 노동감시와 노동현장의 인권침해를 주변에 알려 여론화함으로써 노동자들의 기본 인권을 지켜낼 수 있었다.

### (1) 성진 애드컴

성진 애드컴은 1998년에 창립했고, 서울 중구 인현동에 위치하여 인쇄물품 접수, 기획, 외주 제작 (사장 부친 경영), 출고 업무를 한다. 종업원수 (정규직/비정규직, 성별)는 75-80명으로 모두 정규직. 성비는 반반이다. 작업과정에서 컴퓨터(pc) 사용은 접수 등 업무 위하여 사원마다 1대씩 있다.

노사관계는 2004년 노조를 창립했고, 현재 조합원은 8명이며 민주노총 언론노조 경인인쇄지부 소속이다. 노조 창립시 조합원 21명이었으나 대부분 퇴사하고 8명이 남아있다. 8명 중 1명은 해고되고 분회장 등 4명은 2-3개월의 정직 처분을 받았다. 노조 설립 배경은 사측의 인격 모독, 근무시간이나 식사보장 등 근기법이 제대로 적용 안되는 열악한 노동 환경 때문이었다. 노동조합은 노조 인정과 성실교섭 촉구 위해 2005년 5월 4일부터 천막농성 중이다.  요구 사항은 감시카메라 관련, 단협 제정, 해고자 복직, 김OO 이사의 공개 사과 등이다.

감시시스템과 연관된 사업장 특성에 대하여, 노동자 측은 부품 절도 같은 우려는 없다고 본다. 인쇄업종 치곤 재작년부터 매출도 증가하고 인터넷 접수도 잘되는 편이라 경영 상태 좋음. 업종 특성상 이직률은 높은 편이다.

성진 애드컴은 감시 시스템으로 인터넷 이용 통제(사내 업무용 PC의 개인 인터넷 이용 봉쇄하고 회사 접수 업무만 가능하도록 변경)가 이루어지고 출퇴근 기록용 지문인식기가 현관에 설치되어 있다. 2003년 8월부터 있었고 입사시 오른손 검지 지문을 채취한다(채취 동의서 같은 것은 없었다).

하지만 성진 애드컴에서 가장 특징적인 것은 매우 많은 수의 CCTV이다. 본사 건물에만 17대가 설치되어 있으며 출고장에도 몇 대가 있다. 이는 다른 사업장에 비해서도 극히 비정상적으로 많은 것으로 그 중 1,2번은 건물 밖의 일반 행인까지 비추도록 되어 있다. 직원들의 휴게공간까지 설치되어 있는가 하면, 사무실 내에는 조합원들을 한자리에 모아서 일하게 하고 그 곳을 집중적으로 비추게 함으로써 노조 활동 방해 의도가 매우 뚜렷하다 하겠다.

CCTV는 일과 시간 중 일방적으로 설치되었다. 사측에선 처음엔 가짜 카메라라고 주장했으나 직원이 업무시간 중 자리를 뜨거나 하면 바로 전화로 연락이 와

서 주의를 주고 하는 것을 보고 진짜 카메라라는 것을 곧 알게 되었다. 최초에는 경리부 수납업무 공간 쪽부터 설치했고, 출입구 조망 위치, 휴게실, 조합원 근무 방향 쪽으로 순차적으로 추가 설치되었다. 사측 관계자는 화재예방 또는 보안 때문에 설치한 것이고 감시할 의도는 없다고 주장(KBS "시사투나잇"에서 2005년 5월 11일 방영)한 바 있다.

<표 3-3> 성진애드컴 본사 건물 CCTV 설치 현황

| | |
|---|---|
| 1,2번 | 건물 입구에서 인도까지 감시 |
| 3번 | 건물 2층으로 올라가는 중간화장실 옆 감시카메라 |
| 4번 | 2층 접수실 입구 감시카메라 |
| 5번 | 2층 접수실에 들어서면 보이는 카메라 |
| 6-11번 | 2층 접수실에 들어가면 왼쪽과 오른쪽에 각각 3대씩 카메라 |
| 12번 | 3층 통신실(인터넷접수) 올라가는 계단 감시카메라 |
| 13,14번 | 3층 통신실 안 감시카메라 |
| 15번 | 4층 사장실 올라가는 계단 감시카메라 |
| 16,17번 | 휴게실 내 감시카메라 |

* 성진애드컴 노동조합 발간 화보집 (2005)

반면에 노조는 노조탄압과 노조 해체 의도가 명확하다고 주장한다. 예컨대 비조합원이 조합원 자리 가까이 오면 인사하거나 이야기를 나누지 못하는 분위기가 연출된다. 직원간 상호감시를 강요하여, 이 때문에 퇴사한 직원도 1명이 있었다. 도입시 카메라에 락카칠을 하거나 가리는 등 일부 저항이 있었고, 사측에서는 고소고발 조치를 취하였다. 이후 노조 측은 더 이상의 저항을 못하고 방치한 상황이다. 감시카메라 외에도 경비용역 2인이 상시 근무하여 감시하고 있다. 이들은 2005년 1월 파업 때 처음 채용되었고 5명까지 증가한 적도 있었다.

이러한 CCTV 감시시스템 도입을 주도한 것은 김OO 이사(사장)다. CCTV 시

청을 위한 모니터실이나 관리실이 따로 있지는 않고 사장과 몇몇 관리자(시설관리 시스템 과장)의 컴퓨터에 모니터 프로그램이 깔려 있어서 실시간으로 볼 수 있다. 직원이 업무를 비우거나 하면 이들이 지켜보고 있다가 바로 전화연락을 하여 조치하는 형태다.

노사 간의 첨예한 갈등상황을 감안해야 하겠으나, 노조 측은 성진 애드컴의 감시시스템에 대해 매우 비판적이다. 동종 인쇄업계에서도 CCTV를 통한 감시 사례에 관련하여 들은 바 없으며, 감시카메라로 인해 생산성 향상이나 보안성 강화 같은 효과도 전혀 없다고 본다. 오히려 사업장 분위기가 위축되었고, 동료간 갈등이 조장되고 일할 때는 언제나 신경을 쓰게 되었다는 것이다.

때문에 노조 측에서는 현재 단협 요구안에 감시카메라 관련 내용을 포함하여 제출하고 협상을 촉구하고 있다. 그 내용은 카메라 설치내역(종류, 방식), 자료 보관 유무 등을 공개하고, (대금수납 부서 등 최소한 필요 부분 제외하고는) 불필요하다고 판명되면 철거해야 한다는 것이다.

### (2) A운수

A운수는 창립된지 10년 정도가 된 버스 회사로 최근 A'운수와 통합되었다. 서울 관악구 신림10동에 소재해 있고, 종업원 수는 37명으로 모두 남성이다. 고용형태는 정규직이었으나 노조 결성 이후 전원 계약직으로 바뀌었다.

A운수는 마을버스만을 운행하는데, 지역에서 황금노선을 갖고 있어 회사 경영사정이 좋은 편이나, 임금은 상대적으로 낮은 축에 속한다. 2005년 3월 24일, 37명 중 17명의 조합원으로 노조를 결성하고 민주노총 민주버스노조에 소속되었다. 하지만 곧 이중 14명이 계약만료로 해고되었고, 현재 중노위와 지노위에 복직소송이 계류 중이다

A운수 역시 버스업체에 일반적인 CCTV 시스템이 문제가 되었다. 현재 전국의 모든 영업용 버스에 CCTV가 설치되어 있다고 보면 되는데, 이 사업장에도 처음에는 수익금 관리 문제로 설치한다고 이유를 들었다.

하지만 노조 설립 이후 chip 방식의 최신 장비로 교체되었다. 버스 1대 당 4대의 카메라가 설치되었고, 설치기술자의 이야기로는 실시간으로 영상이 회사로 중계되고 녹음 기능이 있다고 한다(실시간 전송이 사실인지는 확인되지 않았다). 운전사들은 교통카드를 안찍고 승차하는 (조합원 등) 경우 그날 저녁 바로 주의를 받고 시말서를 요구받는 경험을 했다. 앞 배차 차량이 카메라에 찍히면 역시 저녁에 사측의 지적이 들어왔다고 한다. 녹음을 의식해서 말도 조심하게 된다.

일반 버스에 카메라가 1-2대 설치된 것에 비해, A운수 차량의 카메라 설치 대수는 두 배나 많은 편이다. 그 설치 개소는 다음과 같다.

<표 3-4> A운수 버스 차량의 CCTV 설치 현황

| | |
|---|---|
| 카메라 1 | 기사 앞 (전방 조망) - 사고 예방 또는 배차 간격 감시 기능 |
| 카메라 2 | 기사 왼편 - 돈통 및 앞문 조망 |
| 카메라 3 | 기사 앞 - 기사 상체 조망 |
| 카메라 4 | 돈통 뒤 - 승객 및 뒷문 조망 |

* 이 사업장의 경우 직원 휴게공간과 회사마당(주차장)에도 원래 CCTV가 있었음.

A운수는 삥땅, 불규칙 운행에 대한 우려 등 버스업체의 일반적 특성 외에 CCTV를 설치할 이유는 별로 없었다고 한다. 이 사업장에서 그런 문제가 특별히 불거진 경우도 없었다.  회사 내 직원과 사측의 일종의 원한 관계나 트러블이 많았던 것으로 전해진다. 노조 설립도 노사간 극심한 갈등을 배경으로 하였다.

사측에서는 사고 미연방지, 삥땅 방지 등을 CCTV 추가 설치 이유로 내세우고 있지만 노조 측에서는 노조 감시 및 법률적 대응을 목적으로 한다고 확신하고 있다. 차량에 위해를 가할 우려를 방지한다고 하지만, 이 역시 노사간 갈등이 원인이 되었던 것이다.

시스템 관리는 배차 인사관리 등을 전담하는 관리부장 소관이며, VHS 테이프가 기본으로 들어가지만 chip에서 바로 전송되는 것으로 알려져 있다. 높이 40

센티미터 가량의 안테나가 운전석 근처에 부착되어 있다. 하지만 녹화 기록의 보관기간 이나 방식에 대한 자세한 사항은 노동자들이 전혀 알지 못하며, 시스템 운영에 관한 협의나 규정도 존재하지 않는다.

노조 측에서는 CCTV로 인한 정신적 스트레스나 수치심 같은 것은 모두가 느끼는 것이라고 증언한다. 승객들도 불필요하다고 지적한다는 것이다. 물론 감시 시스템이 필요할 수도 있지만 정도를 넘어섰기 때문에 과하다는 것이다. 하지만 현장 노동자들은 관련한 법제도 같은 게 있는지도 모르기 때문에 문제제기하지 못하는 상황이다.

### (3) B버스

B버스는 창립 연도가 30년 이상 된 중견 업체로, 서울 송파구 장지동 92번지에 위치하고 있다. 종업원수는 350명으로 서울에서도 규모가 큰 편이다. 이중 비정규직이 10% 이상인데, 이들은 대부분 58세 연령제한을 넘어서 1년 단위로 계약하는 촉탁기사들이다. 시내버스 110대, 공항버스 51대를 보유하고 있다.

노사관계를 살펴보면, 한국노총 자동차노련 소속으로 현 지부장이 18년째 연임하고 있으며 반대 세력들은 발을 붙이지 못해 왔다. 역으로 사측과 현 노조 집행부 사이의 관계는 가까운 편이다. 사업장 특성은 버스 업체 일반과 다르지 않다. 회사 경영 상황은 공항을 운행하고 황금노선을 갖고 있어 좋은 편이고, 삥땅 같은 부정도 드물었다고 한다.

B버스의 CCTV는 1999년 이전부터 설치되어 있고, 차량마다 2대씩(기사 앞, 돈통 쪽)이다. 증언을 들어 보면, 많은 버스기사들이 CCTV가 녹음도 되는 것으로 알고 있다. 예를 들어 운행 중 전화를 하면 이를 알고 주의를 준다는 경험담이다. 세부적인 CCTV의 설치 사실이나 사양에 대하여 회사로부터 들은 바 없고, 교육도 없었다. 다만 기사들끼리 나누는 이야기로 듣는 정보가 있을 뿐인데, 예를 들어 차량 중간까지 비추게 된다는 것 등이다.

그 외에 공항버스의 경우 차량마다 무전기 1대씩이 지급되어 기사들끼리 운

행 정보를 공유하게 한다. 여기에는 GPS 기능이 부착되어 있어서 센터에서 모니터링 하면서 전무가 호출이나 지시를 하게 된다.

CCTV의 시스템 관리 방식을 보면, 회사 노무과에 테이프를 모니터링하는 전담사원이 두 명 있는데, 기사들도 이들의 신상이나 얼굴을 모른다. 차량 내에서 녹화테이프가 장착된 부분은 운행 중에는 열쇠로 잠겨있다.

기록 매체는 VHS 방식의 비디오 테입이다. 테이프는 매일 교체하며, 2-3일 간격으로 교환, 재활용한다고 한다. 기록되는 데이터가 인사, 처우 등에 직업 반영되기 보다는 운전사의 잘못이 있을 때 호출하여 추궁하려는 목적이 크다. 이러한 경우 회사로 불려 들어가서 녹화된 화면을 본 운전사가 있다. 하지만 운전사가 억울한 일이 있어 이를 증명하고자 테입 내용 확인을 요청해도 회사는 응낙하지 않았다. 감시 수단은 되면서 노동자의 권리 구제 수단은 되지 못하는 것이다. 시스템 운영에 관한 협의나 규정 역시 존재하지 않지만, 기사들은 다른 버스회사도 다 하니까 하나보다 라고 생각하는 편이다.

### 3) IT업종과 인터넷 체킹

2000년대 이후 더욱 두드러지는 사업장 감시 사례는 특히 네트워크 환경에서 작업이 이루어지는 IT업종의 사례들이다. 인터넷으로 연결된 컴퓨터 사이에 오고가는 메일, 메신저는 물론 방문사이트 기록이나 모든 개인 컴퓨터 작업까지가 모니터링될 수 있다는 기술적 특성으로 인해 감시로 인한 충돌이나 잠재적 갈등 가능성이 커지고 있는 것이다.

IT업종의 직원 감시는 상용 솔루션이 광범하게 보급될 정도로 일상화되고 있으며, 큰 규모의 사업장일수록 더욱 두드러짐을 알 수 있다. 예를 들어 2005년 정보보안업체 N사가 선보인 기업 내부자 감시 프로그램을 사용하면 직원들이 보내고 받는 이메일부터 메신저를 통한 대화 내용 및 직원이 열어본 인터넷 사이트까지 모든 PC 이용 행위가 기록으로 남게 되며, 직원별로 정보 접근 권한을 설정해 권한이 없는 직원이 고급 정보에 접근하면 프로그램이 자동으로 경고 메시지를

보내고 접근을 차단하는 기능도 갖추고 있다.

첨단 기술을 사용하는 업종일수록 사용자의 경영권과 노동자 인권 사이의 대립을 제어할 수 있는 사회적 기준은 더욱 모호한 상황이어서, 이에 대한 각별한 관심이 요구된다.

### (1) C사

C사는 국내의 대표적 IT업체 중 하나로 1987년에 창립되었고, 서울 중구 회현동에 본사를 두고 있다. 종업원수는 전국적으로 5800명 가량이다. 주된 작업내용은 모든 IT문제에 대해 컨설팅부터 시스템 구축, 운영까지 토탈 솔루션을 제공하는 종합 IT서비스 회사다.

첨단 IT 업종이므로 1인 1대 이상의 컴퓨터를 이용하며, 그만큼 정보 및 기술 유출 우려가 많다는 예상이 가능하다. 다른 대기업 계열사 IT 업체와 비슷한 상황을 맞이하며 솔루션을 모색하고 있다.

C사는 직원들의 인터넷 업무가 많고 소프트웨어 개발 관련 보안 사항이 많은 관계로 인터넷, PC 관련 감시 시스템이 특징적으로 많으며 다층적으로 구축되어 있고, 보완 개선이 꾸준히 이루어지고 있다. 이러한 솔루션 중 주요한 것에는 다음과 같은 것들이 있다.

첫째, 직원 컴퓨터(LapTop, DeskTop 등 PC)의 문서 및 파일 보안(감시) 툴로 HyperDesk라는 솔루션이다. 이 프로그램은 C사 소유의 모든 PC 및 네트워크를 사용하는 모든 윈도우즈 PC(임직원/협력업체)에 설치된다. PC 사용자가 L사 네트워크에 접속하면 설치여부가 자동 점검되고, 설치 안내 및 미설치 시 보안경고가 뜨게 된다. 이 프로그램은 일단 설치되면 하드디스크를 포맷하거나 전문적인 O/S 지식을 동원할 경우를 제외하곤 삭제가 불가능하다.

이 프로그램은 PC의 파일 사용 내역, 하드디스크, CD 및 DVD, A드라이브, USB로 카피 되는 파일들의 모든 이력을 기록한다. 퇴사 혹은 자산 반납 시 하드디스크에서 이 솔루션이 기록해 놓은 모든 사항에 대한 점검이 가능하다. 퇴사 시

업무 관련 문서를 카피한 사원이 이 기록을 통해 형사 고발되는 사례도 있었다.

둘째, HyperDesk가 그룹 차원에서 PC를 관리하기 전에 자사에서 사용하던 솔루션이고, 최근 그룹 차원에서 PC보안 관련 Tool을 재배포한 것이 Defcon이다. Defcon 역시 C사 소유의 모든 PC 및 네트워크를 사용하는 모든 윈도우즈 PC(임직원/협력업체)에 설치된다. 전자 게시판, 이메일 및 보안담당자를 통해서 설치 권고 메시지를 받게 되며, 설치하지 않으면 해당 PC는 네트워크 사용을 중지당한다. 이 프로그램은 개인 업무 모니터링에 매우 효과적인 툴로 메신저 등 사내에서 사용통제가 필요한 프로그램을 개인 PC에서 구동을 하지 못하게 한다.

셋째, APC라는 솔루션으로 회사 네트워크를 사용하는 모든 윈도우즈 PC(임직원/협력업체)에 설치된다. 주로 웜이나 바이러스 침입을 발견하고 네트워크 내 감염 PC를 자동으로 감지 및 차단하는 클라이언트 프로그램(중앙에 서버가 있음)이다. 자사 전체의 전산자원 보호 차원이지만 개인 자원 혹은 능력으로 관리하기 힘든 바이러스 공격을 차단하는 순기능도 있다고 볼 수 있다.

이 외에 네트워크 차원의 모니터링 수단으로, 자사 네트워크를 사용하는 이메일, 메신저 등에서 미리 설정해 놓은 키워드가 추출되면 네트워크 담당자 및 보안담당자가 경고 메시지를 보낸 후 자세한 사실 확인에 들어가게 된다.

이렇듯 다층적인 차단 장치가 작동하는 속에서, 최근에는 일반 범용 메신저는 대부분 차단되었고, 대신 업무상의 효과를 인정해 그룹 내 사용자만 연결이 가능한 메신저를 배포하여 이용케 하는 상황이다.

이러한 차단 장치나 모니터링 툴은 대부분 설치 내역이 직원에게 고지되지 않으며, 모니터링과 이용 정보 수집의 한계나 기준도 존재하지 않는다. 하지만 IT 업계 종사자들은 이러한 기술에 대한 지식이 있는 편이기 때문에 그 설치나 활용을 파악하게 되며, 스스로 조심하여 처신하게 된다. 사실 인터넷을 이용하는 업무의 경우 업무 용도와 업무외 목적의 개인 활용이 명확히 구분되기 어려운데, 감시당하고 있다는 느낌 혹은 경험을 통해 통제 규범을 내면화하는 노동자들은 인터넷 이용을 자가검열하게 된다. 경영 측은 보안 강화를 도모하는 동시에 노동자들의 업무외 행동을 방지하는 노동 통제의 효과를 거두게 된다.

그러나 IT 업종 종사자들은 대부분 고학력 전문직으로 개인 재량권과 자격에

대한 의식이 높아 인권 침해에 대한 의식은 많지만, 이러한 문제를 집단적으로 제기하지 않는 경향이 있어 공공연한 갈등으로 표출되는 경우는 많지 않다.

### (2) D시스템

IT업체들은 규모에 따라 감시시스템 운영이 전형적으로 나타난다. IT산업 노동조합은 노조가 포괄하는 중소규모 업체들에 대해 일정한 대표성을 가지고 있다. 이 사례는 IT산업노조의 조합원이 일하고 있는 한 회사(D시스템)의 경우를 중심으로 기술한다.

창립 연도는 2002년이며, 서울 강남구 삼성동에 소재해있다. 종업원은 정규직만 15명이며, 이중 여성은 2명이다. 주된 작업내용은 IT 기술지원, 프로그램 개발 등이다. 작업과정에서 컴퓨터를 1인 1대 이상(노트북 있으면 2대) 사용한다.

노사관계는, 단위 사업장에는 노조가 없고 개인적으로 IT산업노조에 가입하여 있다. IT산업노조는 2003년 12월 창립되었고 산별을 지향하는 지역 일반노조다(2005년 11월에 민주노총 서울본부 직가입 결정). 조합원은 45명으로 대부분 중소규모 업체에 다니고 있으며 직종도 유사하다. 이들은 파견 형태로 대기업에 가서 근무하는 경우도 많다. 노조는 조직 확대와 교육 사업에 주력하고 있으며 임원은 4명, 집행부는 4명이다.

감시시스템과 연관된 D시스템의 사업장 특성을 보면, 기술 유출 우려는 심할 수밖에 없고, 대부분의 문서에 대외비 표시가 되어 있다. 근로계약서에 비밀엄수 각서가 포함된다. 퇴직 후 동종업계 취업 제한 부분도 있는데 법적 근거는 없다. 업종 특성상 이익률이 매우 높고 직원들이 대부분 젊고 고학력이다. 기술과 자격 등 경쟁 압박이 상존하며 소수 업체를 제외하곤 대부분 50인 이하의 중소규모 사업장이다.

먼저 인터넷 이용 체킹에 대해서는, 개인에 대한 차단 툴은 없지만 웹사이트 접속을 선별 차단하는 업체들이 있다. 큰 회사의 경우 노조 사이트 접속을 (리스트를 가지고) 차단하거나 네트워킹 체킹 프로그램을 설치하여 모니터링 한다. 작

은 회사는 안하는 편이다.

메신저, 메일 체킹은 없지만 회사 네트워크에 연결되어 있는 이상 기술적으로는 언제나 가능하다고 생각하고 있다. 큰 회사에 파견 나가서 일하면 경험하게 된다. 한 조합원은 메일 체킹을 경험한 바 있다. 자신이 사회운동 활동 관련하여 주고받는 메일들이 있는데, 이를 두고 상급자가 "어느 단체에 있느냐"고 추궁하고 주의를 준 적이 있어 깜짝 놀랐다는 것이다. 체킹에 이용한 솔루션은 모르겠으나, 수신 발신 제목 정도는 파악되는 것으로 짐작된다.

관리, 감시 시스템에 대한 의견을 보면, IT산업 노조 차원에서 문제의식은 있으나 대응 관련 활동계획을 갖고 있거나 당면 문제는 아니라고 생각하고 있다. 근기법 적용이나 불법파견 대응이 IT 노조에겐 더 절박하기 때문이다.

하지만 큰 회사 나가서 근무할 때 인터넷 필터링 같은 것은 노조 활동에도 영향을 미친다는 것을 느낀다. 그러나 개별적 대응은 제약이 불가피하다. 또 업무상 불편이 있어도 일정하게 필요한 것 아니냐는 공감이 있는 것도 사실이다. 극단적이고 노골적인 감시가 아니라면 반발이 가시화되기 힘든 것이다. 그래도 인터넷 블로킹이나 필터링은 이해하나, 모니터링이나 가로채기는 용납할 수 없을 것이라 생각하고 있다.

### 4) ERP의 영향

전사적자원관리프로그램(ERP)은 영업 합리화 또는 현대화의 이름으로 매우 널리 확산되고 있지만, 그 이름을 다양하게 붙이고 나타나는 탓에 노동자 측에서는 ERP가 무엇인지 또 도입되고 있는지 자체도 알지 못하거나 사후에 인지하는 경우가 많다. 그리고 ERP가 '노동자 전자감시'를 위하여 개발된 시스템이라기 보다는 '정보 통합 관리를 통한 생산 자원 통제'라는 체계 속에 그러한 측면을 포함하는 것이기 때문에 노동 통제와 노동권 침해가 잠재적으로 존재하는 경우가 많다는 점에서 사례로 뽑아내기 쉽지 않는 것도 사실이다.

아래의 사례들은 그러한 복합적 측면과 함께, 노동조합 측의 대응 여하에 따

라 사측의 ERP 도입 방식과 수위가 변화했다는 점을 보여준다.

### (1) E사

E사는 대표적인 물류 취급 다국적 기업이다. 1988년 OOO사로부터 고용승계 받아 2000년 E사로 창립되었다. 본사는 서울 종로구 수송동에 있고, 전국에 6개의 지방사무소가 있다. 종업원수는 전국을 합쳐 500명 가까이 되며 99%가 정규직이다. 남녀 비율은 7:3 정도다. 주된 작업내용은 항공특송/픽업-딜리버리가 70%, 나머지는 관리 및 영업직이다. CSA(customer service agent)라 불리는 콜센터는 거의 여직원이 담당한다. 작업과정에서 개인용 컴퓨터를 사용하지 않으나, 일과 후 작업 내용과 결과를 전산 입력하는 공용 PC가 사무소마다 4대씩 배치되어 있다.

E사에는 2001년에 노동조합이 조직되었다. 오픈샵이며 가입률은 50% 남짓이다. 노조는 서울 3개, 인천(공항) 1개의 지회가 존재하고, 상급단체는 민주노총 운송하역노조다. 노조 결성 직후 7명이 해고되는 등 어려운 투쟁과정이 있었고 78일간 총파업 경험도 있다. 매년 시한부 파업을 전개해왔는데, 현재는 임단협을 체결하고 노사간 평행선을 달리고 있는 상황이다.

감시시스템과 연관된 사업장 특성을 보면, 노조를 의식하여 두드러진 감시를 하지는 않는 다. 도난 파손 배달사고가 많이 신경 쓰이는 업종이지만. 파업 이후 많은 장비를 도입하여 분실, 파손은 많이 감소했다. 항공물류 업종이 전체적으로 계속 흑자를 기록하고 있어 경영 상태도 좋은 편이다. 외국계 기업이라는 특성을 고려할 필요가 있다.

E사는 다양한 감시 시스템이 부분적으로 설치되어 있다. 인터넷의 경우 정기적 모니터링이나 블로킹은 없으나, 사무직 직원이 인터넷의 개인적 이용과 관련하여 예기치 못하게 관리부서로부터 지적받은 사례 있었다. 전화 송수신 기록도, CSA 부서는 은행 콜센터와 동일하게 통화 모니터링/기록 이루어진다.

파워텔(무전기)이 모든 배송 직원에게 지급되어 활용되는데, 이는 업무용 무전기와 전화기의 기능을 모두 갖춘 것으로 위치 추적 기능이 있으나 지금은 작동

안시키고 있다. 전화의 경우 통화 내용은 모니터링 안되지만 내역은 남고, 무전은 언제든 본사에서 들을 수 있다.

CCTV도 설치되어 있는데, OO동 사무소의 경우 현관, 주차장, 사업장 내 각 2대 등 화장실 빼곤 모든 곳에 설치되어 있고 탈의실에도 입구에 설치되어 있다. 2001년 파업 이후 설치되었고 조그 셔틀로 조망 범위를 바꾸어 볼 수 있다고 한다. 음성 기록은 되지 않는 것으로 파악되는데, 설치 사실을 직원에게 고지한 적은 없다.

전자신분증도 사용하는데, 그 전에 모든 직원에게 있었으나, 파업 때 노조원의 출입을 막느라 모두 무효화시켰다. 이후 새로 이사하거나 만들어지는 지사, 강남지사 같은 곳에 세콤카드(에스원)를 도입하였다. 이 카드가 단순 출입용인지 ID 체크가 되는지는 알 수 없다. 이 카드로 사측에서 출입 권한과 범위를 제한할 수 있다.

E사나 동종 경쟁업체인 UPS, DHL 등 배송회사에 특징적인 것으로 물류와 직원의 배송을 통합 처리하는 스캐너 시스템의 채용이다. 이는 일종의 ERP라 할 수 있다. UPS, DHL은 이미 PDA를 사용하여 실시간으로 작업 처리 내용을 위성 송신하고 있으며, E사는 그 보다 전 단계인 스캐너를 사용하고 있는데 이를 슈퍼트랙커(EST)라고 한다. 슈퍼트랙커는 레이저 스캐너와 처리 정보 입출력 단자를 함께 갖고 있는 일종의 단말기로, E사의 OOO사 때부터 사용되었다.

<참고> E사 배송 직원들의 업무 과정 (일과)

1. 매일 아침 출근하면 유니폼으로 환복하고 파워텔, 트래커, 프린터를 챙긴다.

2. 트래커에 개인 사번과 지역 번호를 입력하고, 하루 일과를 입력하게 된다.

3. 배송지를 이동하거나 물품을 접수, 인계할 때 바코드를 스캐닝하고 미팅, 차량, 지역 이동도 모두 트래커에 기록한다.

4. 일과를 마치면 사업장으로 돌아와 PC에 트래커를 접속하여 그날의 업무 내용을 전송하고 퇴근한다. 이 때 전송되는 업무 내용에는 배달 물품, 시간, 지역, 경로 등이 모두 그대로 포함된다.

미국의 E사 본사는 서비스 품질지수(SQI) 개념을 도입하면서 보다 강화된 작업 과정 관리를 채택하고 있는데, 이는 E사 보다 한 단계 나아간 시스템임을 보여준다.[3)]

E사의 슈퍼트랙커는 1988년부터 도입되었고, 그 간 몇 차례 기술적 업그레이드가 있었다. 먼저 사측에서 제시하는 도입 이유는 직무생산성 제고와 물품의 도난방지, 물품의 위치 추적 통한 고객 서비스 향상 등이다. 면접에 참여한 종업원들도 이러한 취지와 효과에 반대하지는 않으나 직원의 하루 일과가 드러나므로 근로자의 행동 규제 차원이 있을 수 있다고 지적하였다. 한편 트래커에 기록되는 정보는 성과급 등으로 직결되지는 않으며, 1년 단위의 직원 평가 때 일정하게 포함된다. (연단위로 급여수준에 5% 정도 차이가 생김)

피면접자들은 물류 운송업상 특성으로 업무에 필수적이며 효율 면에서도 탁월하다고 생각하는 경우가 많았다. 반면에 트래커 등을 이용하여 일상 업무를 하다보니 스스로 자기 통제를 하게 되는 경향이 있고, 거기에 적응이 불가피하다고 이야기한다. 예컨대 E사 직원들이 다른 회사 사원들보다 '계획적'인 측면이 많다는 것이다. 스케줄이 명확하니까 사생활을 거기에 맞추게 된다.

이와 관련하여 아직까지는 통제, 억압 보다는 자율적인 분위기이므로 트러블

3) "SQI의 측정은 슈퍼트랙커(Super Tracker)라는 휴대용 컴퓨터시스템의 지원을 받는데 그 운영방식은 다음과 같다. 화물이 다른 사람에게 넘어갈 때마다 종업원들은 작은 휴대용 스캐너를 화물의 바코드 위로 갖다 댄다. 스캐너가 읽어들인 정보는 밴트럭에 있는 기기에 입력되고, 여기에 집약된 정보는 800메가 헤르쯔의 전파로 가까운 중계소에 전송된다. 그러면 중계소는 인공위성을 경유하여 멤피스에 있는 거대한 전산센터에 이 새로운 정보를 전달하게 된다. 슈퍼트랙커는 고객 서비스의 평가척도인 SQI의 측정을 가능하게 하고 애초에 창업자가 꿈꾸던 100%의 고객만족에 가까이 다가설 수 있도록 해준다. 1988년 슈퍼트랙커가 도입되기 전에도 이러한 목표를 추구하기는 했지만 여기에 얼마나 근접했는지를 정확하게 알 수가 없었다. 이제는 슈퍼트랙커를 통해 고객서비스를 정밀하게 측정할 수 있다. 슈퍼트랙커는 모든 사람이 고객을 위해 일한다는 패더럴 익스프레스의 이념에 새로운 생명과 활기를 불어넣고 있는 것이다." (출처: 미국본사 홍보문구)

은 없는 편이지만, 스트레스를 받는 것은 사실이다. 감시 받는 게 비가시적이지만 느껴지기는 한다는 이야기다. 예를 들어 업무가 빨리 끝나도 쉬기가 어렵다(자기검열), 스케줄 완수(경쟁)에의 압박감이 있다.

피면접자들은 회사에서 개인을 문제삼거나 개인에 대해 감시하는 것이 아니므로 문제점을 인식하지 못하고 그냥 넘어가게 된다고 이야기한다. 인권 침해나 보호방도 차원에서 구체적으로 떠오르는 것이 없다.

하지만 ERP는 노동자의 생산성을 최대한 짜내는 기능이 있다. 노동조합은 노조의 존재가 ERP의 악용을 막아내는 역할을 한다고 생각한다. 예를 들어 노조가 없던 2000년 3월-5월 사이 E사로 넘어가면서 공항에서 물품과 작업을 스톱워치로 파악하면서 적정 인원과 시간을 상정한 적이 있다. 노조 간부와 평사원 사이에 인식 차이가 있겠지만, 다국적기업 물류회사로서 작업통제 수단화할 상시적 위험이 존재한다고 생각한다. 몇 해 전 노조에서 일본 견학을 간 일이 있는데, 비슷한 유형의 물류회사 직원의 작업 강도가 매우 높고 빡빡하다는 것을 확인하였다.

### (2) F사의 ERP 시스템

학습지 교육업체 F사는 1971년에 창립되었고 서울 봉천동에 본사를 두고 있다. 종업원은 전국적으로 정규직 3천명, 비정규직 1만 6천 명 이상이다. 비정규직은 교사 1만 5천명, 여직원 1천 가량으로 흔히 '눈높이 교사'로 불리는 학습지 교사가 모두 비정규직이다. 교사를 포함한 전 직원 중 남녀 비율은 1:9 가량으로 여성이 압도적으로 많다.

주된 작업 내용은 방문 교육, 교재전달, 영업활동 등으로 학습지를 통한 대표적인 민간 교육 서비스업이다. 외근이 주를 이루지만 2004년부터 진도그래프 입력, 입금, 회원관리 등에서 컴퓨터를 활용한다.

F사 노조는 민주노총 민간서비스연맹 학습지노조로 편재되어 있다. 학습지 교사 중 2-3% 정도가 조직되어 있는데, F사의 노동조합 조직율은 1% (150명) 가량이다. F사의 노사관계는 처음부터 대립적인 편이었는데, 현재에도 조합원에 대

한 탄압과 쟁의가 진행 중이다. 지점별 부당영업행위 대응 투쟁이 이루어지고 있다.

F사는 ERP의 한 형태가 도입되어 있는데, 특히 그 주된 수단인 PDA가 도입된지 1년 가량 된다. 사측에서는 업무효율화 및 회원관리 효율화, 영업 활성화를 이유로 내세우고 있다. F사에서는 2003년부터 전사적인 GWP(Great Work Place) 프로그램을 추진했는데, 이는 ERP와 기업문화를 접목한 형태의 신경영전략이라 할 수 있다.

F사의 ERP 도입시기부터 노동조합의 관심을 끌었는데, 당시 ERP 도입에 대하여 사측은 다음 세 가지를 의도할 것이라 예상되었다. 첫째, 학습지교사들에게 업무를 더욱 많이 부과함으로써 일정한 노동강도 효과를 노리게 될 것이다. 입회관리, 입금관리, 잠재회원관리 등의 업무가 컴퓨터와 인터넷을 통해 네트워킹됨으로써 자본은 실시간으로 모든 정보를 입수할 수 있으며 이에 따른 업무효율성을 기대할 수 있을 것이다. 둘째, F사 자본이 노동자들을 직접 감시 관리 통제할 수 있다. ERP는 기술적 시스템을 통한 통제기제이기 때문에 중간관리자의 역할을 ERP시스템이 일정정도 해낼 수 있게 된다. 예를 들어, 경리, 서무직원, 파트장 등이 하던 업무가 교사들에게 전가되므로 이들 인원의 고용불안이 가중될 수 있다. 실제 ERP를 도입한 많은 사업장에서 중간관리자들의 업무가 필요없게 되어 중간관리자, 현장감독자들이 구조조정의 대상이 되기도 하였다. 셋째, ERP시스템이 인터넷을 통해 관리되는 동시에 교사들에게 PDA를 사용하게 함으로써 누릴 수 있는 감시 통제효과가 배가된다는 점이다. PDA는 GPS시스템을 통해 운영되는데, 이 GPS시스템이 교사의 업무시간은 물론 일상활동까지도 감시해 교사들의 시간과 공간을 통제할 수 있는 위력적인 시스템이 된다. 교사들은 이제 자본에게 일거수일투족을 감시통제 당하는 상태로 전락하게 될 것이다.

F사에서 ERP를 도입하고 2005년에 PDA를 사용하게 하면서 사측이 주장한 것은 첨단기기 도입으로 업무효율성을 제고하고 편리한 영업을 실현하겠다는 것이었다. 하지만 노조에서는 업무표준화를 통한 이익 극대화와 교사의 영업활동 감시가 주 목적이라고 주장한다. 교사를 개별화시키고 회사와 직접 관계를 강화한다는 것이다.

실제로 면접에서 만난 노동자 대표는 PDA 도입으로 인해 발생하는 문제점이 적지 않다고 이야기하였다. 첫째, 과거에 여직원이 하던 업무를 교사에게 전가하여 작업량이 증가했다. 둘째, 감시 통제의 수단으로 사용될 여지가 있다. 셋째, 회원의 주민정보, 월 소득, 은행계좌 등 회원 가족 정보까지 입력하게 되어 개인정보 누출의 우려가 있다. 넷째, PDA를 교사 부담으로 구입하게 하여 부담과 분쟁이 발생하게 되었다. PDA의 과다한 인터넷 사용료에 대한 불만도 많은 편이다.

도입 시에도 ERP 도입 관련 공문을 받은 적은 있으나 세부적인 고지나 협의가 없었고, 2003년 10월경 ERP 도입 저지투쟁이 6개월간 벌어지기도 했다. 노동조합 활동하는 사람들은 2004년 중반 이후 PDA 도입에 대하여 사전 저지투쟁을 벌이고, 구입을 거부하다가 해고 위협을 받고 결국 구입하게 되기도 했다. PDA 도입과 관련한 운영 방침이나 규정 같은 제도적 문제는 논의된 적이 없다.

노조에서는 회사의 이미지를 제고하고 영업실적이 증가하는 효과가 있는 듯이 보이나, 그것은 다분히 외견상일 뿐이라고 주장한다. 오히려 관리비용이 월 10만원 정도 추가 지출되고 업무량이 증가하고, 계약해지와 해고 협박 수단으로 이용되는 등 내부 갈등을 조장한다고 부정적인 입장을 피력하였다. 또한 영업내용이 실시간으로 체크됨으로써 스트레스나 감정 불안이 생기고, 감청에 대한 불안감 때문에 PDA는 통화수단으로 거의 사용하지 않는다고 한다.

애초 PDA 도입시에는 위치파악 기능(GPS)을 탑재하기로 되어 있었으나 비용 및 노동조합 측의 반발로 유보되었으나 언제든지 탑재될 수 있어, 그럴 경우 노동통제가 더욱 강화될 것으로 우려된다.

PDA를 중심으로 한 ERP 시스템에 대한 F사 노동자들의 반응은 몇 가지로 나뉜다. 게 중에서 영업에 더 능력이 있다고 여기거나 개인사업자라는 인식을 갖고 있는 교사들은 PDA에 문제의식을 갖지 않거나 좋아하는 경우도 있다. 어문계열 교사들의 경우 활용도가 있는 편이다. 그러나 실제로 영업 효율성이나 관리 효과가 증대되었는지 의문이며, 도입과 이용이 억압적으로 이루어지고나 계약해지 위협을 빌미로 한 노동통제 수단이 되는 것에는 강하게 반대하는 입장이었다.

### (3) 전북대병원 ERP

전북대병원은 1908년 설립된 자혜의원과 뒤를 이은 도립의료원을 모체로 하여 1975년 2월 1일 전북대학교 의과대학 부속병원으로 출발하였고, 전라북도 전주시 덕진구 금암동에 소재하고 있다. 종업원수는 정규직 1354명, 비정규직 247명이 근무하고 있다. 국립대병원 중 비정규직 간호사가 가장 많은 곳이며, 매년 1,000억원의 수익을 올리고 있는 병원이다.

노조는 민주노총 전국병원노동조합연맹 전국보건의료산업노조 소속이며, 2004년도, 2005년도 보건의료노조 산별 파업에 참여하는 등 조직력이 탄탄한 노조에 속한다.

전북대병원은 지난 2002년, 보건의료노조 소속 160개 병원에서 최초로 ERP 도입하여 여러 논의가 이루어졌다. 이 사업 예산은 12억, 업체는 오라클 코리아가 시행하였다. 2001년 1월, 오라클 측에 ERP 제안을 요청했고, “e-healthcare” 워크샵을 실시한 후 계약을 체결했다. 모델 설계와 개발을 거쳐 2004년에 도입이 완료되었다. 병원 측은 ERP 프로젝트를 통합 "Healthcare Solutions"으로 설명하며, 수익 내는 병원 경영을 위해 오류와 낭비, 수익성 분석 불가한 기존 경영방식을 깨나가야 한다고 주장했다.

당시 병원측이 제시한 도입 이유는 7대 핵심 과제로 제시되었는데, 그것은 1)회계관리 개선 2)원가 관리 구축 3)선진구매 프로세스 구축 4)전략성과 관리 구축 5)진료/연구 데이터 분석 6)의료의 질 향상 7)고객서비스 강화 등이었다.

당시 ERP와 관련하여 갈등이 발생한 이유는 다음과 같다. 먼저 원가분석에 따라 부서별 비용 절감을 경쟁적으로 하게 될 것이고 그 중 핵심인 인건비 절감에 매몰되다보면 인력감축, 비정규직 확대가 자연스럽게 증가할 것이라는 측면에서 노조는 크게 반발하였다. 또한 활동과 근무분석을 하게 되면 업무효율을 이유로 업무 단순화, 다기능화, 지나친 노동강도 강화를 수반하게 될 것이 우려되었다.

개인과 부서별 정보구축, 인사기본시스템(상벌, 학력, 교육, 경력 등등을 데이터화 하게 되면 부, 과, 실별로 인사 발령 및 근태 정보 관리)은 직원 개개인에 대한 감시와 통제 기능과 함께 직원간의 치열한 경쟁관계로 발전할 것이라는 판

단이었다.

아울러 수익창출에 직접 도움이 되지 않는 부서인 행정부서나 치료지원부서는 고용불안을 느끼게 되고, 지나친 물자 절약은 충분한 의료서비스를 하지 못하도록 하는 제약 요건이 될 것이며, 항상 보이지 않는 CCTV의 감시를 받는 것과 같아 직장 내 분위기가 직원간의 협력적 관계가 아니라 상호 경쟁관계로 바뀌게 될 것이라는 우려였다. 보다 근본적인 문제로 환자 정보를 집적하고 공유하게 되는데 만약 정보가 공개된다면 심각한 인권 침해의 여지가 있다는 우려도 있었다.

도입시 노-사간 고지 및 협의는 전혀 없었다. 노조는 도입 초기에 이와 같은 시스템의 도입 사실을 알지 못하다가 2003년부터 대응 준비를 하게 되었다. 2003년 1월 직종별 현장위원, 지부간부, 보건의료노조 전북본부, 보건의료노조 정책국, 노동조합기업경영연구소가 결합하여 '전북대병원 공공성 강화와 ERP 저지를 위한 대응팀'을 구성하였다. 이 대응팀에서 토론회, 부서별 인터뷰, 설문조사, 조사연구를 통해 조합원들에게 ERP에 대한 단점을 설명하였고 결국 노사합의에 도달하게 되었다. 이는 현재까지 ERP로 논란이 되었던 사업장 중에서 가장 전향적인 단협안이라고 볼 수 있다.

<참고> 전북대병원 경영정보통합시스템(ERP) 관련 합의안 (부속합의서)

▲ 병원은 경영정보통합시스템(ERP)을 병원경영을 위한 기초자료로 사용하고, 산출된 자료의 활용범위는 노사합의하여 정한다.

▲ 병원은 경영정보통합시스템(ERP) 자료를 이용하여 직원 인사고과 및 인사상 불이익을 주지 아니한다.

▲ 병원은 경영정보통합시스템(ERP)을 연봉제, 성과급제, 인력감축 등 구조조정의 수단으로 사용하지 아니한다.

▲ 병원은 직원의 고용과 직접적으로 관련된 개인정보를 보호해야 하며 정보활용이 필요한 경우 노동조합과 합의 시행한다.

▲ 병원은 경영정보통합시스템(ERP) 등 병원 전산화와 정보화에 따라

취득한 환자의 개인정보를 보호해야 한다. 단, 기초자료 및 학술·연구 등의 활용은 예외로 한다.

▲ 병원은 향후 전산 및 정보화 관련 기술 도입시 노동조합과 사전 협의하며 직원의 노동조건과 관련된 사항은 노동조합과 합의 후 시행한다.

▲ 경영정보통합시스템(ERP) 운영과 관련하여 실무협의체(각 3~4인)를 구성하고 필요시 진행 경과 보고 및 운영사항을 논의한다.

현재는 노사관계가 무난하고 2003년 노사합의를 한 이후 병원 측도 불신감을 주지 않으려하는 상황이기 때문에 특별한 문제는 없다고 본다. 그러나 노조는 합의서에도 불구하고 마음만 먹으면 언제든지 부서별 원가 확인이 가능하다고 판단한다. 업무성과를 분석한 상태에서 노사관계가 악화된 상황에서 성과급제를 도입하는 자료로 활용할 경우 노동조합에서 대응하기 어렵게 될 것이다. 현재 조합원 대부분은 국립대병원이기 때문에 성과급이나 연봉제를 도입하지는 않을 것이라 생각한다. 그러나 정부지원이 점점 줄어들고, 적자가 늘어나는 상황이며, 조합원들은 근속연수가 늘어 1-2년 후에는 만호봉에 이르는 직원이 60-70%에 이를 것인데 이렇게 될 경우 강도 높은 구조조정과 성과급 도입이 시도될 수 있다는 것이다.

노조는 감시시스템에 대하여 노동조합이 꾸준히 지속적으로 감시하는 것이 필요하다고 생각한다. 노사협의회 등에서 계속적인 점검이 필요하고, 현장에서 어떻게 변화하는지에 대하여 체크해야 한다는 것이다. 또 시스템이 인지하지 못하는 상황에서 서서히 변화 확산될 수 있으므로 현장별로 위원회를 계속 유지하고 점검할 계획이다.

### (4) 광명성애병원

광명성애병원은 1983년 광명병원으로 개원하였고, 1992년에 허가병상이 363병상, 진료과목 19개과로 늘어나면서, 광명성애병원으로 명칭이 변경되었다. 경기도

광명시 철산동에 소재해 있으며, 직원은 624명으로, 이 중 비정규직은 50여명이다.

노조는 민주노총 전국보건의료노조 소속이고, 조합원은 150명 안팎이다. 2002년 노조를 결성한 이후 두차례 파업, 30일, 54일 파업을 진행한바 있으며, 노사관계는 원만하지 못한 상태다.

감시시스템과 연관해서는 ERP 시스템, 스마트 카드, CCTV, 지문인식, 홈페이지 접속 통제 등이 여러 장치가 사용되고 있어 갈등이 다각도로 불거지고 있다.

먼저 지문인식은 출퇴근 시 체크 카드처럼 활용되는데 본인의 사번을 누른후 지문을 대는 형식이다. 스마트 카드는 전자의무기록시스템(EMR)을 도입하기 위하여 불가피하게 공인인증을 위하여 도입해야 하는 것이라는 사측의 주장에 따라 노조가 합의서를 작성하는 수준에서 동의하였다. 스마트 카드 사용은 당초 2005년 9월부터 활용할 예정이었으나 현재 연기된 상태이다. 모든 의무기록을 디지털화하여 저장하고, 진료에 필요한 정보를 공급하는 시스템으로 EMR이 가동되면 광명성애병원은 통합 의료정보를 제공하는 디지털 병원으로 바뀔 것으로 예상된다.

인터넷 이용과 관련하여 사내 업무 중에는 외부 홈페이지를 접속할 수 없으며 오직 인트라넷만을 쓸 수 있다. 노동조합의 경우에는 홈페이지 회선을 별도로 운영하는 대신 내부 인트라넷에 접근하지 못하고 있다.

CCTV는 2002년부터 33개가 설치되었는데 병동마다 설치되어 있고, 큰 병동은 2개씩 설치되어 있다. 병원 측은 환자들의 난동을 감시하기 위해서라고 하지만 노조 측은 노조활동을 감시하기 위한 것이라 보고 있다. 이에 따라 갈등이 격화되었고, 노동조합이 완강히 저항하면서 2002년 노사는 “각 병동의 CCTV 카메라는 간호사실 앞 방향으로 각 층의 사정에 맞게 노사 간에 협의하여 결정한다. 6층 강당의 CCTV 카메라는 노동조합이 집회를 실시할 때에는 미리 폐쇄한다.”라는 문구를 포함한 별도 합의서를 체결하였다.

광명성애병원에서 가장 문제가 된 것은 ERP 시스템이었다. 도입은 2003년경부터 시작되었는데, 사측 관계자의 회사가 병원 실정에 맞는 EMR 등을 개발하여 다른 병원에 판매할 목적을 가지고 적극적으로 프로그램 개발을 하고 있다.

병원측이 주장하는 ERP 도입 목적은 △시스템 표준화를 통한 데이터의 일관성 유지, △ 개방형 정보시스템 구성으로 자율성, 유연성 극대화, △클라이언트-

서버 검퓨팅 구현으로 시스템 성능 최적화, △GUI 등 신기술 이용, 사용하기 쉬운 정보 환경 제공, △재고관리 능력의 향상, △업무의 효율화, △계획 구매 제체의 구축 및 효과적 재고 관리, △인사, 근태, 물품청구, 자재, 회계관리에 이르는 정보 흐름의 일원화, △데이터의 중복 및 오류 배제 등이었다. 요컨대 필요 정보의 공유화로 복잡 다양해져 가는 시대에 충분한 확장성을 보장 받을 수 있으며, 중장기적인 관점에서 비용을 절약하는 효과를 가져올 것이라는 주장이다.

사측은 ERP 도입과 관련하여 사전에 아무런 고지를 하지 않았고, 노조는 도입 초기에 이와 같은 시스템의 도입 사실을 알지 못하다가 2004년 대응준비를 하게 되었다.

2004년 8월 임금, 보충협약을 통해 신기술 도입과 관련, "병원은 ERP, 전산 및 정보화 관련 도입시 노동조합과 사전 협의하며 직원의 노동조건과 관련된 사항은 노동조합과 합의 후 시행한다"라고 합의하였다.

광명성애병원에서도 ERP 시스템으로 인한 대립구도는 명확하다. 병원 경영의 효율화에 도움을 줄 수 있겠으나, 환자의 인권 침해 가능성, 노동통제 강화 가능성이 제기된다는 것이다. 현재까지는 ERP가 휴가처리, 물품신청 수준의 작업만 이루어지고 있어 직원들의 업무량이 증가하였다거나 스트레스를 받고 있지는 않다. 노조는 그것이 아직 ERP가 본격적으로 도입되지 않았기 때문인 것으로 보고 있으며, 이려한 현상이 ERP 구축이 완료되면 어떻게 변화할지 예측할 수 없다고 우려한다. 또 현장의 작업자가 활용하는 수준이 휴가/외근/당직 그리고 구매관리(물품청구) 에 국한되어 있지만 실제로 인사파트나 기획 파트에서 어떠한 추가적인 작업이 입력되고 있는지는 전혀 알 수가 없는 상황이다.

노조는 감시시스템에 대하여 노동조합이 꾸준히 지속적으로 감시하는 것이 필요하기는 하지만, 전문적인 영역이라서 잘 모르는 부분이 많고, 막연히 걱정은 하고 있지만 뚜렷한 대응 방안이 없다는 고충을 피력하였다.

### 5) RFID 카드로 인한 분쟁

일반적으로 RFID의 활용 중 가장 대표적인 것은 대형 유통점에서 창고관리와 매장관리의 편리성을 도모하고자 물품에 태그를 부착하는 정도이다. 외국의 경우 대형마트에서 RFID를 부분적으로 사용, 유통경로 추적을 하고 있으며, 국내 일부 기업에서도 제품 재고관리와 정산시스템의 일환으로 RFID를 시범 적용하고 있는 것으로 알려졌다.

그런데 2004년 삼성전자 탕정공장에서는 이를 사람에게 직접 부착한다는 의혹이 제기되어 언론에 보도된 바 있다. 탕정 공장에서 일하는 한 직원의 경우 공장 정문을 통과하면서 사원카드 안에 부착된 RFID카드가 작동을 시작하고, 이와 동시에 이 직원의 행동 하나하나가 컴퓨터 화면을 통해 확인할 수 있다는 것이었다. 이는 사원번호, 주민번호만 입력하면 이 직원이 몇 시에 출근했으며, 또 어디로 가고 있으며, 현재 위치한 직원까지 소상히 알 수 있다는 것을 의미한다. 사람과 차량에 RFID를 부착하는 것은 심각한 프라이버시 침해로 결국 이것이 직원들의 감시와 통제로 이어질 경우 심각한 폐해를 낳을 수 있다는 이유로 노동계에서는 우려했다. 하지만 삼성전자 측은 RFID 기술력은 아직 미비한 수준으로, 직원들의 RFID 부착 감시 운운은 억측이라고 주장한 바 있다.

#### (1) G사

G사는 1975년 설립되어 영광3,4호기, 울진3,4호기 원자력발전소를 설계하였으며, 현재 북한 신포에 건설중인 KEDO 원자력발전소를 비롯하여 영광5,6호기 및 울진 5,6호기 원자력발전소의 설계를 독자적으로 수행하고 있다. 본사는 경기도 용인시에 소재해 있고, 직원은 1910명(본사는 1400명)이다.

노조는 1987년 설립되어 민주노총 공공연맹 환경에너지분과에 소속되어 있다. 조합원 수는 1200명 정도이고 노조체계는 본조만 있다. 노사관계의 성격은 대결적인 편으로 주로 정부의 일방적 지침에 기인하는 문제들이다. 1998년 IMF사태 이

후 정부의 획일적 구조조정에 맞서 투쟁해 왔고, 당시 회사는 플랜트 사업단을 매각(사유화) 의도했고, 이 과정에서 111명이 정리해고 되고 151명이 회사 내 자회사로 분사되었다.

2000-2002년, 정부의 30% 일률 인원감축 지침으로 지속적인 구조조정 압박이 있었고, 부분파업 등으로 지속적 투쟁 전개했다. 2002년 12월에 와서야 임금 최초로 노사 합의에 이르렀다. 지금은 '전력연대'와 함께 주5일 근무 단일한 공동요구, 배전분할매각 철회 및 발전매각 철회, 정비부문 경쟁도입 반대 등 공동투쟁 전개하고 있다.

G사에서 문제가 되었던 것은 출입통제 시스템의 설치와 관련한 일련의 노사 갈등이다. 사측의 2004년 구매시방서에 따르면 품명은 "출입통제 시스템"으로, 한전기술의 "정보유출 방지 및 시설보안을 위한 출입관리 시스템에 적용한다"고 되어 있다.

이 시스템은 회사 자체 감사에서 시간외근무(OT)가 제대로 체크되지 않으니 이를 해결할 방안을 검토할 것이 주문되었고 이에 따른 후속조치라는 노조 측의 주장이 있고, 이에 대해 회사 측은 잡상인 출입을 막고 보안을 유지하기 위한 목적이라고 주장하였다.

당시 사측은 "기업정보 유출 방지책 강화와 허가된 출입자 이외의 불필요한 방문객의 출입을 통제해 보다 안전하고 쾌적한 근무환경 조성 및 외부로부터 기업 이미지 향상에 기여하고자" 한다며 출입관리시스템의 설치 이유를 밝혔고, 이에 반해 노조는 "보안강화용이라면 전 직원에 대한 통제가 아닌 방문자 출입통제만 하면 된다"며 "직원들의 출퇴근 시간과 OT(시간외 근무) 관리 등 근태관리를 위한 시스템이 분명한데도 회사는 시스템 설치에 대해 노조와 단 한마디도 논의한 바 없다"고 주장했다.

노조가 사측의 주장을 신뢰하지 않은 이유는 같은 시방서에 명시되어 있는 내용 중 특히 인사DB 연동, 개인 출입정보 수집을 시스템의 필요조건으로 요구한 부분 때문이었다. 시방서의 "운전 및 설계조건" 항목에, "서버컴퓨터는 출입통제와 감시, 인사DB 연동 및 방문객 관리 기능을 수행할 수 있도록 24시간 운영"이 가능해야 하며, "출입자, 출입방법, 출입시간, 출입지역, 콘트롤러 및 카드리더기

등 장비와 운영에 필요한 자료의 등록 및 편집, 수정기능이 있어야 한다"고 명시되어 있었다.

<표 3-5> G사의 Lock, 센서, Gate, 리더기 설치 수량

| 구분 | 위치 | 출입문 Lock (센서리더기) | E/V앞 (카드리더기) | 차량바 (Gate) | 자동문 (카드리더기) | 플랩 Gate (카드리더기) | 계 |
|---|---|---|---|---|---|---|---|
| 본사 | 지상1층 | 2 | | 1 | | Gate : 6개<br>리더기:10개 | 13 |
| | 지하1층 | 2 | 2 | | | | 4 |
| | 지하2층 | | 2 | | | | 2 |
| | 지하3층 | | 2 | | | | 2 |
| 별관 | 지상4층 | 2 | | | 자동문 1<br>리더기 3 | | 5 |
| | 지상5층 | 2 | | | 자동문 1<br>리더기 3 | | 5 |
| | 지상6층 | 2 | | | 자동문 1<br>리더기 3 | | 5 |
| 합계 | | 10 | 6 | 1 | 9 | 10 | 36 |

2005년 1월 열린 G사 2005년도 제2회 경영회의 문건에서도 '회사 보안강화를 위한 출입자관리시스템 설치 공사'에 대해 '회사정보 유출 방지 및 출입자 관리 강화'가 목적이라고 밝히면서 '실제 OT 수행여부 Check 기능 추가 필요'라는 내용을 첨부하고 있다. 그러나 회사쪽 실무자는 "사생활에 관련된 인사 DB와는 연결돼 있지 않다"며 "다만 한전기술 직원임을 확인하기 위해 인사 DB에서 이름과 사번만 빌려온 것일 뿐 출입자관리시스템의 통계 자료를 인사팀에 넘겨준다거나 근태관리를 하는 것은 소관사항이 아니"라고 밝혔다.

G사의 출입통제시스템은 2005년 2월, 일요일 저녁 시간에 사측에 의해 설치되었고, 도입대수와 개소는 다음과 같다. 본사와 별관을 합쳐서 게이트, 리더기 등 36개의 장치가 설치되었다.

카드는 총 3000여개가 제작, 배포되었고 협력업체 직원까지 포함하여 사원증 겸용으로 이용된다. 카드에는 이름, 사번(5자리), 주민번호, 바코드가 기록되어 있고 RFID칩이 장착되어 있다. 카드는 출입시간과 통과장소 기록 외에, 식사비 결재에도 쓰인다. 하지만 그것은 바코드 리더기를 통하여 일괄 정산하는 것이고, 카드 자체가 결재통장에 연동되어 있는 것은 아니다.

노조는 출입시스템이 도입되지 마자, 노조 자체의 판단으로 개인정보 보호에 문제가 있고 시간외근무 체크를 통한 노동통제 수단으로 남용될 것이라 생각하여 반대 투쟁에 돌입했다. 먼저 노조는 출입자관리시스템이 설치되기 시작한 1월 24일 정문 앞 철야농성을 진행하다 28일 이 시스템과 관련 노사협의를 진행키로 하고 농성을 풀었다. 그러나 1월30일부터 2월24일까지 진행된 노사 실무협의에서 노조가 요구한 △개인들의 출입에 관한 이력관리 및 인사 DB와의 연동 중지 △이 사항에 대한 사장과 노조위원장간의 합의서 작성 및 단체협약 반영을 사측에서 받아들일 수 없다고 밝혀 25일 협상이 결렬됐다. 이에 사측은 27일 출입자관리시스템의 잔여 공사를 강행, 2월 3일부터 시스템을 작동했으며 이후 노조 사무실로 장소를 옮겨 3개월 가까이 농성을 진행하였다. 노조가 농성을 시작하면서 플래카드를 부착하자 사측에서 제거하고, 이에 대해 도난 신고를 하는 등 해프닝이 벌어지기도 했다.

다수의 조합원들이 이 출입시스템은 노동자 감시를 의도하는 것이며, 수용할 수 없다는 의식을 가졌고, 노조에서는 수용할 수 없음을 명백히 밝혔다. 만약 회사의 주장대로 설치가 필요하다면 보안상 문제가 있는 중요한 자료실이나 임원실, 잡상인이 들아가서는 안되는 곳에만 제한적으로 하면 될 것이라고 주장했다. 이 사안을 가지고 조합원 총회도 개최했는데 80% 이상이 출입시스템을 없애야 한다는 의견을 밝혔다.

노조는 2005년 단협안에 “회사는 출입자 인증시스템 운영과 관련하여 인권보호에 관한 제반 법규를 준수하며 이를 직원 개인의 사생활을 침해할 목적으로 사용하지 않는다”와 “회사는 출입자인증시스템을 외부출입자 통제와 보안강화 목적 이외의 목적으로 사용하지 않는다”, 그리고 “회사는 향후 출입자인증시스템의 변경, 추가 등의 경우 노사합의 하에 시행한다” 등의 문구 삽입을 요청하였고, 오랜

논의 끝에 2005년 12월 체결된 임단협에서 출입자 통제시스템은 보안 목적 이외에는 활용하지 않는다고 적시하게 되었다.

현재 게이트를 옮기거나 폐쇄한 것은 아니지만, 시간외근무 등 인사와 연동은 안하고, 단순한 직원 출입통제 기능만 하고 있다. 시간외 근무의 경우, 필요하면 근태관리자가 시간외근무 시행을 명령하고 동의한 사람에 대해서만 실시하며, 그 내역은 관리자가 전산 입력하는 방식으로 처리하고 있다.

단협을 통해 갈등이 일단락되기는 했지만, 출입시스템의 영향은 여전하다. 예를 들어 직원들이 차를 같이 타고 회사로 들어올 때 지하주차장을 통과하면서 카드를 찍으면, 운전사는 기록 남는데 동행 직원은 이력이 남지 않기 때문에 막연한 불안감을 느끼게 된다. 인사 정보와 연동되지 않는다고는 하지만 불안감 때문에, 주차장에서 올라와 개인별로 엘리베이터 앞에서 카드를 찍는 것이다. 출입통제시스템이 잠재 심리 속에 감시 기제로 작용하고 있음을 알 수 있다.

출입 편의와 관련해서는 별관은 원래 잡상인이 많아 불만이 적은 편이나, 본사는 출퇴근 및 점심시간에 게이트에 사람이 몰려 출입 시간이 오래 걸리는 불만도 빈발한다.

가장 큰 문제는, 비록 회사가 단협을 통해 보안 외 목적에 사용하지 않는다고 약속하기는 했으나, 카드에 어떤 수준의 정보가 수록되고 어떻게 DB에 축적되는지 하는 것을 알 수 있는 정례적인 회의나 규정 같은 장치가 없다는 것이다. 이러한 문제를 노조도 인지하고 있으나, 변호사의 자문에 의하면 단협을 통한 약속이 위반되거나, 출입통제 시스템에서 기인한 조합원의 불이익이 생겼을 경우에만 사후적으로 문제삼을 수 있다는 해석이다.

### 6) 전화 통화 녹취

전화 송수신 기록과 통화 내용 녹취는 공개적으로, 상호 인지 속에 이루어지는 관리 방식이다. 금융권 콜센터가 대표적이지만 최근에는 전자상거래나 홈쇼핑 사업이 팽창하면서 더욱 많은 곳에서 통화 녹취가 이루어지고 있으며, 아날로그

기록에서 하드디스크 레코딩으로 바뀌면서 기록 용량도 더욱 커지고 편집, 이용도 훨씬 간편해졌다.

전화 통화 녹취는 관리자 측뿐 아니라 노동자 측에서도 필요성을 공감하는 측면이 있고 상호 동의 하에 이루어진다는 점에서 여타의 전자적 노동감시 기술과는 다른 성격을 갖는다. 그럼에도 불구하고 사례에서 드러나듯 노동 통제와 감시의 속성을 갖는다는 점, 그리고 녹취의 범위와 이용의 범위에 관한 명확한 규정이 없다는 점에서 작업장에서의 갈등 가능성과 인권 침해의 가능성을 안고 있음을 알 수 있다.

### (1) H은행 콜센터

H은행의 콜센터는 40명 규모의 고객만족센터로 운영되던 것이 2002년에 200명 규모의 고객센터로 확장되었다. 소재는 서울 을지로 본점에 같이 있다가 2005년 8월 경기도 용인시 동천동으로 이전하였다. 전체 직원은 270여명 가량이다.

고객센터는 전체 관리와 책임을 맡는 팀장이 있고, 가장 말단에 상담원이 있으며, 상담원 8명당, 리더 1명(상담근무도 참여함), 리더 3명당 파트장 1명이 있고, 파트장은 10명이다. 파트는 인바운드 7개, 아웃바운드 2개, 대출상담 1개, 업무지원팀 1개로 구성된다. H은행 고객센터가 규모가 큰 편이고 이직율도 낮은 편이다. 평균 근속연수는 1년 6개월 가량으로, H은행 고객센터가 다른 은행에 비해 근속연수 긴 편이나 용인시로 이전하면서 출퇴근 문제 등으로 퇴사자가 많았다. 입사는 아는 사람 소개를 통하여 시험을 보아 하게 되는데 경쟁률이 높은 편이다.

파트장까지 모두 여성이며, 팀장은 남성이 많다. 1년 단위로 재계약을 하는 계약직(비정규직)인데, 그로 인한 고용불안이 심각하지는 않으나 내년부터는 하위 20%에 속하면 재계약 않는다는 방침이 전해지고 있다. 주된 작업내용은 파트별 전화 상담 안내로, 인바운드 파트가 선호되는 편이다. 직무순환도 소폭으로 이루어진다. 근무시간은 오전 9시부터 오후 6시이며, 점심시간은 1시간 2교대, 팀별로 휴식 및 교육 계획표가 있다.

개인당 1인 1대 혹은 2대의 컴퓨터가 있다. 모든 것이 컴퓨터와 전화를 통해 이루어지므로 필수적이다. 하지만 개인 인터넷은 사용 불가하며, 한글(워드) 정도만 필요한 사람들에 한해 설치되어 있다.

노사관계를 보면, 정규직 노조는 한국은행 금융노조 소속이나, 비정규직은 노조나 협의회가 따로 존재하지 않는다. 고객센터 책임자(정규직 대표)가 노사 협의에 참여하여 간접적으로 발언하는 형태다.

고객센터의 컴퓨터는 인터넷 개인 이용 자체를 할 수 없도록 (방화벽) 되어 있다. same-time 이라는 행내 메신저가 있는데, 이것도 업무 지장을 우려로 관리자는 안좋아하여 비공식적으로 사용한다. 고객센터 내에서 상호 쪽지를 주고 받을 수 있다. 그리고 직원은 출입카드(RFiD)를 모두 갖고 있는데 여기에는 개인 고유 ID가 포함되어, 식비나 주차 결재 기능도 갖고 있다.

고객센터에서 가장 특징적인 것은 전화 송수신 기록으로 센터 내 상담서비스망을 통한 모든 통화가 녹취된다. 녹음이 안되도록 개인 통화를 하려면 로그-아웃 하면 되지만, 로그-아웃은 출퇴근처럼 계산되므로 안하게 된다. 녹취된 내용은 10분 정도 뒤에 관리자도 들을 수 있고, 민원 통화 중일 때도 파트장은 실시간으로 모니터링 할 수 있다.

녹음 자료의 활용은 주로 QA(quality assurance)를 통해 이루어진다. QA 평가가 한 달에 한 번 있는데, 한달 중 상담원이 수행한 통화 중 3개의 콜을 랜덤 추출하여 녹취, 평가하는 것이다. 이 때문에 통화를 매우 긴장하여 주의깊게 하게 된다. 인사에 연동되는 것은 QA 20%, 정기적인 시험 20%, 생산성(콜수, 시간) 40%, 기타(근태 등) 20%로 합산하며, 3개월마다 종합 평가하여 최고 30만원 정도 급여 차이가 난다.

통화는 하드 레코딩하여 CD 자료로 보관되는데 보존, 폐기 연한은 분명치 않다. 아직 버리지 않고 모두 모아두고 있으며, 전화 송수신 기록에 대한 공식적 사용방식이나 관련 규정 같은 것은 사측으로부터 설명 들은 적 없다.

전화 송수신 기록의 도입 이유는 무엇보다도 모니터링/증빙 자료가 된다는 것이다. 고객에게 정확, 친절하게 상담하는지, 오상담은 없는지 하는 것이 은행 고객센터에게는 매우 중요하기 때문이다. 일례로 민원 발생시 직원-고객 간에 발언

을 대조할 필요가 생긴다. 은행 업무상 한마디로 많은 돈이 왔다 갔다 할 수 있는 경우도 있다.

직원 교육자료로 활용된다는 점도 중요한 기능이다. 상담원의 실수에 대해 바로 정정해주기 때문에 긴장하게 되며, 송수신 내용 청취를 통해 고객의 needs를 파악하고 컴플레인 콜에 대한 대응법을 개발하여 교육하게 된다.

직원의 입장에서도 송수신 녹취는 필요한 측면이 크다고 한다. 우선 QA 점수로 반영되어 스스로를 모니터링하여 자신의 업무 방식을 개선할 수 있다. 즉각적인 모니터링과 정정 지시에 직원이 고마워하는 경우도 많다고 한다. 또 직원 입장에서 고객의 폭언이나 민원 발생시 업무방해를 증빙할 수 있는 법적 자료가 된다. 소위 '블랙리스트' 고객에 대한 대처도 가능해진다.

전화송수신 기록장치의 도입으로 인한 트러블이라 할만한 것은 없었고, 업무 중 개인 사생활이 보장 안되니까 위축되거나 회의감이 드는 경우는 있다. 특히 신규/초년 직원들에게 그런 경우 있다. 한편 고객에게 (녹음 기록으로 인해) 자신이 다칠까봐 함부로 대화 못하게 되고, 고객도 녹취사실을 알고 발언하는 경우도 빈번하다.

피면접자들은 전화 기록에 대하여, 모든 통화가 녹음되기 때문에 감시라 할 수 있고, 개인전화를 많이 쓰는지 알 수 있으므로 근태관리 측면이 있다고 인정한다. 예를 들어 30분 이상 통화하거나 같은 번호로 통화를 여러 번하면 구두 주의가 주어진다. 3진 아웃제라고 해서 민원을 유발하거나 콜을 조작하거나 하면 시말서를 쓰게 되는데, 시말서를 3번 이상 쓰면 재계약에서 제외하는 제도가 있다.

그리고 누군가 자신의 통화를 다 듣는다는 것이 유쾌한 일은 아니지만 입사시 알고 들어왔으므로, 또 필요한 측면이 있다고 생각하므로 크게 개의치는 않는 분위기다.

### 7) 생체인식 기술과 노동 통제

생체인식 시스템은 확산 속도가 점차 빨라지고 있다. 이미 우체국, 관공서, 군부대 등 공공분야는 물론 금융권, 일반 기업까지 생체인식을 이용하는 곳이 속속

늘고 있다. 아파트단지에도 거주민 출입 인증을 위해 생체인식을 이용하는 곳이 많아졌다.

2003년을 전후로 시간외근무 수당과 연관하여 전국 관공서 여러 곳에 지문인식기가 설치되면서 생체인식 기술의 인권 침해 문제가 본격적으로 논란이 되기 시작했다. 그런데 지자체 공무원의 시간외근무 기록은 사례에서 살펴보는 강남구청 외에도 모든 지자체에 해당하는 사안이므로, 어떤 방식이든 전자 기록 시스템이 도입되고 있으며 그에 따른 갈등도 빈발하고 있다. 공통적으로 시간외근무의 성격과 체크 방식에 대한 갈등이 상존하고, 생체정보 제공과 활용에 관한 동의나 규정이 존재하지 않는 등 인권침해 요소가 존재하며, 기술적 문제점도 드러나기 때문이다.

서울시청은 2003년 1월 직원들의 시간외 수당 점검용으로 지문 인식기를 설치해 사용했다가 인권침해 소지가 있다는 직원들의 반발에 따라 올해부터 사용하지 않고 있다. 서울시청 역시 도입 당시 생체정보 제공 동의서 같은 것이 없었고 시청에 의해 일방적으로 설치되었다. 서울시청 공무원직장협의회에서 항의하며 서울시장과 협의를 한 끝에 지문인식기는 2005년에 철거되고, 시간외근무는 자기 고유번호 네 자리를 입력하는 식으로만 체크하게 되었다. 서울시청은 내년부터 개인카드를 도입할 예정이다.

서울 마포구청도 본청과 동사무소 등 24곳에 28대의 정맥인식기를 설치하였으나, 현재 거의 사용하지 않고 있다. 초과근무수당 지급방식이 예산의 범위 내에서 균등지급하는 방식으로 바뀌어서 필요성이 없어졌기 때문이다. 결국 시간외 근무수당이라는 논란 많은 제도 때문에 지자체 집행부와 일선 직원들 사이의 불신과 갈등을 빚어내고, 무원칙한 생체정보 이용이 이루어지고 있는 상황이다.

### (1) 서울 I구청

서울시 I구청에는 산하 동사무소까지 포함하여 총 1338명의 직원이 근부하고 있으며, 이 중 전국공무원노조 I구청지부 소속 조합원은 579명이다.

이중 지문인식 대상은 초과근무수당(OT) 지급 대상인 5급까지의 공무원 전체에서 원격지 근무자(청소과, 재활용 차량기지 등)와 간부 등 100여명을 제외한 나머지이다.

지문인식 시스템 도입은 감사원의 감사와 직결된다. I구청은 시간외 수당의 부정 지급 문제로 감사원으로부터 세 차례 지적받은 바 있다. 직원들이 일과시관외 시간외 근무를 대리 체크하거나 위장 기입하여 부당하게 수당을 타내는 경우가 있으며, 이를 막을 수단이 강구되어 있지 않다는 것이었다.

그 때까지 시간외 근무시간 체크는 구청은 개인카드(ID 카드)를 이용했고, 동사무소는 수기 대장에 기록하는 식이었다. 감사원이 대안 마련을 요구했고, 구 집행부는 지문인식기가 가장 효과적이라고 판단하여 도입하게 된 것이다.

구청 공무원의 기준 근무시간은 오전 9시에서 오후 6시까지(점심시간 제외 8시간)이고, 오전 8-9시, 오후 6-8시 사이는 출퇴근 및 정비시간으로 근무시간에 포함되지 않는다. 때문에 구청 직원들이 시간외 근무 시간으로 인정받기 위해서는 오전 8시 이전에 일찍 나와 근무하고나 오후 8시 이후 자정까지 근무하여 그 시간이 기록되어야 한다.

지문인식기는 본청에 3대, 구의회에 1대, 관내 동사무소에 각 1대가 설치되어 있다. 시간외 근무에 해당하는 오전 8시 이전 또는 오후 8시 이후 직원이 직접 인식기에 네 자리 비밀번호를 입력한 후 손가락을 접촉하여 체크하는 방식이다. 구의회에서 설치비용 관련 예산안을 통과시켰고, 기기 단가보다 프로그램 비용이 큰 편이다.

도입은 2004년 2월에 되었고, 구청의 각 과별로 업자와 담당직원이 함께 돌아다니면서 기기에 지문을 입력하도록 했다. 아무 손가락이나 지문이 잘 나오는 손가락을 1개 입력토록 했다. 지문인식 입력을 실시한다는 시행공문은 있었으나 생체정보 제공과 관련한 동의서나 정보 활용에 관한 약정서는 없었다. 신규직원은 구청 총무과에서 지문을 입력하고 고유번호를 부여받는다.

지문인식기와 관련한 불만은 우선 시간외 근무가 당연한 것이 되다 보니 가정생활이 제대로 되지 않는다는 것이다. 한 사람이 찍을 수 있는 초과근무 시간은 한 달에 총 67시간인데, 이를 다 하면 40여 만원을 더 받게 되므로 초과근무 수당

은 직원들에게 매우 큰 비중으로 여겨질 수밖에 없다.

그런데 공무원노조의 주장에 따르면, 시간외 근무 수당은 초과근무 보상이라기 보다는 사실상 생계비 보조분으로서의 성격을 갖고 있다고 한다. 김대중 정부 때 열악한 공무원봉급을 일반 기업의 90% 수준으로 인상해 주기로 하고, 그 방편으로 도입되었다는 것이다.

그래서 노조는 구청 집행부가 지문인식기가 시간외수당을 통해 직원을 통제하는 수단이 되고 있다고 생각한다. 시간외수당 문제가 워낙 큰 관심사이다 보니, 직원들의 다른 불만이나 애로사항은 부차화되고 희석된다는 것이다.

다음으로, 인권 침해 소지의 문제다. 직원들은 "교도소도 아닌데 지문을 찍느냐"며 거부감을 표시하는 경우가 잦다. 정맥인식기를 설치하는 지차체 관공서들도 있는데, 그것은 지문인식에 비해 거부감이 덜하기 때문이기도 하다. 하지만 에러율은 지문인식에 비해 정맥인식이 높다.

하지만 지문인식기에 대한 직원들의 불만은 인권침해 부분이 30% 정도라면, 업무 효율을 담보하지도 못하면서 공연히 시간만 때우게 하는 시간외근무 체제 자체에 대한 것이 50% 정도라고 할 수 있다.

지문인식기의 오류나 사용 불편에 대한 불만도 있다. 체온도 같이 감지하기 때문에 추운 날씨에는 제대로 인식이 안되는 경우가 잦고, 20여분을 시도해도 인식이 제대로 안되어 홧김에 지문인식기를 파손한 직원도 있었다.

이러한 문제들과 관련하여 노조와 구청은 이제까지 세 차례의 협의를 진행했다. 2004년에 1차 협의를 하여 단체협약서에 "시간외근무를 측정하기 위한 현재의 지문인식 방법은 기계오작동 등 문제점이 발생되고 있으니 이를 2004년 9월 중 새로운 시간외근무 시간측정 방법으로 개선토록 하고 개선시에는 을(노조)과 사전 협의하여 추진한다"고 명시하였다. 하지만 공무원노조가 아직 법제화되지 않아 단체협약이 강제사항이 아니며, 시행되지 못했다. 당시 노조의 요구는 지불기능이 있는 스마트카드로 대체하자는 것이었는데, 통장과 연계되므로 직원들끼리 대여 가능성이 없어서 감사원의 요구를 충족할 수 있으면서 인권침해나 이용불편의 문제를 해결할 수 있다는 것이었다. 하지만 비슷한 시기에 공무원들의 시간외근무 수당이 편법으로 지급되고 있다는 언론 보도가 몇 군데에서 나오면서 여론이 좋

지 않아졌고, 구청도 지문인식기를 다른 방식의 시스템으로 교체할 필요성에 동의하면서도 협약 이행을 보류하게 된 것이다. 노조는 2005년의 협약서에도 동일한 내용을 포함하여 구청과 협의를 시도하고 있다.

## 3. 요약 및 함의

실지조사를 통해 살펴본 사례들은 몇 가지 유형으로 구분되었다. 우선 노조활동에 대한 탄압이 전자감시 시스템을 통해 더욱 증폭된 경우들로, 사용자들은 CCTV에서 위치추적(GPS)에 이르는 다양한 기술적 수단을 이용하여 매우 전방위적인 감시를 행하고 그에 따른 갈등과 충돌도 격렬히 일어났다.

CCTV의 사용을 보여주는 사례에서 관리비용의 절감이라는 이점과 사회적 견제 장치의 부재 속에서 사용자 측에서는 아무런 문제의식 없이 CCTV를 과용하는 경우가 많으며, 노동자 측에서도 그것을 당연한 것으로 생각하는 경향이 있다는 것을 알 수 있었다. 현행 법제도 내에서도 허용될 수 없는 설치 및 이용의 경우가 다수 발생하지만 이에 대한 환기는 이루어지지 않고 있다.

인터넷을 업무에서 반드시 사용하게 되는 IT업종의 직원 감시는 그러한 규범과 기준이 존재하지 않는 가운데 더욱 광범한 문제를 일으킬 가능성을 보여주었다. 첨단 기술을 사용하는 업종일수록 사용자의 경영권과 노동자 인권 사이의 대립을 제어할 수 있는 사회적 기준을 설정하고 적용할 필요성이 크다 하겠다.

전사적 자원관리프로그램(ERP)은 '노동자 전자감시'를 위하여 개발된 시스템이라기 보다는 생산 자원의 효율적 통제를 목적으로 한 것이지만, 현실 속에서는 노동강도 강화와 노동 통제 수단으로 작용하며 이에 대한 노동자의 반발도 빈발하고 있었다. ERP의 사례에서 또 하나 눈여겨 볼 것은, 노동자의 대응 여하에 따라 기업 측의 도입 방식과 수위가 변화할 수 있다는 것이었다.

전화 통화 녹취는 노사 상호간의 필요에 의해 이루어지는 경우에도 녹취의 범위와 이용의 범위에 관한 명확한 규정이 없다는 점에서 작업장에서의 갈등 가

능성과 인권 침해의 가능성을 안고 있었다. RFID 카드를 이용한 출입통제 시스템과 생체인식 시스템 역시 빠른 확산 속도에 비해 개인정보의 취득과 활용에 대한 기준이 사회적으로 존재하지 않음으로 해서 불필요한 노사 간 대립과 인격 침해의 가능성을 제공하고 있다.

이상에서 얻을 수 있는 공통적 함의는 다음과 같다. 첫째, 전자감시 시스템이 갖는 인권 침해와 노동권 침해의 가능성에 대한 인식이 노사 모두에게 부족하였다. 기업 측에서는 재산권과 기업 자원 보호라는 명목으로 별다른 문제의식 없이 감시 시스템을 채용하며, 첨단 기술에 해당하는 것일 수록 인격적 측면에 대한 민감성이 작용하지 않는 모습을 보인다. 이는 전자감시와 노동권에 대한 사회적 감수성을 전반적으로 끌어올릴 필요성을 보여준다고 하겠다.

둘째, 현행 법상으로 문제가 되는 경우에 있어서도 전자감시 시스템이 제어받지 않은 가운데 남용되며, 중소규모 사업장일수록 그리고 노동조합이 조직되어 있지 않거나 미약한 사업장일수록 그러한 경향은 더욱 두드러지는 것으로 나타난다.

세째, 노동조합의 대응 여부, 그리고 사용자의 이해와 노력에 따라 전자감시 시스템의 도입과 활용의 수위와 방식은 매우 달라질 수 있음을 알 수 있었다. 결국 노동자의 조직력이 취약한 부문과 업체에서 더욱 빈발하는 노동권 침해를 막기 위해서라도 보편적으로 적용될 수 있는 가이드라인과 제도적 장치가 강구되어야 한다.

네째, 이러한 장치는 구체적인 법제도로 제시되고 강제적으로 적용될 필요가 있다. 감시장치를 둘러싼 분쟁 끝에 단체협약이나 상호 협의를 통한 문서로 감시 시스템의 한계와 이용 절차를 규정한 경우도 매우 유의미한 것으로 나타난다. 하지만 전자감시 시스템에 대한 사회적 규제는 이를 우선 보편적으로 적용하고 이를 사회적 통념으로 끌어 올릴 수 있는 장치는 강제적 법제도와 비강제적 가이드라인, 개별 사업장의 노사 간 협의 등 중층적으로 구축될 필요가 있다. 그 적절한 방식과 내용은 현행 법제와 국내 여건을 감안하여 구체화되어야 할 것이다.

# 4장. 조합원 설문조사

## 1. 조사의 개요

본 조사는 전자 노동감시 기술의 사용 실태와 이에 대한 현장 노동자의 인식을 알아보고 전자기술에 대한 규제의 필요성 및 대안에 대한 의견을 파악함으로서, 향후 우리 사회가 전자 감시기술에 대한 대책을 마련하는 근거로 활용하고자 이루어졌다.

조사를 위해 사업장 감시시스템이 많이 도입됐다고 기존 연구에서 알려진 대표적인 산업부문인 △제조, △공공, △금융, △판매서비스, △보건 부문을 대상으로 설문지를 배포하였다. 원활한 설문지 배포 및 수거를 위해 한국노총과 민주노총 양대 노총에서 제공한 사업장 리스트에서 해당 연맹 산하 단위노조를 무작위 추출하여 각 노조별로 3명씩 할당하여 배포하였다. 설문지 배포 부수는 민주노총 981부 한국노총 1021부이며, 총 수거 부수는 204부로 수거율은 10.2%였다. 수거된 설문지는 SPSS+를 사용해 분석하였다.

연구의 주제가 민감하여 사업장 접근이 어려웠고 결과적으로 설문지 수거율이 낮았다. 노동조합을 통하지 않고 개별 사업장을 접근하여 전자기술에 대한 설문지를 배포, 수거하는 것은 제한이 있어 노동조합을 통해서 할 수 밖에 없던 한계를 지니고 있다. 또한 정해진 연구기간으로 인해 설문지 배포 시기가 제한적이었는데 설문지 배포시기가 단위노조 및 연맹의 활동이 적극적으로 이루어지던 시기였던 것도 설문지 수거가 원활하지 못한 이유로 작용했다.

설문지 수거의 한계에도 불구하고 통계적으로 유의미한 분석을 위한 대상자 규모는 충분하며, 전자감시기술에 대한 노동자의 인식 파악과 향후 정책적 방향을 설정하는데 큰 무리가 없다고 판단한다.

설문지를 통해서 구체적으로 알아 본 사항은 다음과 같다.

<표 4-1> 설문지 구성 항목

| 영역 | 질문항목 |
|---|---|
| 인구·사회적 특성 | 성, 연령, 학력, 고용형태, 소득, 직업, 업종, 사업장 규모, 근속년수, 노동조합가입여부 및 노조간부여부, 노사 신뢰수준 |
| 전자기술의 종류와 사용실태 | - 각 전자기술의 사용여부<br>- 사용되고 있는 전자기술 목적 인지여부<br>- 전자기술의 정보수집여부에 대한 인지여부<br>- 수집된 정보의 활용에 대한 인지여부 |
| 전자기술에 대한 인식 | - 전자기술의 관찰 및 감시의 목적 인식<br>- 전자기술로 인한 감시여부<br>- 각 전자기술의 형태가 주는 불안감의 수준 |
| 전자기술직장설치 과정 및 노동자참여 권한의 범위 | - 전자시스템 설치 목적<br>- 전자기술 설치시 노동자 개인에 대한 고지여부<br>- 전자기술 설치시 노동자대표에 대한 고지여부<br>- 전자기술 설치시 노동자와의 협의 유무<br>- 전자기술 도입시 노동자의 참여수준 |
| 전자기술사용효과에 대한 인식 | - 생산성 향상, 회사보안향상, 업무효율성 향상, 관리비용절감, 안전 및 산재예방과 인사평가합리화, 인사상 불이익<br>- 노동통제 강화, 개인사생활 침해, 안전향상 및 산재예방, 노사간 불신증대, 건강악화, 노조활동 저해 |
| 규제의 필요성과 대책 | - 헌법의 사생활침해방지에 대한 조항 인지여부,<br>- 전자기술의 관찰 및 감시에 대한 규제의 필요성,<br>- 전자기술의 관찰 및 감시에 대한 규제의 수단,<br>- 전자기술사용 규제를 위한 규정의 내용<br>(전자기술감시 통고, 전자기술도입이유 설명, 전자기술 도입에 대한 동의, 전자기술선택권, 전자감시기록 결과의 접근성, 업무이외의 전자기술 사용금지, 업무이외의 감시자료 수집 제한, 부적절한 감시자료 및 자료해석에 대한 이의제기 절차, 개인정보유출에 대한 동의) |

## 2. 조사결과

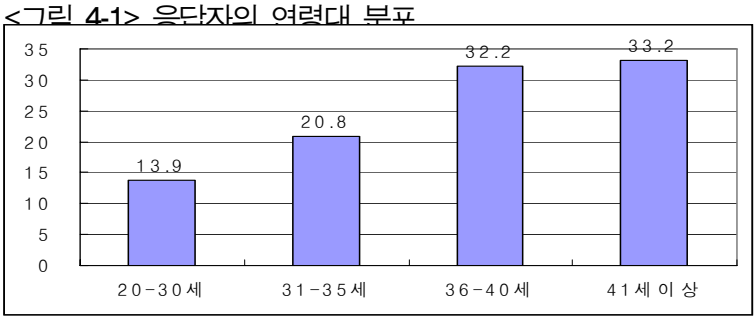
### 1) 인구·사회적 특성

조사대상자의 인구사회적 특성을 알아보았다. 총 응답자 중 남성은 181명으로 88.7%이었으며 여성은 22명으로 10.8%로 나타나 남성이 압도적으로 많았다. 조사자의 연령대는 주로 중년층이라 부를 수 있는 41세 이상 33.2%로 가장 많은 분포를 보였다. 36세-40세는 32.2%, 31-35세가 20.8%였으며, 20세-30세는 13.9%를 차지했다.

<표 4-2> 응답자의 연령 분포

| | 20-30세 | 31-35세 | 36-40세 | 41세이상 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 28 | 42 | 65 | 67 | 202 |
| 백분율 | 13.9 | 20.8 | 32.2 | 33.2 | 100.0 |

<그림 4-1> 응답자의 연령대 분포

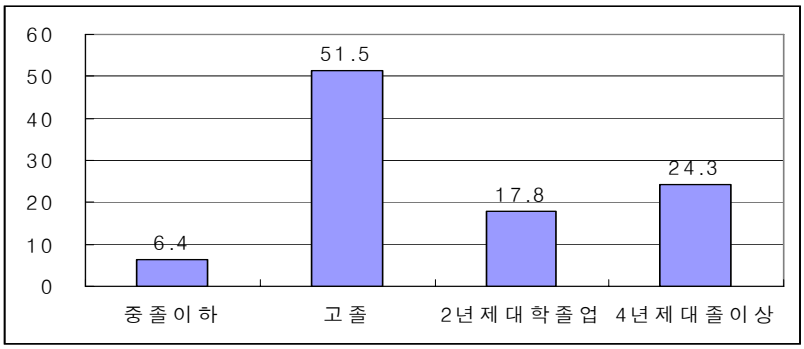



조사 대상자들의 학력은 고졸이 51.5%로 절반 이상을 차지했으며, 4년제 대학졸업 이상인 사람이 24.3%였다. 2년제 대학 졸업자가 17.8%, 중졸이하의 학력인 사람은 6.4%를 차지했다.

<표 4-3> 응답자의 학력분포

| | 중졸이하 | 고졸 | 2년제 대졸 | 4년제 대졸이상 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 13 | 104 | 36 | 49 | 202 |
| 백분율 | 6.4 | 51.5 | 17.8 | 24.3 | 100.0 |

<그림 4-2> 응답자의 학력 분포

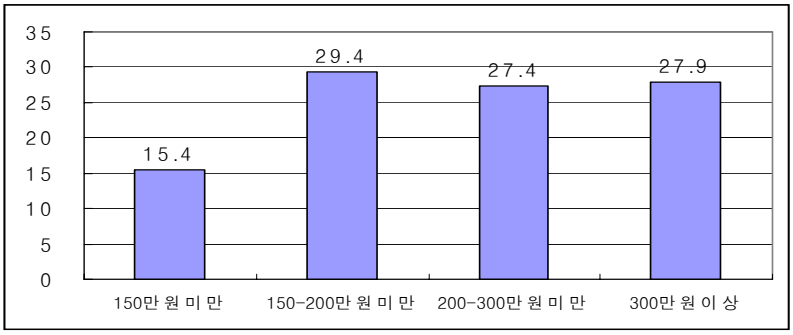



응답자의 월평균 소득을 전체적으로 보면 소득이 150만원 이하의 저소득층은 15.4%였고 300만원 이상의 소득을 가진 노동자는 27.9%였으며 대부분은 중간에 위치하고 있다. 구체적으로 보면 150-200만원미만이 29.4%로 가장 많았으며, 200-300만원미만이 27.4%였다.

<표 4-4> 응답자의 소득분포

| | 150만원 미만 | 150-200만원 미만 | 200-300만원 미만 | 300만원 이상 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 31 | 59 | 55 | 56 | 201 |
| 백분율 | 15.4 | 29.4 | 27.4 | 27.9 | 100.0 |

<그림 4-3> 응답자의 소득 분포

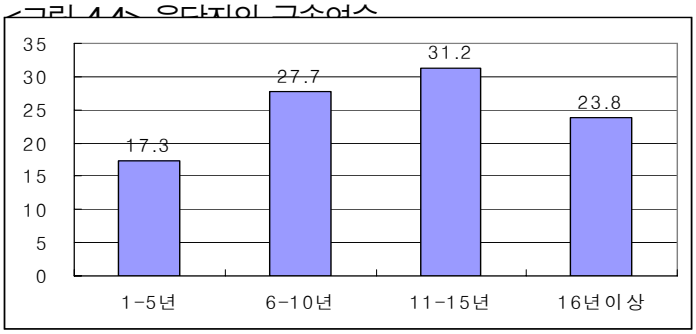



응답자의 고용형태를 보면 조사대상자 204명 중 거의 대부분이 정규직(96.6%)이었으며, 비정규직은 5명, 기타는 1명에 불과했다. 근속 년수는 11-15년이 31.2%로 가장 많았고, 그 다음은 6-10년 근무한 노동자로서 27.7%로 나타났다. 장기 근속한 16년 이상 근속 노동자도 23.8%였다. 1-5년 근무한 노동자는 17.3%였다.

<표 4-5> 응답자의 근속연수

| | 1-5년 | 6-10년 | 11-15년 | 16년 이상 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 35 | 56 | 63 | 48 | 202 |
| 백분율 | 17.3 | 27.7 | 31.2 | 23.8 | 100.0 |

<그림 4-4> 응답자의 근속연수

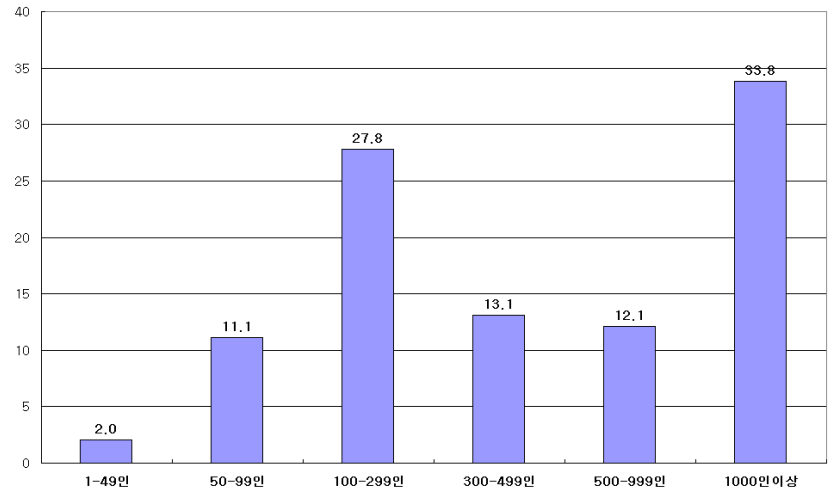


사업장의 규모는 1000인 이상의 대규모 사업장이 33.0%로 가장 많았으며, 100인에서 300인 미만의 사업장이 27.9%로 그 다음 순위를 차지했다. 300인에서 500인미만의 사업장은 13.2%, 500인 이상 1000인 미만이 12.1%였으며, 비교적 소규모 사업장이라 볼 수 있는 50인에서 100인 미만 사업장은 11.1%였고, 1인-50인 미만 사업장은 2.0%였다. 따라서 중소기업과 대기업의 비율이 비교적 적정한 비율로 섞여 있다고 할 수 있다.

<표 4-6> 응답자의 사업장 규모

| | 1-49 | 50-99 | 100-299 | 300-499 | 500-999 | 1000이상 | 전체 |
|---|---|---|---|---|---|---|---|
| 사례수 | 4 | 22 | 55 | 26 | 24 | 67 | 198 |
| 백분율 | 2.0 | 11.1 | 27.8 | 13.1 | 12.1 | 33.8 | 100.0 |

<그림 4-5> 응답자의 사업장 규모

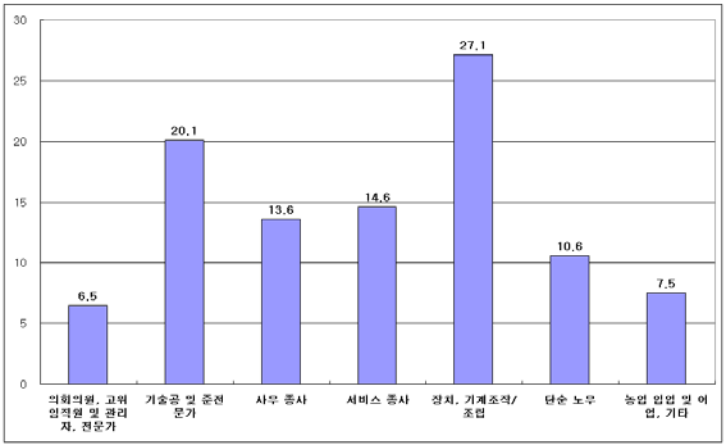


응답자의 직종은 기계조작 및 조립이 27.1%, 기술공 및 준전문가가 20.1%로 나타났다. 서비스 종사자는 14.6%, 사무 종사자는 13.6%, 단순 노무 10.6%, 농업, 임업 어업 및 기타는 7.5%, 의회의원, 고위 임직원 및 관리자, 전문가는 6.5%였다.

<표 4-7> 응답자의 종사직종

| | 의회의원, 고위임직원 및 관리자, 전문가 | 기술공 및 준전문가 | 사무 종사 | 서비스 종사 | 장치, 기계조작/ 조립 | 단순 노무 | 농업 입업 및 어업, 기타 | 전체 |
|---|---|---|---|---|---|---|---|---|
| 사례수 | 13 | 40 | 27 | 29 | 54 | 21 | 15 | 199 |
| 백분율 | 6.5 | 20.1 | 13.6 | 14.6 | 27.1 | 10.6 | 7.5 | 100.0 |

<그림 4-6> 응답자의 종사직종

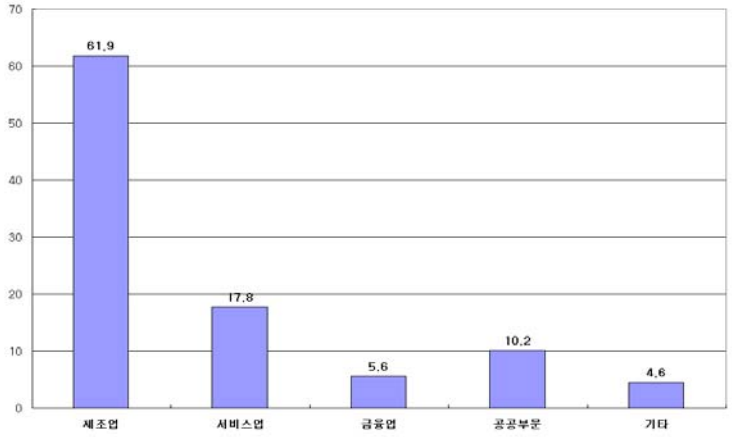



응답자가 종사하고 있는 업종으로는 제조업이 절반이상인 61.9%로 가장 많았으며, 서비스업이 17.8%였고, 공공부문이 10.2%, 금융업이 5.6% 등의 순서로 나타났다.

<표 4-8> 응답자의 종사 업종

| | 제조업 | 서비스업 | 금융업 | 공공부문 | 기타 | 전체 |
|---|---|---|---|---|---|---|
| 사례수 | 122 | 35 | 11 | 20 | 9 | 197 |
| 백분율 | 61.9 | 17.8 | 5.6 | 10.2 | 4.6 | 100.0 |

<그림 4-7> 응답자의 종사 업종



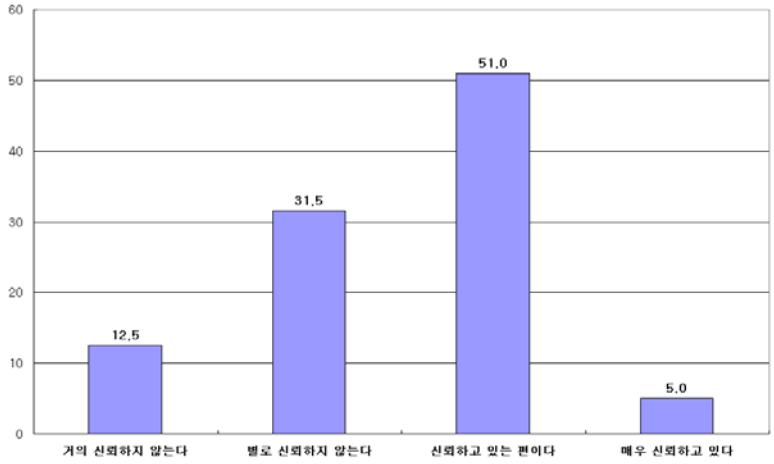

응답자가 종사하고 있는 사업장에서 노조에 가입된 수는 92.6%인 188명이었다. 이들 중 70.9%가 노조 간부였고 평조합원은 29.1%였다.

설문 대상자가 응답한 회사 경영진과 노동자간의 상호 신뢰도는 '신뢰하고 있는 편이다'가 51.0%, '매우 신뢰하고 있다'는 5.0%로 과반수 이상이 회사경영진에게 우호적임을 표방했고, '별로 신뢰하지 않는다'는 31.5%, '거의 신뢰하지 않는다'는 12.5%, 로 나타났다.

<표 4-9> 응답자의 노사간 신뢰정도 판단

| | 거의 신뢰하지 않는다 | 별로 신뢰하지 않는다 | 신뢰하고 있는 편이다 | 매우 신뢰하고 있다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 25 | 63 | 102 | 10 | 200 |
| 백분율 | 12.5 | 31.5 | 51 | 5 | 100.0 |

<그림 4-8> 응답자의 노사간 신뢰정도 판단




### 2) 전자기술의 종류와 사용실태

노동자들이 사업장에서 사용하고 있는 전자기술의 현황을 알아보았다.

사업장에서 다양한 전자기술이 사용되고 있고 업종 및 업무에 따라 기술의 종류도 상이하겠지만 대다수가 사용하고 있을 것으로 추측되는 전자기술에 대해 알아보았다. 설문지에서 사용한 전자기술은 인터넷이용 모니터링, 컴퓨터하드디스크 모니터링, 전화송수진내역기록, CCTV, RFID, 전자신분증(출입카드), 지문 및

생체인식, ERP(전사적 자원관리)에 국한하였다.

전체적으로 볼 때, 8종류의 전자감시기술 중 개인당 평균 2.36개의 전자감시기술이 확실히 사용되고 있다고 응답하였다. 각 전자감시기술 간의 상관관계를 통해 살펴보면, 인터넷모니터링과 하드디스크 모니터링을 같이 할 가능성이 44.6%로 나타났으며, 그 다음으로 높은 것이 CCTV와 지문 및 생체인식 기술을 같이 사용할 가능성이 35.7%로 나타났다. 그 다음으로는 CCTV와 RFID(35.2%), RFID와 지문 및 생체인식(34.8%) 등의 순서였다.

<표 4-10> 특정한 전자기술과 다른 전자기술이 함께 사용될 수 있는 상관성

| | 인터넷 모니터링 | 하드디스크모니터링 | 전화 모니터링 | CCTV | RFID | 출입카드 | 지문및 생체인식 | ERP |
|---|---|---|---|---|---|---|---|---|
| 인터넷모니터링 | | | | | | | | |
| 하드디스크모니터링 | .446(**) | | | | | | | |
| 전화모니터링 | .283(**) | .227(**) | | | | | | |
| CCTV | .225(**) | .225(**) | .176(*) | | | | | |
| RFID | .192(**) | 0.09 | .253(**) | .352(**) | | | | |
| 출입카드 | -0.056 | 0.085 | -0.039 | 0.133 | 0.038 | | | |
| 지문및생체인식 | 0.128 | 0.058 | 0.092 | .357(**) | .348(**) | -0.062 | | |
| ERP | .272(**) | 0.073 | .187(*) | .148(*) | .298(**) | -0.001 | 0.107 | |

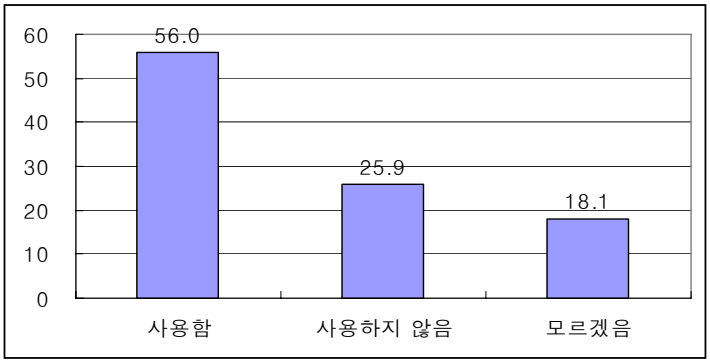
* $p < 0.05$ ** $p < 0.01$

이러한 전자기술 각 항목에 대해 널리 사용되고 있는 인터넷에 대한 모니터링여부를 먼저 질문하였다. 인터넷사용을 모니터링 하는가하는 문항에 대해 절반이 넘는 56.0%가 모니터링이 되고 있다고 응답하였다. 이에 반해 사용하지 않는다고 응답한 경우는 25.9%였으며 모르겠다는 응답도 18.1%로 나타났다.

<표 4-11> 인터넷 사용 모니터링 여부

| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 사례수 | 108 | 50 | 35 | 193 |
| 백분율 | 56.0 | 25.9 | 18.1 | 100.0 |

<그림 4-9> 인터넷 사용 모니터링 여부

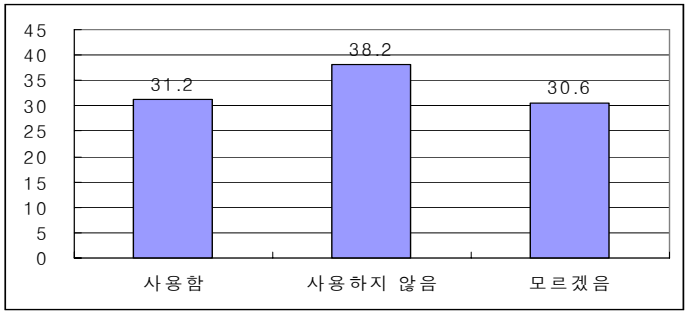



컴퓨터 하드디스크 내용을 모니터링하는가에 대해서는 38.2%가 모니터링을 하지 않는다고 응답하였으나 모니터링한다고 응답한 경우도 31.2%로 나타나 그 차이가 크지 않은 것을 알 수 있다. 모르겠다고 응답한 경우 역시 30.6%로 다른 응답과 비슷한 분포였다.

<표 4-12> 컴퓨터 하드디스크 내용 모니터링 여부

| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 사례수 | 58 | 71 | 57 | 186 |
| 백분율 | 31.2 | 38.2 | 30.6 | 100.0 |

<그림 4-10> 컴퓨터 하드디스크 내용 모니터링 여부

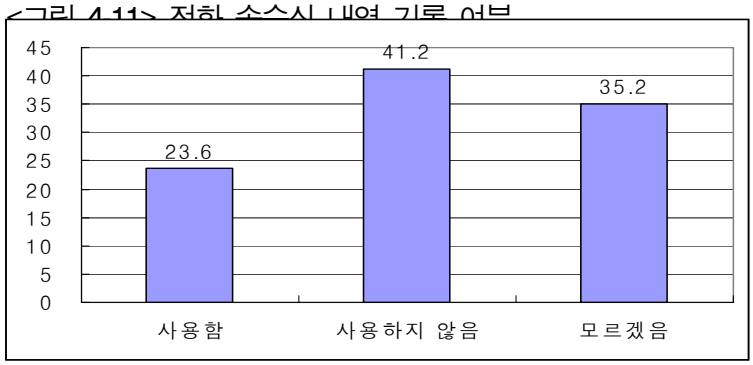



전화 송수신 내역 기록 여부에 대해 41.2%가 사용하지 않는다고 대답한 반면에 사용한다는 응답은 23.6%였으며 모르겠다는 응답은 35.2%로 높게 나타났다.

<표 4-13> 전화 송수신 내역 기록 여부

| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 사례수 | 43 | 75 | 64 | 182 |
| 백분율 | 23.6 | 41.2 | 35.2 | 100.0 |

<그림 4-11> 전화 송수신 내역 기록 여부

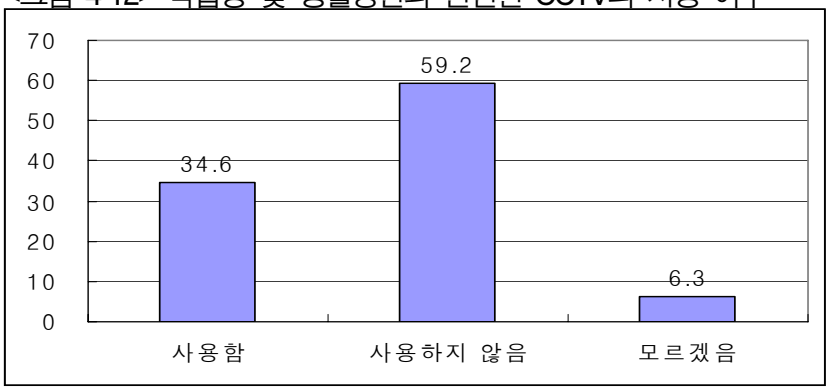


작업장 및 생활공간과 관련한 CCTV의 사용 여부에 대해서는 사용하지 않는다는 응답이 절반이 넘는 59.2%였다. 사용한다는 응답은 34.6%로 나타났으며, 모르겠다고 응답한 경우는 6.3%로 CCTV에 대해서는 상대적으로 사용여부에 대해 명확히 알고 있는 것으로 나타났다.

<표 4-14> 작업장 및 생활공간과 관련한 CCTV의 사용여부

| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 사례수 | 66 | 113 | 12 | 191 |
| 백분율 | 34.6 | 59.2 | 6.3 | 100.0 |

<그림 4-12> 작업장 및 생활공간과 관련한 CCTV의 사용 여부

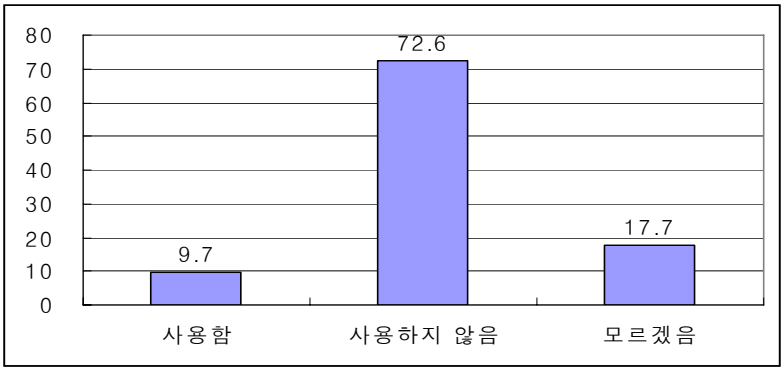



무선인식장치로 불리는 RFID에 대해서는 대다수인 72.6%가 사용하지 않는다고 대답하였으며 9.7%는 사용한다고 대답하였다. 모르겠다는 응답은 17.7%로 나타났다.

<표 4-15> RFID 사용여부

| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 사례수 | 18 | 135 | 33 | 186 |
| 백분율 | 9.7 | 72.6 | 17.7 | 100.0 |

<그림 4-13> RFID 사용여부

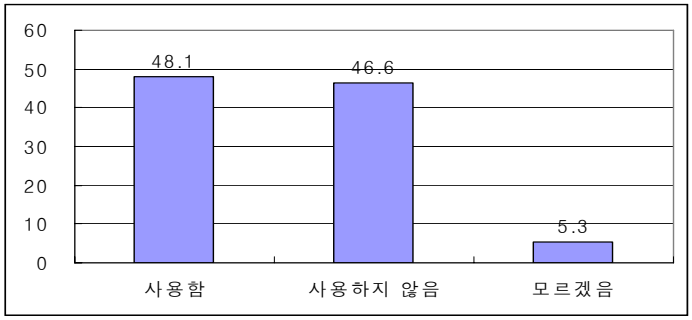



한편 전자 신분증 (출입카드)를 사용하는가에 대해서는 48.1%가 사용한다고 대답하였으며 사용하지 않는다고 응답한 경우는 46.6%로 비슷했다. 모르겠다는 응답은 5.3%였다.

<표 4-16> 전자신분증(출입 카드) 사용 여부

| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 사례수 | 91 | 88 | 10 | 189 |
| 백분율 | 48.1 | 46.6 | 5.3 | 100.0 |

<그림 4-14> 전자신분증(출입 카드) 사용 여부

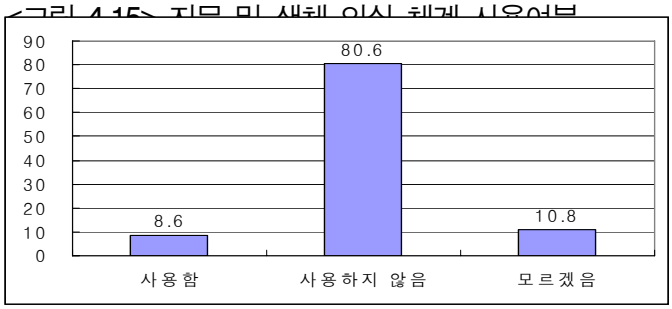



지문 및 생체 인식 체계를 사용하는가라는 질문에 대해 대다수인 80.6%가 사용하지 않는다고 대답해 아직까지 지문 및 생체 인식 체계는 많이 사용되지 않는 것으로 나타났다. 사용한다는 응답은 8.6%, 모르겠다는 응답은 10.8%로 나타났다.

<표 4-17> 지문 및 생체 인식 체계 사용 여부

| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 사례수 | 16 | 150 | 20 | 186 |
| 백분율 | 8.6 | 80.6 | 10.8 | 100.0 |

<그림 4-15> 지문 및 생체 인식 체계 사용여부

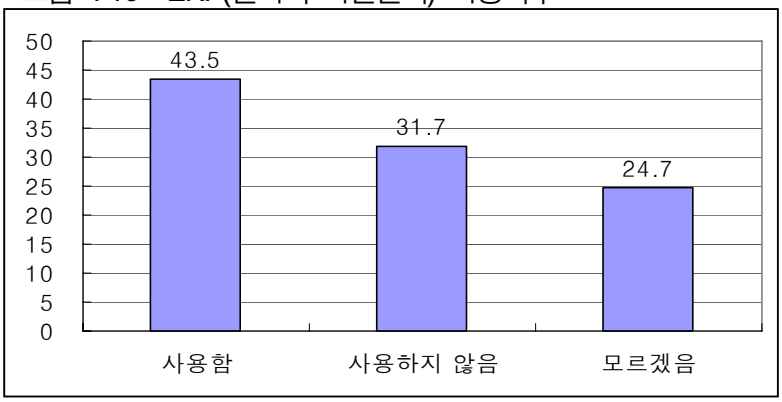


ERP(전사적 사원관리)를 활용하고 있는가라는 질문에 대해서는 43.5%가 그렇다고하였고 사용하지 않는다는 응답이 31.7%로 사용한다는 응답이 약간 높은 것으로 나타났다. 모르겠다는 응답은 24.7%였다.

<표 4-18> ERP(전사적 사원관리) 사용여부

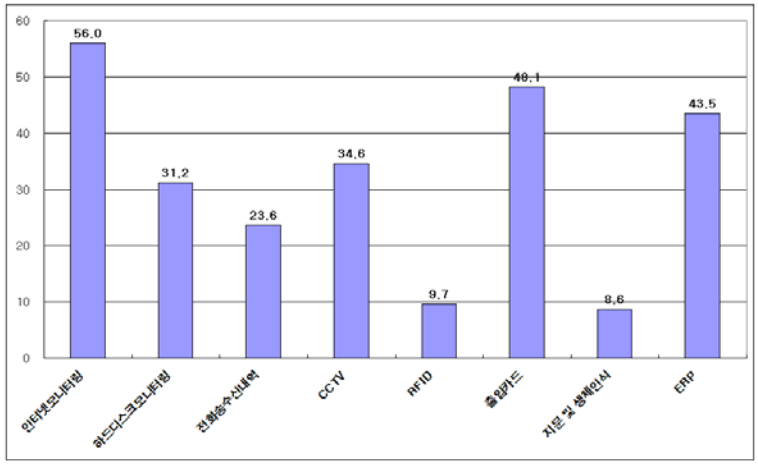
| | 사용함 | 사용하지 않음 | 모르겠음 | 전체 |
|---|---|---|---|---|
| 백분율 | 43.5 | 31.7 | 24.7 | 100.0 |
| 사례수 | 81 | 59 | 46 | 186 |

<그림 4-16> ERP(전사적 사원관리) 사용여부



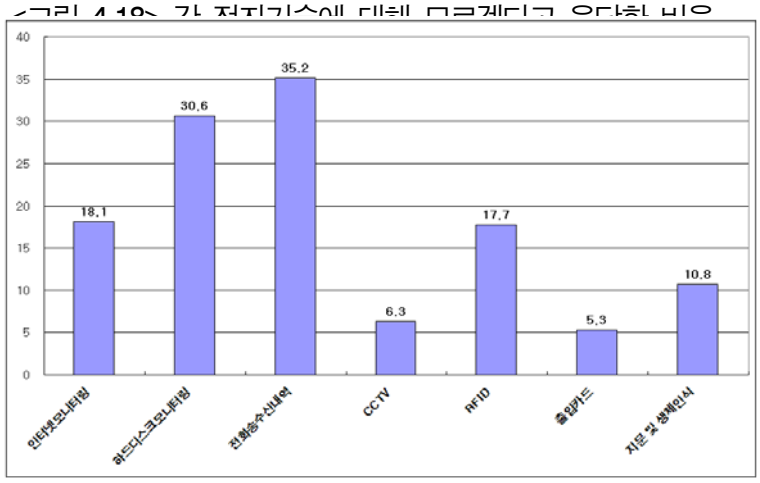

설문지에서 열거된 전자기술 중에서 확실하게 사용하고 있다는 응답이 가장 높은 것은 인터넷이용모니터링이었고 그 뒤를 전자신분증, ERP, CCTV, 컴퓨터 하드디스크 모니터링, 전화송수신 내역기록 등의 순으로 나타났고 RFID와 지문 및 생체인식이 가장 낮게 나타났다.

<그림 4-17> 각 전자기술에 대해 사용하고 있다고 응답한 비율




한편 열거된 전자기술 중 현재 사업장에서 사용하고 있는지를 모르겠다는 비율이 가장 높았던 것은 전화송수신내역 기록여부(35.2%)였고 그 뒤를 컴퓨터 하드디스크 모니터링(30. 6%), ERP(24.7%), 인터넷 사용모니터링(18.1%), RFID(17.7%), 지문 및 생체 인식체계 사용여부(10.8%), CCTV(6.3%), 전자신분증(5.3%)의 순으로 나타났다.

<그림 4-18> 각 전자기술에 대해 모르겠다고 응답한 비율



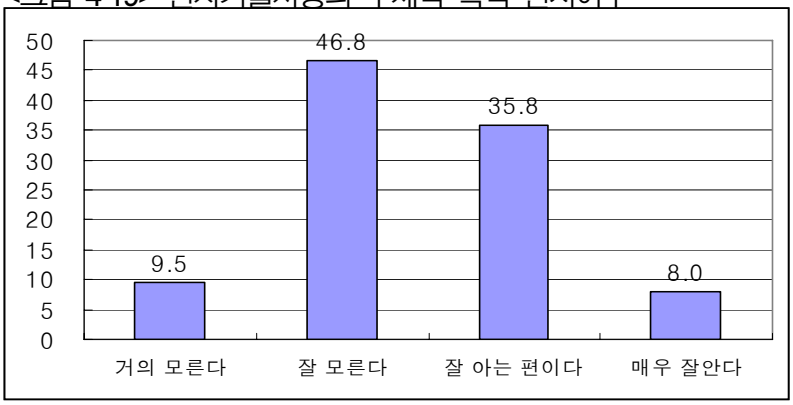
### 3) 전자기술의 목적 및 관찰 감시에 대한 인식

현재 직장에서 사용되고 있는 전자기술의 활용에 대한 인지도를 알아보았다. 직장에서 활용되는 전자기술의 구체적 목적에 대해 아는가에 대해 '거의 모른다'는 응답이 9.5%, '잘 모른다'는 응답은 46.0%로 전체적으로 모른다고 응답한 비율이 51.9%였다. '잘 아는 편이다'는 응답은 35.8%였으며, '매우 잘안다'는 8.0%였다.

<표 4-19> 전자기술사용의 구체적 목적 인지 여부

| | 거의 모른다 | 잘 모른다 | 잘 아는 편이다 | 매우 잘 안다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 19 | 94 | 72 | 16 | 201 |
| 백분율 | 9.5 | 46.8 | 35.8 | 8.0 | 100.0 |

<그림 4-19> 전자기술사용의 구체적 목적 인지여부




전자기술사용의 구체적 목적에 대한 인지도를 성별, 연령, 최종학력, 소득, 직장근속년수, 노조가입여부, 사업장 규모, 직업, 노사간 신뢰수준에 따라 달라지는

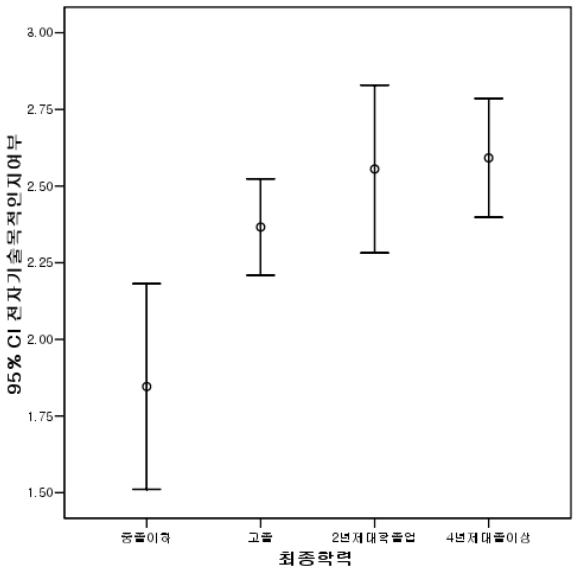
가를 살펴본 결과, 최종학력만이 유의미한 것으로 나타났다. 학력별 전자기술사용의 구체적 목적에 대한 인지여부의 차이는 중졸이하 학력과 나머지 학력에서 나타났으며, 중졸이하의 학력을 보유한 사람들이 다른 학력을 보유한 사람들에 비해 전자기술사용의 구체적 목적을 인지하는 정도가 낮았다.

<표 4-20> 학력에 따른 전자기술 사용목적인지도 점수 평균차

| (I) 최종학력 | (J) 최종학력 | 평균차 (I-J) | 표준오차 | 유의확률 |
|---|---|---|---|---|
| 중졸이하 | 고졸 | -0.52 | 0.22 | 0.15 |
| | 2년제대학졸업 | -0.71(*) | 0.25 | 0.04 |
| | 4년제대졸이상 | -0.75(*) | 0.24 | 0.02 |
| 고졸 | 중졸이하 | 0.52 | 0.22 | 0.15 |
| | 2년제대학졸업 | -0.19 | 0.15 | 0.65 |
| | 4년제대졸이상 | -0.23 | 0.13 | 0.41 |
| 2년제대학졸업 | 중졸이하 | 0.71(*) | 0.25 | 0.04 |
| | 고졸 | 0.19 | 0.15 | 0.65 |
| | 4년제대졸이상 | -0.04 | 0.17 | 1.00 |
| 4년제대졸이상 | 중졸이하 | 0.75(*) | 0.24 | 0.02 |
| | 고졸 | 0.23 | 0.13 | 0.41 |
| | 2년제대학졸업 | 0.04 | 0.17 | 1.00 |

* P < 0.05, Schaffe test 결과

<그림 4-20> 최종학력에 따른 전자기술 목적 인지여부 정도



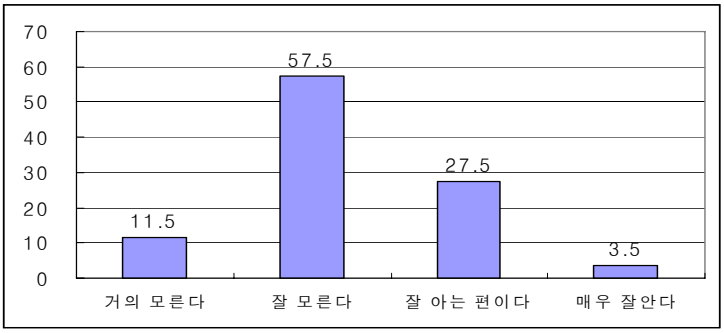

* 평균, 신뢰수준 95%

직장에서 활용되는 전자기술에 의한 정보 수집 내용을 인지하고 있는지 알아본 결과 '거의 모른다'는 응답이 11.5%였으며, 절반이 넘는 57.5%가 '잘 모른다'고 응답하여 전체 응답자 중 69%가 전자기술이 정보를 수집하고 있는지의 여부를 알수 없다고 응답하였다. '잘 아는 편이다'는 응답은 27.5%, '매우 잘 안다'는 3.5%로 31%만이 현재 직장의 전자기술 정보수집내용에 대해 인지하고 있는 것으로 나타났다.

<표 4-21> 전자기술에 의한 정보 수집 내용 인지 수준

| | 거의 모른다 | 잘 모른다 | 잘 아는 편이다 | 매우 잘안다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 23 | 115 | 55 | 7 | 200 |
| 백분율 | 11.5 | 57.5 | 27.5 | 3.5 | 100.0 |

<그림 4-21> 전자기술에 의한 정보 수집 내용 인지수준



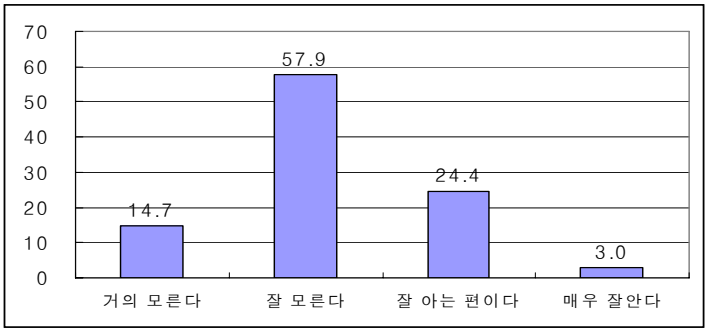

전자기술사용에 의한 정보 수집의 내용을 어느 정도 인지하는지를 성별, 연령, 최종학력, 소득, 직장근속년수, 노조가입여부, 사업장 규모, 직업, 노사간 신뢰도에 따라 달라지는가를 살펴본 결과, 유의미한 차이는 보이지 않았다.

직장 내 전자 기술에 의해 수집되는 정보가 회사에서 어떻게 활용되는지에 대해 알고 있는가를 물었을 때, '거의 모른다'는 응답이 14.7%였으며, 역시 절반이 넘는 57.9%가 '잘 모른다'고 응답하여 전체 응답자 중 74.6%가 수집된 정보가 어떻게 활용되고 있는지를 모르고 있는 것으로 나타났다. '잘 아는 편이다'는 응답은 24.4%, '매우 잘 안다'는 3.0%로 나타나 전체 응답자의 27.4%만이 수집된 정보를 회사가 활용하는 방식에 대해서 알고 있었다.

<표 4-22> 전자기술에 의해 수집된 정보의 활용

| | 거의 모른다 | 잘 모른다 | 잘 아는 편이다 | 매우 잘안다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 29 | 114 | 48 | 6 | 197 |
| 백분율 | 14.7 | 57.9 | 24.4 | 3.0 | 100.0 |

<그림 4-22> 전자 기술에 의해 수집된 정보의 활용



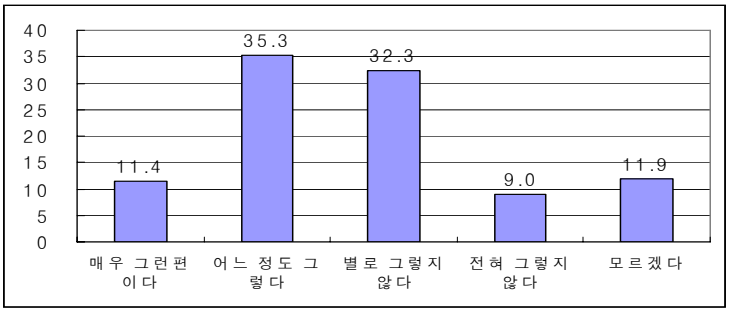

전자기술사용에 의해 수집된 정보 활용에 대한 인지도가 성별, 연령, 최종학력, 소득, 직장근속년수, 노조가입여부, 사업장 규모, 직업, 노사간 신뢰수주에 따라 차이가 나는지를 살펴본 결과, 각 변수별 유의미한 차이는 보이지 않았다.

직장의 전자기술이 노동자를 관찰, 감독, 감시할 목적으로 사용되고 있다고 보는가에 대해 '매우 그런 편이다'는 11.4%, '어느 정도 그렇다'는 35.3%로 나타나 전자기술의 사용이 관찰, 감독, 감시의 목적이라고 인지한 경우는 응답자의 46.7%로 나타났다. '별로 그렇지 않다'고 응답한 경우는 32.3%, '전혀 그렇지 않다'는 9.0%로 전자기술이 가진 관찰, 감독, 감시의 역할에 대한 부정적인 응답은 41.3%였다. 모르겠다는 응답은 11.9%였다.

<표 4-23> 노동자 관찰, 감독, 감시목적으로 사용한다고 인식한 비율

| | 매우 그런편이다 | 어느 정도 그렇다 | 별로 그렇지 않다 | 전혀 그렇지 않다 | 모르겠다 | 전체 |
|---|---|---|---|---|---|---|
| 사례수 | 23 | 71 | 65 | 18 | 24 | 201 |
| 백분율 | 11.4 | 35.3 | 32.3 | 9.0 | 11.9 | 100.0 |

<그림 4-23> 노동자 관찰, 감독, 감시할 목적으로 사용

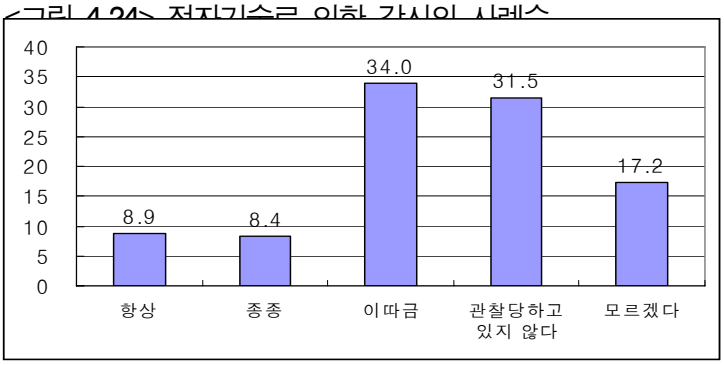



전자 감시 기술에 의해 감시당하는 정도가 어느 정도인가라는 질문에 '항상'은 8.9%, '종종'은 8.4%, '이따금'은 34.0%로 전체의 51.3%가 감시가 있는 것으로 파악하고 있었다. '관찰당하고 있지 않다'는 응답은 31.5%였으며, '모르겠다'는 응답은 17.2%였다.

<표 4-24> 전자기술로 인한 감시 비율

| | 항상 | 종종 | 이따금 | 관찰당하고 있지 않다 | 모르겠다 | 전체 |
|---|---|---|---|---|---|---|
| 사례수 | 18 | 17 | 69 | 64 | 35 | 203 |
| 백분율 | 8.9 | 8.4 | 34.0 | 31.5 | 17.2 | 100.0 |

<그림 4-24> 전자기술로 인한 감시의 사례수

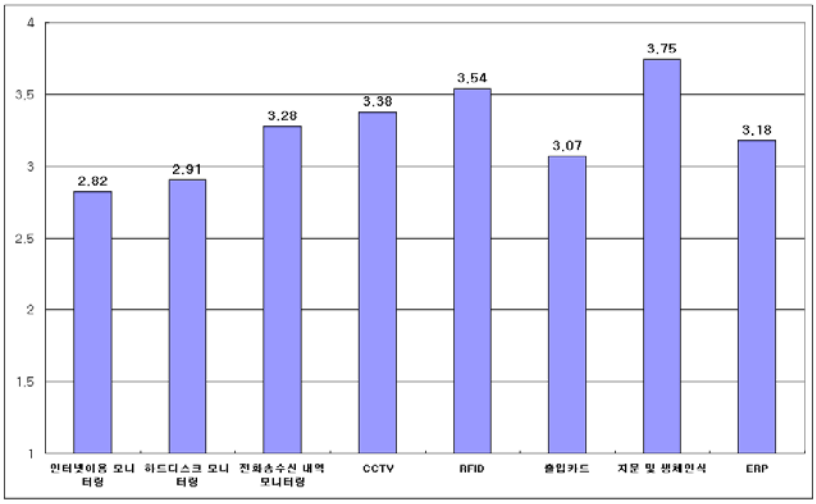


전자 감시 기술이 노동자에게 주는 불안감을 평균 점수로 살펴보았다. 전체적으로 볼 때 전자기술의 종류에 관계없이 불안감 정도는 2.5점을 넘어서고 있어 노동자의 전자기술로 인한 불안감의 정도를 잘 나타내고 있다. 전자기술의 종류별로 보았을 때 불안감의 정도는 지문 및 생체인식이 3.75점으로 가장 높았으며 그 다음으로 RFID 3.54점, CCTV(3.38점), 전화송수신 내역 모니터링(3.28점), ERP(3.19점), 출입카드(3.07점), 하드 디스크 모니터링(2.91점), 인터넷 모니터링(2.82점) 순으로 잇고 있었다.

<표 4-25> 전자기술 유형에 따른 불안감

| | 인터넷 모니터링 | 하드디스크 모니터링 | 전화송수신 내역 모니터링 | CCTV | RFID | 출입카드 | 지문 및 생체인식 | ERP |
|---|---|---|---|---|---|---|---|---|
| 평균 | 2.82 | 2.91 | 3.28 | 3.38 | 3.54 | 3.07 | 3.75 | 3.18 |
| 표준편차 | 1.41 | 1.52 | 1.48 | 1.52 | 1.61 | 1.60 | 1.55 | 1.45 |
| 사례수 | 195 | 191 | 194 | 194 | 186 | 190 | 189 | 188 |

<그림 4-25> 전자기술유형에 따른 불안감




* 4점 척도 (1점 거의 없음, 2점 약간 있음, 3점 큰 편, 4점 매우 큼), 2.5점이 준거점
** 사용하고 있다는 응답자만으로 평균 구성

### 4) 전자기술 직장 설치 과정

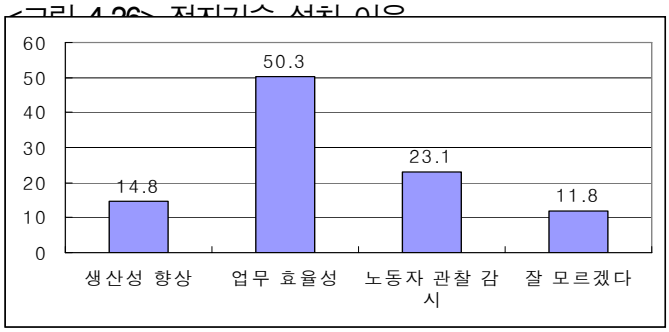
이 절에서는 전자기술이 직장에서 설치되는 과정에서 노동자의 참여 및 협의 과정을 살펴보고 전자기술 설치시 전자기술 활용의 대상자인 노동자의 바람직한 참여정도에 관해 알아보았다.

전자시스템이 사업장에 어떠한 형태로든 설치되었다고 응답한 169명(87.1%)을 대상으로 설치과정을 알아보았다. 전자 시스템 설치 이유에 관해서는 절반 정도인 50.3%가 '업무 효율성을 위해' 설치한 것으로 생각한다고 응답했다. '노동자를 관찰 감시하기 위하여' 설치했다는 응답은 업무효율성의 절반 정도로서 전체 23.1%로 그 뒤를 잇고 있었다. '생산성 향상을 위해' 설치되었다고 생각하는 경우는 14.8% 였으며, '잘 모르겠다'는 응답은 11.8%로 나타났다. 따라서 많은 사람들이 전자기술의 사용이 생산성 및 업무와 관련되어 설치되었다고 인식하고 있고 순수하게 노동자를 관찰, 감시하기 위해서라고 응답한 비율은 23.1%로 나타났다.

<표 4-26> 전자기술 설치 이유

| | 생산성 향상 | 업무 효율성 | 노동자 관찰 감시 | 잘 모르겠다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 25 | 85 | 39 | 20 | 169 |
| 백분율 | 14.8 | 50.3 | 23.1 | 11.8 | 100.0 |

<그림 4-26> 전자기술 설치 이유

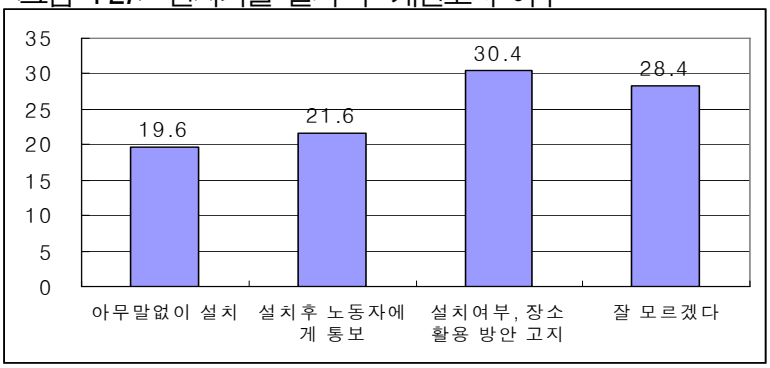


전자기술 설치시 노동자 개인에게 통보했는가에 대해 '아무 말 없이 설치하였다'는 응답이 19.6%로 나타났다. '설치 후 노동자에게 통보했다'는 응답은 21.6%, '설치여부 및 장소, 활용방안을 고지했다'는 응답은 30.4%로 나타났다. '잘 모르겠다'는 응답은 28.4%로 나타났다.

<표 4-27> 전자기술 설치 후 개인고지 여부

| | 아무말 없이 설치 | 설치후 노동자에게 통보 | 설치여부, 장소 활용 방안 고지 | 잘 모르겠다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 38 | 42 | 59 | 55 | 194 |
| 백분율 | 19.6 | 21.6 | 30.4 | 28.4 | 100.0 |

<그림 4-27> 전자기술 설치 후 개인고지 여부

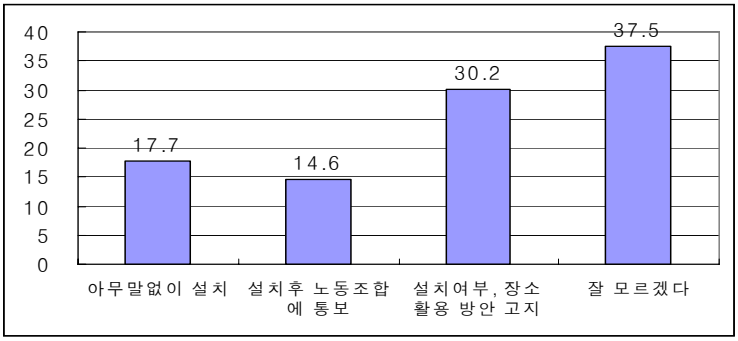



전자기술을 노동조합이나 이에 걸맞는 노동자 대표기구에 통보했는가에 대해서는 '아무 말 없이 설치했다'는 응답이 17.7%로 개인 통보 수준과 비슷하게 나타났다. '설치 후 노동조합에 통보했다'는 응답은 14.6%, '설치여부, 장소 및 활용방안을 고지했다'는 응답은 30.2%로 나타나 개인에게 통보한 것과 비슷했다. '잘 모르겠다'는 응답은 37.5%로 노동자 개인 고지에 대해 모르겠다고 응답한 것보다 더 높게 나타났다.

<표 4-28> 전자기술 노동조합 통보여부

| | 아무 말없이 설치 | 설치후 노조에 통보 | 설치여부, 장소 활용 방안 고지 | 잘 모르겠다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 34 | 28 | 58 | 72 | 192 |
| 백분율 | 17.7 | 14.6 | 30.2 | 37.5 | 100.0 |

<그림 4-28> 전자기술의 노동조합 통보여부

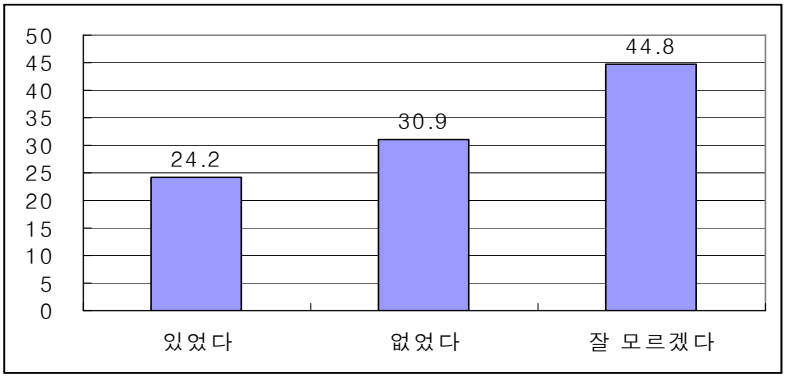



전자기술 설치시 노동자 혹은 노동자 대표와의 협의 혹은 합의가 있었는가에 대해 '있었다'는 응답은 24.2%로 나타났다. '없었다'는 응답은 30.9%였으며, '잘 모르겠다'는 응답은 절반에 약간 못 미치는 44.8%로, 이러한 과정 자체에 대해 잘 알지 못하는 것으로 나타났다. 이를 '협의 혹은 합의가 없었다'는 응답과 합할 경우 80%에 이르는 정도가 협의 혹은 합의 과정에 대한 부재를 표현한다고 볼 수 있다.

<표 4-29> 전자기술 설치시 노조와의 합의 및 협의 여부

| | 있었다 | 없었다 | 잘 모르겠다 | 전체 |
|---|---|---|---|---|
| 사례수 | 47 | 60 | 87 | 194 |
| 백분율 | 24.2 | 30.9 | 44.8 | 100.0 |

<그림 4-29> 전자기술 설치시 노조와의 합의 및 협의 여부

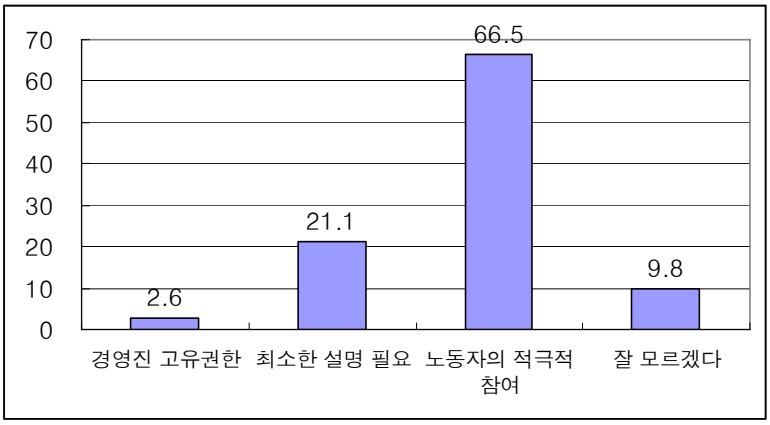



전자 기술 시스템 도입 및 운영에 노동자가 어떠한 정도로 참여해야 하는가에 대해 66.5%가 '노동자의 적극적 참여'가 있어야 한다고 대답해 이 문제에 대한 노동자의 참여를 강조하고 있었다. '최소한의 설명이 필요하다'는 응답은 21.1%였으며, '경영진 고유의 권한'이라고 생각하는 경우는 2.6%에 불과하였다. '잘 모르겠다'고 응답한 경우는 9.8%로 나타났다.

<표 4-30> 전자기술 설치시 노동자 참여 필요성에 대한 인식

| | 경영진 고유권한 | 최소한 설명 필요 | 노동자의 적극적 참여 | 잘 모르겠다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 5 | 41 | 129 | 19 | 194 |
| 백분율 | 2.6 | 21.1 | 66.5 | 9.8 | 100.0 |

<그림 4-30> 전자기술 설치시 노동자 참여 필요성에 대한 인식




### 5) 전자기술 사용의 효과에 대한 인식

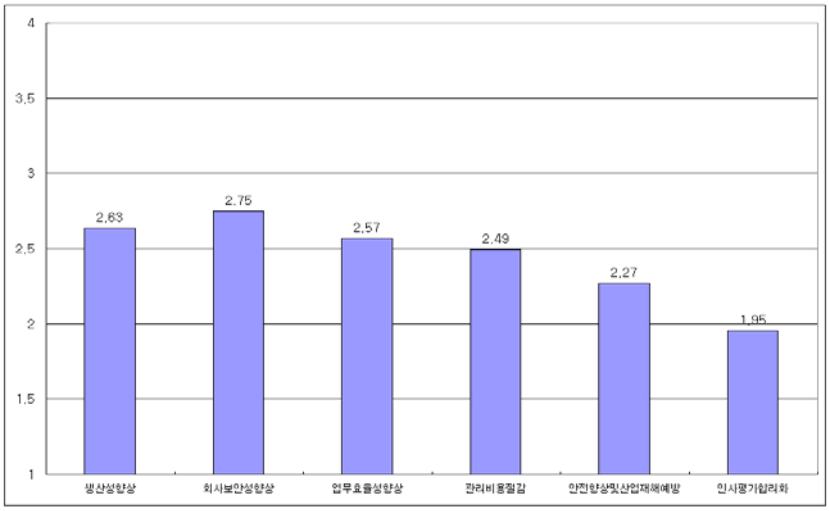
전자기술이 사용됨으로서 어떠한 결과를 초래할 수 있는지에 대한 노동자의 인식을 알아보았다. 전자기술의 사용효과에 대해서는 그 동안 노-사간에 상이한 시각이 존재하여 갈등의 소지가 존재하는 것으로 알려져 왔다. 기업 측에서 전자기술사용을 정당화하기 위한 근거로 사용되고 있는 생산성 향상, 회사보안향상, 업무효율성 향상, 관리비용절감, 안전 및 산재예방과 인사평가합리화에 대한 노동자의 인식을 먼저 알아보았다.

각각의 항목에서 '전혀 그렇지 않다'는 1점으로 '매우 그렇다'는 4점으로 점수화하여 알아 본 결과, 전자기술 효과에 관한 사항 중 회사와 관련되어서는 전자기술이 회사의 보안성을 향상시키는데 가장 도움이 되는 것으로 인식하고 있는 것으로 나타났으며 그 뒤를 생산성 향상과 결부되어 있다고 보는 것으로 나타났다. '회사 보안성 향상'은 평균 점수가 2.73점이었으며, '생산성 향상'은 2.63점이었다. 그 다음으로 '업무 효율성 향상'이 2.57점이었으며 '회사관리비용 절감'은 2.49점이었다. '안전 향상 및 산업 재해 예방' 효과는 2.27점이고 '인사 평가 합리화'에 대해서는 1.92점으로 가장 낮았다.

<표 4-31> 전자기술사용효과 1

| | 생산성향상 | 회사보안성 향상 | 업무효율성 향상 | 관리비용 절감 | 안전향상및산업재해예방 | 인사평가합리화 |
|---|---|---|---|---|---|---|
| 평균 | 2.6 | 2.8 | 2.6 | 2.5 | 2.3 | 2.0 |
| 사례수 | 197 | 196 | 193 | 198 | 195 | 197 |

<그림 4-31> 전자기술사용효과 1




* 4점 척도 (1점 거의없음, 2점 약간 있음, 3점 큰 편, 4점 매우 큼)

** 사용하고 있다는 응답자만으로 평균 구성

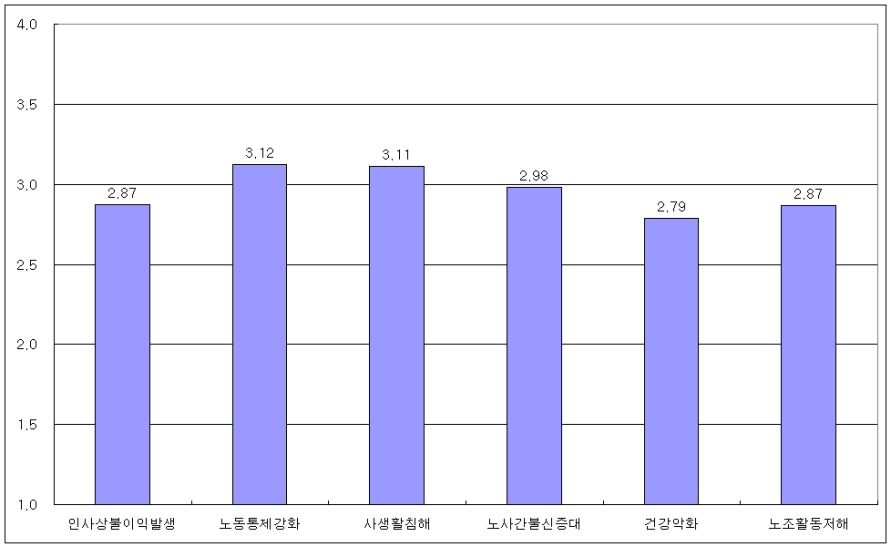
전자감시 기술의 효과 중 주로 노동계에서 문제를 제기했던 측면과 관련해서는 '노동 통제 강화'가 3.12점으로 가장 높았으며, 근소한 차이로 3.11점을 기록한 '사생활침해'가 그 뒤를 이었다. '노사간 불신 증대' 2.98점, '인사상 불이익 발생', '노동조합활동저해' 2.87점, '건강 악화'가 2.79점 순이었다. 노동통제강화는 앞서의 생산성향상을 목적으로 전자기술이 설치되었다는 주장과 상통하는 부분이 있고 사생활침해에 대한 문제의식도 높은 것으로 나타났다. 가장 낮은 점수를 받은 것

은 건강악화였는데 전자기술감시로 인해 건강의 문제가 오기 위해서는 장기간 노출되어야 한다는 점, 전자기술감시를 하고 있는지를 잘 모르고 있다는 점 등으로 인해 건강과의 상관성을 노동자 스스로가 인식하기에는 무리가 있을 수 있기 때문인 것으로 풀이 된다.

<표 4-32> 전자기술 사용효과 2

| | 인사상불이익 발생 | 노동통제강화 | 사생활침해 | 노사간불신증대 | 건강악화 | 노조활동저해 |
|---|---|---|---|---|---|---|
| 평균 | 2.9 | 3.1 | 3.1 | 3.0 | 2.8 | 2.9 |
| 사례수 | 195 | 198 | 198 | 198 | 199 | 198 |

<그림 4-32> 전자기술사용효과 2




* 4점 척도 (1점 거의없음, 2점 약간 있음, 3점 큰 편, 4점 매우 큼)

** 사용하고 있다는 응답자만으로 평균 구성

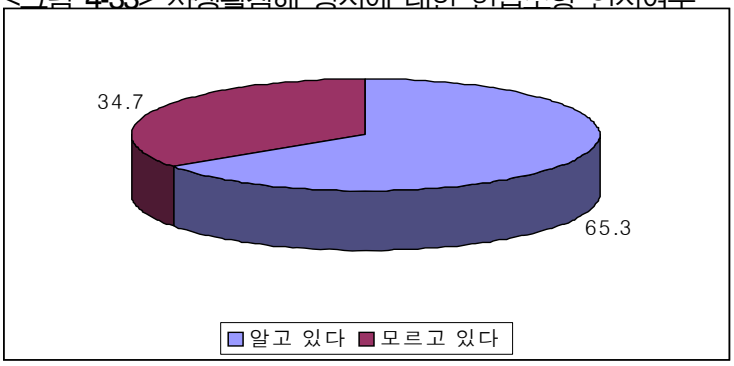
### 6) 전자기술사용 규제의 필요성과 대책

전자기술을 이용하여 노동자를 관찰, 감시하는 것에 대한 규제의 필요성과 향후 대책에 관해 알아보았다. 먼저 인권 침해 방지를 위해 헌법 17조에 명시되어 있는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다"라고 명시한 사실에 대해 인지하고 있는지 알아보았다. 전체 응답자의 절반이 넘는 65.3%가 '알고 있다'고 응답하였으며 '모르고 있다'라고 응답한 비율은 34.7%로 나타났다.

<표 4-33> 사생활침해 방지에 대한 헌법조항 인지여부

| | 알고 있다 | 모르고 있다 | 전체 |
|---|---|---|---|
| 사례수 | 132 | 70 | 202 |
| 백분율 | 65.3 | 34.7 | 100.0 |

<그림 4-33> 사생활침해 방지에 대한 헌법조항 인지여부



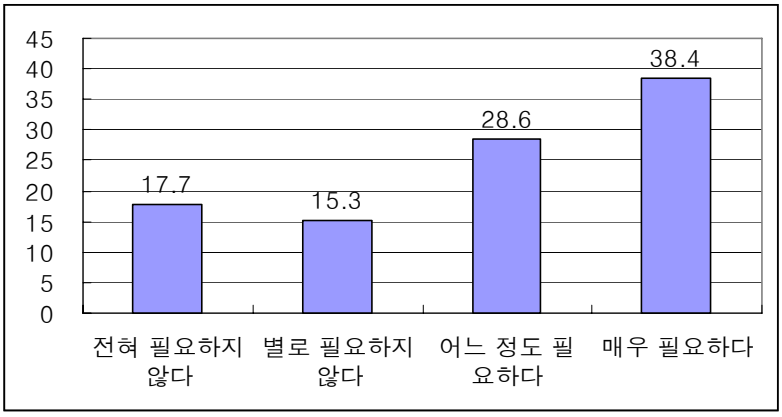

전자 기술을 활용한 회사의 노동자 관찰 및 감시에 대한 규제가 있어야 하는가에 대해 '어느 정도 필요하다'는 응답은 28.6%, '매우 필요하다'는 응답은 38.4%로 나타나, 규제의 필요성에 대해서는 67.0%가 공감하고 있었다. 반면 '전혀 필요

하지 않다'는 17.7%, '별로 필요하지 않다'는 15.3%로 나타나 전체 33.0%는 감시에 대한 규제가 별로 필요하다고 느끼고 있지 않은 것으로 나타났다.

<표 4-34> 전자기술감시에 대한 규제의 필요성

| | 전혀 필요하지 않다 | 별로 필요하지 않다 | 어느 정도 필요하다 | 매우 필요하다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 36 | 31 | 58 | 78 | 203 |
| 백분율 | 17.7 | 15.3 | 28.6 | 38.4 | 100.0 |

<그림 4-34> 전자기술 감시에 대한 규제의 필요성




전자기술 감시에 대한 규제의 필요성을 느끼는 정도가 성별, 연령, 최종학력, 소득, 직장근속년수, 노조가입여부, 사업장 규모, 직업, 노사간 신뢰 정도, 감시를 목적으로 전자기술 사용인식, 감시 사례수 등에 따라 달라지는가를 살펴본 결과, 학력과 노사간 신뢰정도가 유의미한 것으로 나타났다. 학력의 경우 중졸이하집단과 고졸집단간의 차이가 명확하게 나타나, 고졸집단이 높은 수준의 동의에 비해 중졸이하는 이보다 낮게 나타났다. 다른 학력 집단과의 편차는 무의미했다.

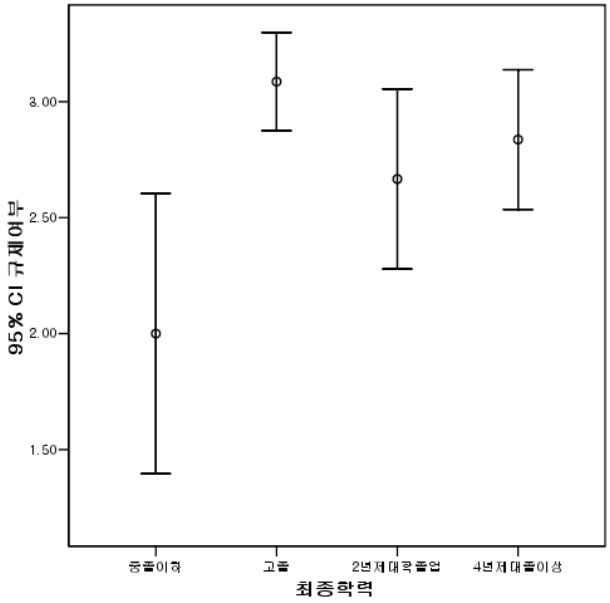
<표 4-35> 학력 집단별 규제 필요성 평균차이

| (I) 학력 | (J) 학력 | 평균차 (I-J) | 표준오차 | 유의확률 |
|---|---|---|---|---|
| 중졸이하 | 고졸 | -1.09(**) | 0.3 | 0.0 |
| | 2년제대학졸업 | -0.7 | 0.4 | 0.3 |
| | 4년제대졸이상 | -0.8 | 0.3 | 0.1 |

** P < 0.01

※ 4점 척도. 전혀 필요하지 않다 1점에서 매우 필요하다 4점까지. Scheffe test 결과

<그림 4-35> 학력 집단별 규제 필요성 평균 오차 그래프




* 4점 척도. 전혀 필요하지 않다 1점에서 매우 필요하다 4점까지, 유의수준 95%

노사 간 신뢰 정도에 따른 차이는 '별로 신뢰하지 않는다'라고 응답한 집단과 '신뢰하고 있는 편이다'고 응답한 집단간 차이로 나타났다. '별로 신뢰하지 않는다'

고 응답한 사람들이 규제의 필요성을 상대적으로 높게 공감하고 있었던 반면, '신뢰하고 있는 편이다'라고 응답한 사람들의 경우 상대적으로 규제의 필요성을 느끼지 않고 있었다.

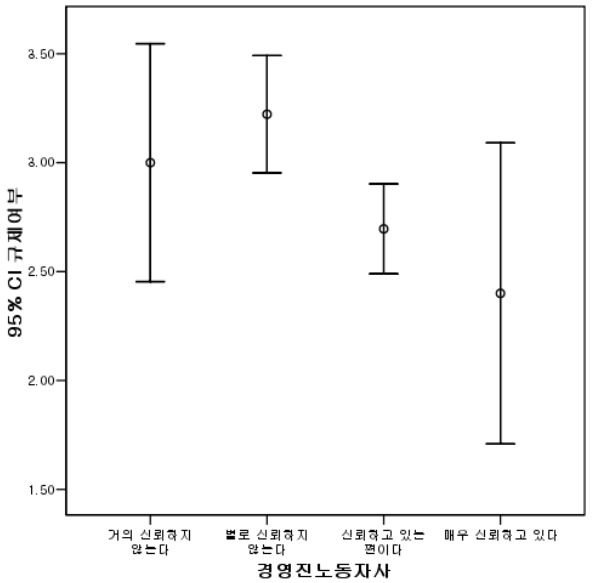
<표 4-36> 노사간 신뢰정도별 규제 필요성 평균차이

| (I) 노사간신뢰정도 | (J) 노사간신뢰정도 | 평균차 (I-J) | 표준오차 | 유의확률 |
|---|---|---|---|---|
| 별로 신뢰하지 않는다 | 거의 신뢰하지 않는다 | 0.2 | 0.3 | 0.9 |
| | 신뢰하고 있는 편이다 | 0.5 (**) | 0.2 | 0.0 |
| | 매우 신뢰하고 있다 | 0.8 | 0.4 | 0.2 |

** P< 0.01. Scheffe test 결과

※ 4점 척도. 전혀 필요하지 않다 1점에서 매우 필요하다 4점까지.

<그림 4-36> 노사간 신뢰정도별 규제 필요성 평균오차 그래프



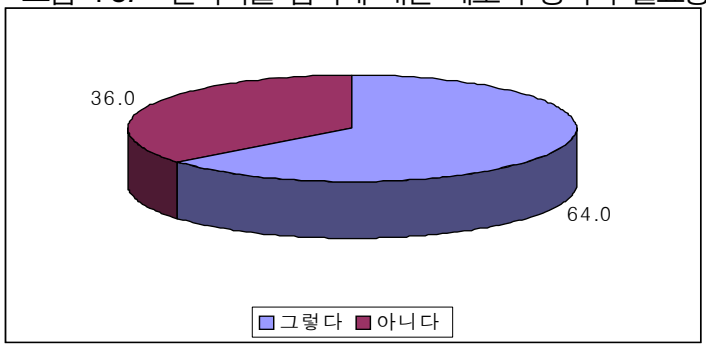

※ 4점 척도. 전혀 필요하지 않다 1점, 매우 필요하다 4점, 유의수준 95%

전자 기술을 활용한 회사의 노동자 관찰 및 감시에 대한 규제를 담당하는 제도적 장치가 필요한가에 대해서 '그렇다'는 응답이 64.0%로 나타났으며 '아니다'라는 응답은 36.0%로 나타났다.

<표 4-37> 전자기술 감시에 대한 제도적 장치의 필요성

| | 그렇다 | 아니다 | 전체 |
|---|---|---|---|
| 사례수 | 130 | 73 | 203 |
| 백분율 | 64.0 | 36.0 | 100.0 |

<그림 4-37> 전자기술 감시에 대한 제도적 장치의 필요성




전자기술 감시에 대한 제도적 장치의 필요성을 느끼는 정도가 성별, 연령, 최종학력, 소득, 직장근속년수, 노조가입여부, 사업장 규모, 직업, 노사간 신뢰 정도, 감시목적으로 전자기술 사용, 감시 사례수 등에 따라 달라지는가를 살펴본 결과, 학력만이 유의미한 것으로 나타났다. 중졸이하집단과 다른 모든 학력 집단과의 명확하게 나타나, 중졸이하의 사람들의 경우 제도적 장치의 필요성을 느끼지 못하였으나 다른 집단은 모두 필요성을 느끼고 있는 것으로 나타났다.

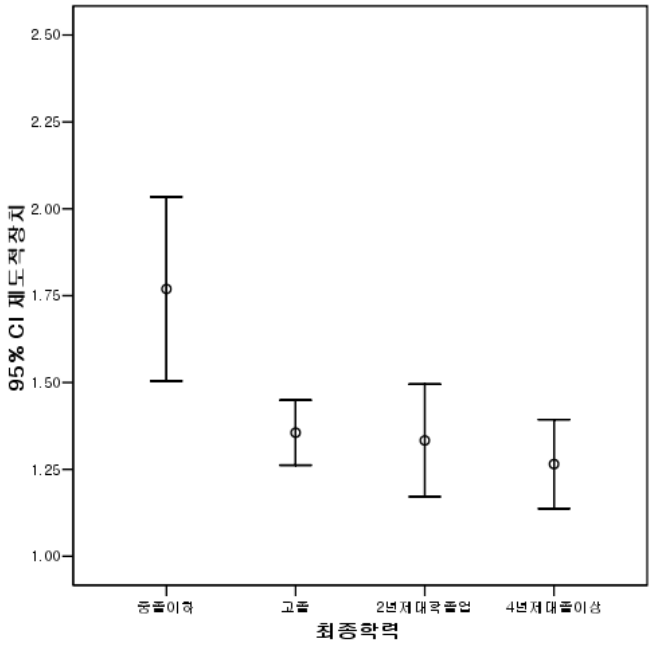
<표 4-38> 학력 집단별 전자감시기술에 대한 제도적 장치의 필요성 평균차이

| (I) 학력 | (J) 학력 | 평균차 (I-J) | 표준오차 | 유의확률 |
|---|---|---|---|---|
| 중졸이하 | 고졸 | 0.4 (**) | 0.1 | 0.0 |
| | 2년제대학졸업 | 0.4 (**) | 0.2 | 0.0 |
| | 4년제대졸이상 | 0.5(**) | 0.1 | 0.0 |

** P < 0.01

※ 1점 필요하지 않다, 2점 필요하다. Scheffe test 결과

<그림 4-38> 학력 집단별 제도적 장치의 필요성 평균오차 그래프




* 1점 : 그렇다 2점: 아니다. 유의수준 95%

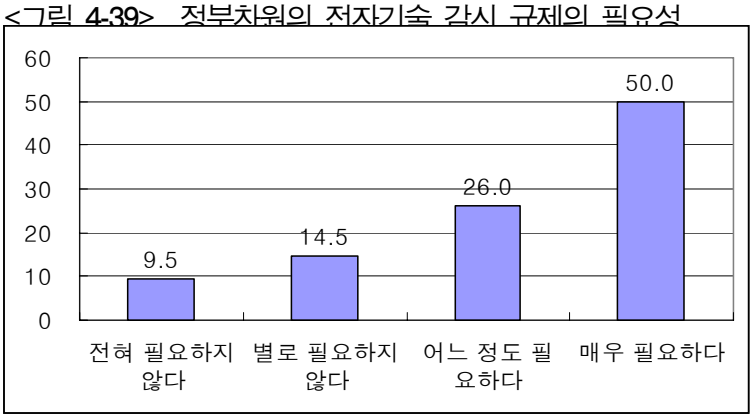
회사가 전자기술을 통하여 노동자를 관찰 또는 감시하는 것을 규제하는 제도나 규정이 정부의 법안, 회사 내의 업무규정, 단체협약 등 노사간 합의문 각각에 어느 정도 필요하다고 보는지에 대해 알아보았다.

회사의 전자기술을 통한 노동자 관찰 및 감시의 규제 수준과 관련하여 정부차원의 법안이 '어느 정도 필요하다'는 응답은 26.0%, '매우 필요하다'는 응답은 절반인 50.0%로 나타나 필요성에 공감하는 전체 비율은 76.0%였다. 한편 정부차원의 법안이 '전혀 필요하지 않다'는 응답은 9.5%, '별로 필요하지 않다'라는 응답은 14.5%로 나타나 필요하지 않다는 응답은 전체의 24.0%에 불과했다.

<표 4-39> 정부차원의 전자기술 감시 규제의 필요성

| | 전혀 필요하지 않다 | 별로 필요하지 않다 | 어느 정도 필요하다 | 매우 필요하다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 19 | 29 | 52 | 100 | 200 |
| 백분율 | 9.5 | 14.5 | 26.0 | 50.0 | 100.0 |

<그림 4-39> 정부차원의 전자기술 감시 규제의 필요성

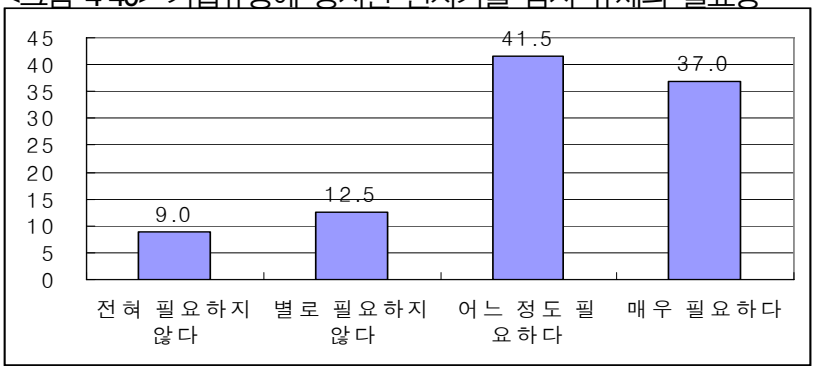


한편 회사의 전자기술을 통한 노동자 관찰 및 감시의 규제 수준과 관련하여 회사 내 업무 규정 수준이 '어느 정도 필요하다'는 응답은 41.5%, '매우 필요하다'는 응답은 37.0%로 나타나 필요성에 공감하는 전체 비율은 78.5%로 높게 나타났다. 그러나 '전혀 필요하지 않다'는 응답 9.0%, '별로 필요하지 않다'라는 응답 12.5%가 있어 필요하지 않다는 응답은 전체의 21.5%로 나타났다.

<표 4-40> 기업규정에 명시된 전자기술 감시 규제의 필요성

| | 전혀 필요하지 않다 | 별로 필요하지 않다 | 어느 정도 필요하다 | 매우 필요하다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 18 | 25 | 83 | 74 | 200 |
| 백분율 | 9.0 | 12.5 | 41.5 | 37.0 | 100.0 |

<그림 4-40> 기업규정에 명시된 전자기술 감시 규제의 필요성



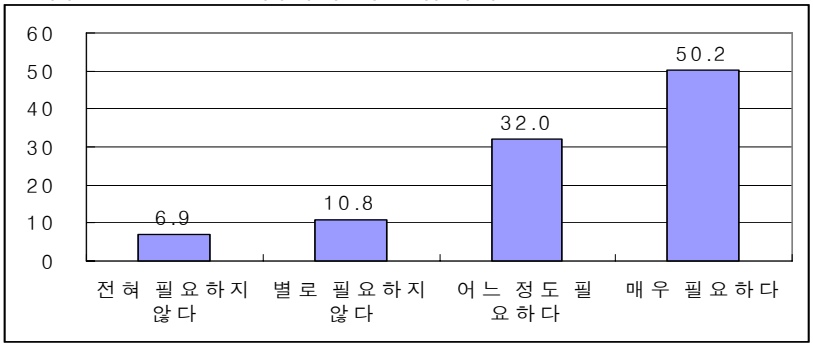

회사의 전자기술을 통한 노동자 관찰 및 감시의 규제 수준과 관련하여 각 사업장의 이해 당사자인 노사간의 합의문 수준의 필요성에 대해서 알아보았다. 노사간 합의문은 '어느 정도 필요하다'는 응답은 32.0%, '매우 필요하다'는 응답은 절반인 50.2%로 나타나 필요성에 공감하는 전체 비율은 82.2%로 노동자 관찰 및 감

시의 규제와 관련하여 노사간 합의에 대한 필요성이 정부차원의 법이나 회사 내 업무규정보다 높게 나타났다.

<표 4-41> 노사간 합의에 의한 규제의 필요성

| | 전혀 필요하지 않다 | 별로 필요하지 않다 | 어느 정도 필요하다 | 매우 필요하다 | 전체 |
|---|---|---|---|---|---|
| 사례수 | 14 | 22 | 65 | 102 | 203 |
| 백분율 | 6.9 | 10.8 | 32.0 | 50.2 | 100.0 |

<그림 4-41> 노사간 합의에 의한 규제의 필요성

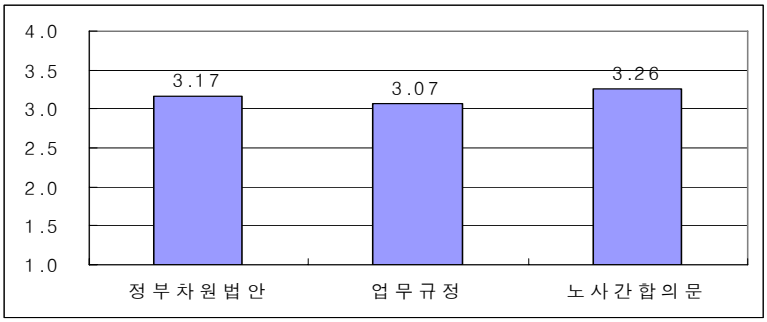



전자기술을 감시의 목적으로 사용하는 것에 대한 규제의 수준을 정부차원의 법안, 회사 내의 업무규정, 단체협약 등 노사간 합의문에서 얼마나 공감하고 있는지를 알아보았다. 전체 응답을 '전혀 필요하지 않다'를 1점에서 '매우 필요하다' 4점으로 점수화하여 알아본 결과 '노사간 합의문'이 3.26점으로 가장 높았고, '정부차원의 법안'이 3.17점, '업무 규정'이 3.07점으로 나타났다. 즉, 모든 영역에서 중간점 이상의 필요성을 느끼고 있으나 특히 노사간 합의의 형태에 관한 점수가 가장 높아 실제 직장에서 적용될 수 있는 규제의 필요가 높은 것으로 나타났다.

<표 4-42> 전자감시규제의 다양한 제도적 방안에 대한 필요성

| | 정부차원법안 | 업무규정 | 노사간합의문 |
|---|---|---|---|
| 평균 | 3.17 | 3.07 | 3.26 |
| 사례수 | 200 | 200 | 203 |

<그림 4-42> 전자감시규제의 다양한 제도적 방안에 대한 필요성




* 4점 척도 (1점 거의 없음, 2점 약간 있음, 3점 큰 편, 4점 매우 큼), 2.5점이 준거점

** 사용하고 있다는 응답자만으로 평균 구성

### 7) 전자감시 규정의 구성

전자감시 규정이 작성된다면 어떤 내용으로 구성되어야 할 것인지에 대해 알아보았다. 총 10개의 문항으로 감시규정의 내용을 구성하여 각각의 필요도를 알아보아 향후 우리사회의 감시규정의 근간으로 삼고자 하였다.

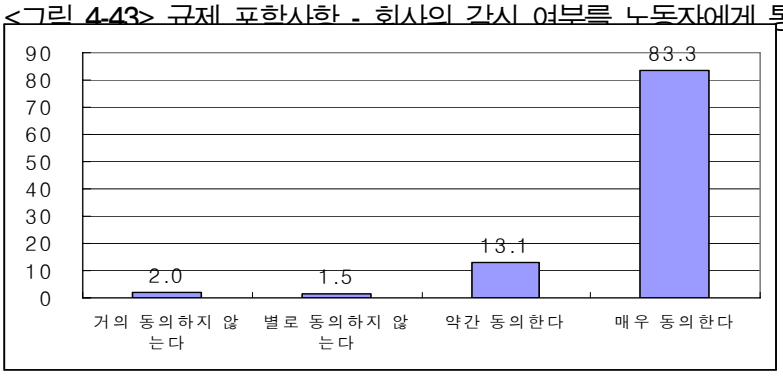
### (1) 회사의 감시 여부 통보

규제를 위한 규정에 포함될 사항으로 회사에 감시 여부를 통보해야 할 의무를 부여하는 것에 대해 어느 정도 동의하는가에 대해 '거의 동의 하지 않는다'는 2.0%, '별로 동의하지 않는다'는 1.5%로 3.5%에 불과했다. 이에 반해, '약간 동의한다'는 13.1%였으며 '매우 동의한다'는 다수인 83.3%를 기록했다. 절대 다수라 할 수 있는 96.4%가 회사가 감시여부를 통보해야 한다는 것에 동의하는 것으로 나타났다.

<표 4-43> 규제 포함사항 - 회사의 감시 여부를 노동자에게 통보

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 2.0 | 1.5 | 13.1 | 83.3 | 100.0 |
| 사례수 | 4 | 3 | 26 | 165 | 198 |

<그림 4-43> 규제 포함사항 - 회사의 감시 여부를 노동자에게 통보



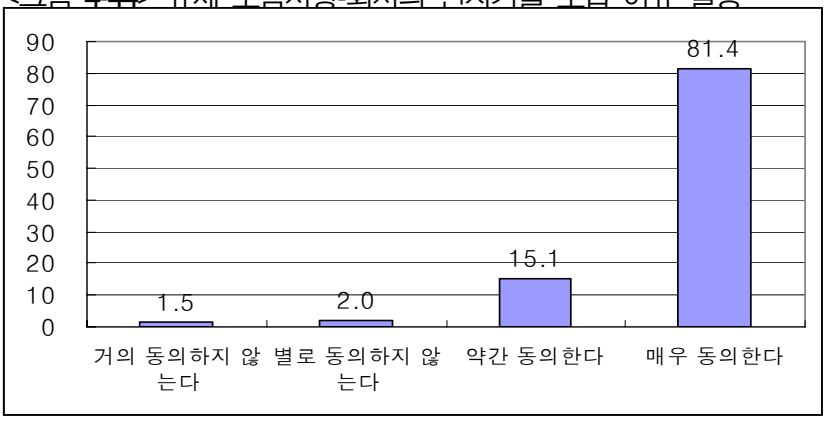
### (2) 회사의 전자기술 도입 이유 설명

회사가 노동자에게 특정 전가 기술을 도입할 때 그 이유를 설명해야 한다는 사항에 대해서도 '약간 동의한다'는 15.1%였으며 '매우 동의한다'는 다수인 81.4%를 기록하여 96.5%가 동의하는 것으로 나타났다. 이에 반해 '거의 동의 하지 않는다'는 1.5%, '별로 동의하지 않는다'는 2.0%로 3.5%에 불과했다.

<표 4-44> 규제 포함사항 - 회사의 전자기술 도입 이유 설명

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 1.5 | 2.0 | 15.1 | 81.4 | 100.0 |
| 사례수 | 3 | 4 | 30 | 162 | 199 |

<그림 4-44> 규제 포함사항-회사의 전자기술 도입 이유 설명



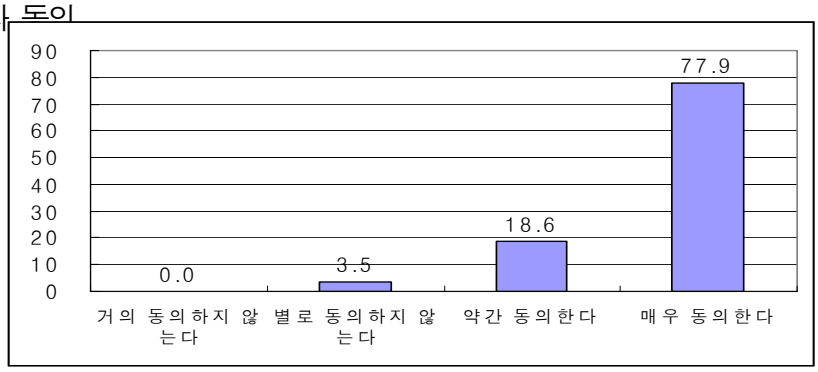
### (3) 새로운 전자감시시스템 도입, 설치에 관한 노동자 동의

새로운 전자감시 시스템을 도입 및 설치 할 때 노동자가 동의해야 한다는 항목을 포함시켜야 한다는 의견에 대해 '거의 동의 하지 않는다'는 한 명도 없었으며, '별로 동의하지 않는다'는 3.5%에 불과했다. 이에 반해, '약간 동의한다'는 18.6%였으며 '매우 동의한다'는 다수인 77.9%를 기록하여 96.5%가 동의하는 것으로 나타났다.

<표 4-45> 규제 포함사항 - 새로운 전자감시시스템의 도입, 설치에 관한 노동자의 동의

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 시스템 결측값 |
|---|---|---|---|---|---|
| 백분율 | 0.0 | 3.5 | 18.6 | 77.9 | 100.0 |
| 사례수 | 7 | 37 | 155 | 199 | 5 |

<그림 4-45> 규제 포함사항 - 새로운 전자감시 시스템 도입, 설치에 관한 노동자 동의



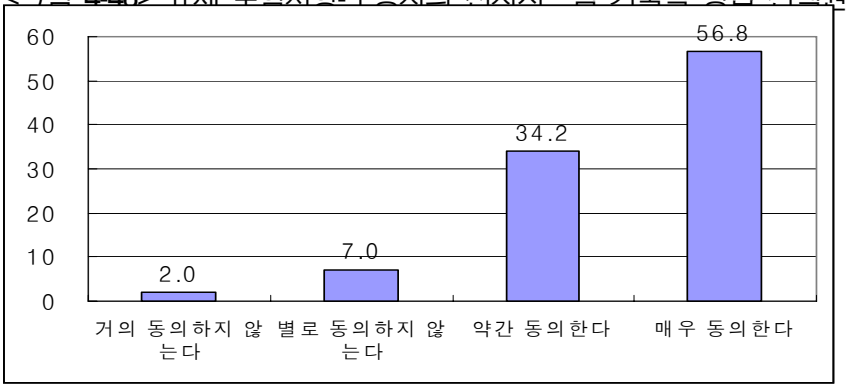
### (4) 노동자의 전자시스템 기술적 방법 선택권

다양한 전자기술이 사용되고 있는 가운데 전자기술을 선택할 수 있는 규정에 대한 동의 정도에 대해 알아보았다. 노동자가 전자시스템의 기술적 방법에 관한 선택권을 가져야 한다는 것에 대해서는 '거의 동의 하지 않는다'는 2.0%, '별로 동의하지 않는다'는 7.0%로 9.0%가 노동자의 기술적 방법 선택권에 동의하지 않았다. 이에 반해, '약간 동의한다'는 34.2%였으며 '매우 동의한다'는 절반을 넘어서는 56.8%로 전체 동의자는 응답자의 91.0%로 나타났다.

<표 4-46> 규제 포함사항 - 노동자의 전자시스템 기술적 방법 선택권

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 2.0 | 7.0 | 34.2 | 56.8 | 100.0 |
| 사례수 | 4 | 14 | 68 | 113 | 199 |

<그림 4-46> 규제 포함사항-노동자의 전자시스템 기술적 방법 선택권



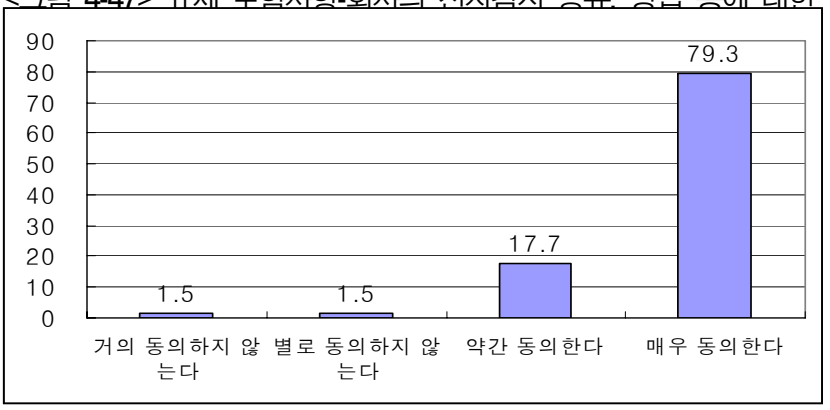
### (5) 회사의 전자감시 종류, 방법, 감시시기 및 기간에 대한 설명

회사가 전자 감시의 종류, 방법 그리고 감시 시기 및 기간에 대한 설명을 해야 한다는 부분에 대해서는 '약간 동의한다'는 17.7%, '매우 동의한다'는 다수인 79.3%로 전체 동의자는 응답자의 97.0%로 나타났다. '거의 동의하지 않는다'는 1.5%, '별로 동의하지 않는다'는 1.5%로 3.0%가 회사의 전자감시 종류, 방법, 감시 시기 및 기간에 대한 설명 의무에 동의하지 않았다.

<표 4-47> 규제 포함사항 - 회사의 전자감시 종류, 방법 등에 관한 설명

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 1.5 | 1.5 | 17.7 | 79.3 | 100.0 |
| 사례수 | 3 | 3 | 35 | 157 | 198 |

<그림 4-47> 규제 포함사항-회사의 전자감시 종류, 방법 등에 대한 설명



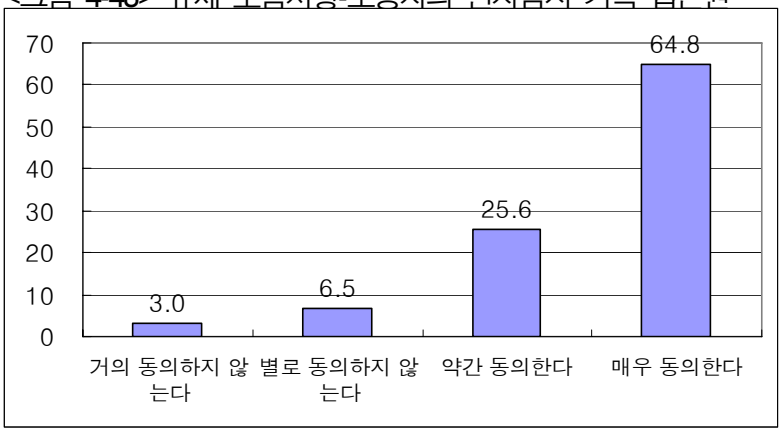
### (6) 노동자의 전자감시 기록 접근권

노동자가 전자감시 기록에 대한 접근권을 가져야 한다는 항목에 대해서는 '거의 동의 하지 않는다'는 3.0%, '별로 동의하지 않는다'는 6.5%로 9.0%가 노동자의 전자감시 기록 접근권에 동의하지 않았다. '약간 동의한다'는 25.6%, '매우 동의한다'는 64.8%로 전체 동의자는 응답자의 90.4%로 나타났다.

<표 4-48> 규제 포함사항 - 노동자의 전자 감시 기록 접근권

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 3 | 6.5 | 25.6 | 64.8 | 100 |
| 사례수 | 6 | 13 | 51 | 129 | 199 |

<그림 4-48> 규제 포함사항-노동자의 전자감시 기록 접근권



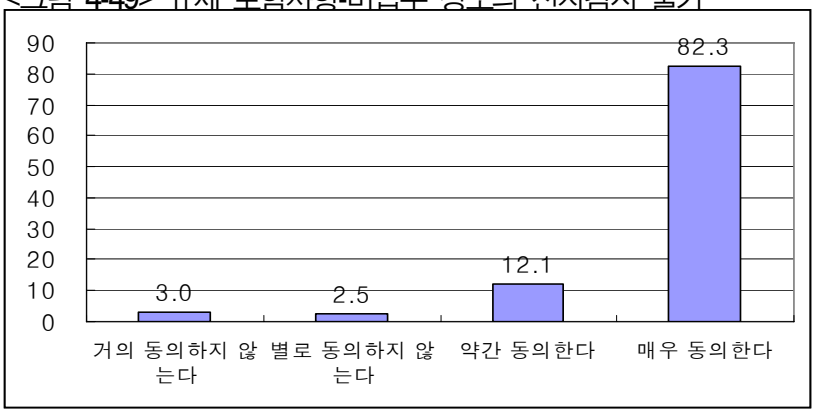
### (7) 비업무 장소의 전자감시 불가

일과 관련되지 않은 비업무 장소에서의 전자 감시를 불가해야 한다는 항목에 대해서 '약간 동의한다'는 12.1%, '매우 동의한다'는 82.3%로 전체 동의자는 응답자의 94.4%로 나타났다. '거의 동의 하지 않는다'는 3.0%, '별로 동의하지 않는다'는 2.5%로 5.5%가 비업무 장소의 전자감시 불가에 동의하지 않았다.

<표 4-49> 규제 포함 사항 - 비업무 장소외 감시 불가

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 3.0 | 2.5 | 12.1 | 82.3 | 100.0 |
| 사례수 | 6 | 5 | 24 | 163 | 198 |

<그림 4-49> 규제 포함사항-비업무 장소의 전자감시 불가



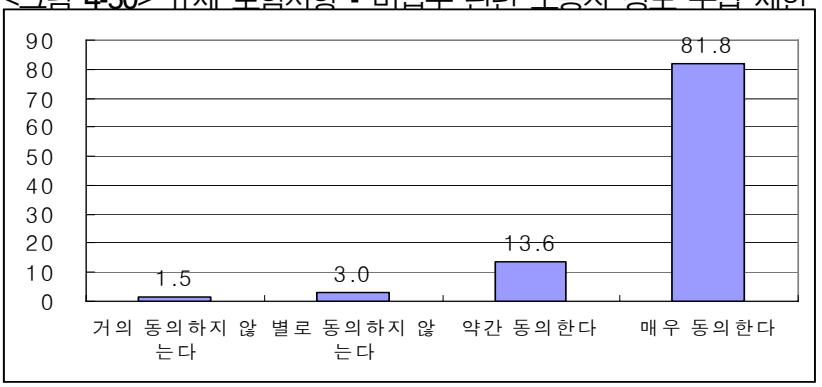
### (8) 비업무 관련 노동자 정보 수집 제한

비업무 관련 노동자 정보 수집을 제한해야 하는가의 항목에 대해서 '거의 동의 하지 않는다'는 1.5%, '별로 동의하지 않는다'는 3.0%로 전체의 4.5%가 동의하지 않았다. '약간 동의한다'는 13.6%, '매우 동의한다'는 81.8%로 전체 동의자는 응답자의 95.4%로 나타났다.

<표 4-50> 규제 포함 사항 - 비업무 관련 노동자 정보 수집 제한

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 1.5 | 3.0 | 13.6 | 81.8 | 100.0 |
| 사례수 | 3 | 6 | 27 | 162 | 198 |

<그림 4-50> 규제 포함사항 - 비업무 관련 노동자 정보 수집 제한



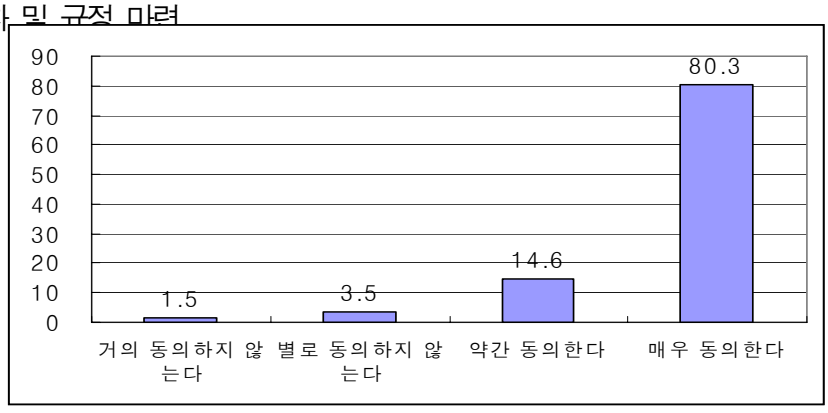
### (9) 부적절한 감시 자료나 해석에 관한 이의 제기 절차 및 규정 마련

부적절한 감시 자료나 해석에 관한 이의 제기를 할 수 있는 절차 및 규정이 마련되어야 하는가의 항목에 대해서 '약간 동의한다'는 14.6%, '매우 동의한다'는 80.3%로 전체 동의자는 응답자의 94.9%로 나타났다. '거의 동의 하지 않는다'는 1.5%, '별로 동의하지 않는다'는 3.5%로 전체의 5.0%가 동의하지 않았다.

<표 4-51> 규제 포함 사항 - 부적절한 감시자료/해석에 관한 이의 제기 절차 및 규정 마련

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 1.5 | 3.5 | 14.6 | 80.3 | 100.0 |
| 사례수 | 3 | 7 | 29 | 159 | 198 |

<그림 4-51> 규제 포함사항 - 부적절한 감시 자료·해석에 관한 이의 제기 절차 및 규정 마련



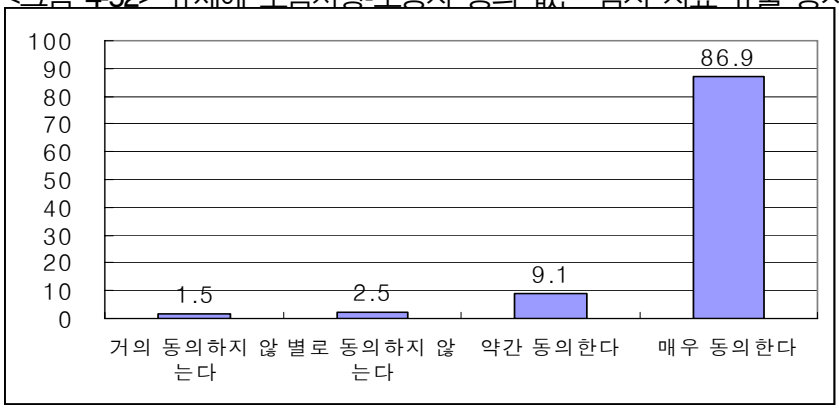
### (10) 노동자 동의 없는 감시 자료 유출 방지

노동자의 동의가 없는 전자 감시 자료의 유출을 방지해야 하는가의 항목에 대해 '거의 동의 하지 않는다'는 1.5%, '별로 동의하지 않는다'는 2.5%로 전체의 4.0%가 동의하지 않았다. '약간 동의한다'는 9.1%, '매우 동의한다'는 86.9%로 전체 동의자는 응답자의 96.0%로 나타났다.

<표 4-52> 규제 포함 사항 - 노동자 동의없는 감시 자료 유출 방지

| | 거의 동의하지 않는다 | 별로 동의하지 않는다 | 약간 동의한다 | 매우 동의한다 | 전체 |
|---|---|---|---|---|---|
| 백분율 | 1.5 | 2.5 | 9.1 | 86.9 | 100.0 |
| 사례수 | 3 | 5 | 18 | 172 | 198 |

<그림 4-52> 규제에 포함사항-노동자 동의 없는 감시 자료 유출 방지




이상 노동자를 관찰, 감시하는 규정이 마련될 경우 포함될 수 있는 사항에서 동의 여부를 물은 평균 점수를 알아보았다. 각 항목에 '거의 그렇지 않다'는 1점

부터 '매우 그렇다'는 4점으로 점수화하여 어떤 항목이 특히 전자기술 감시의 규제 조항에 삽입되어야 하는지를 알아보았다.

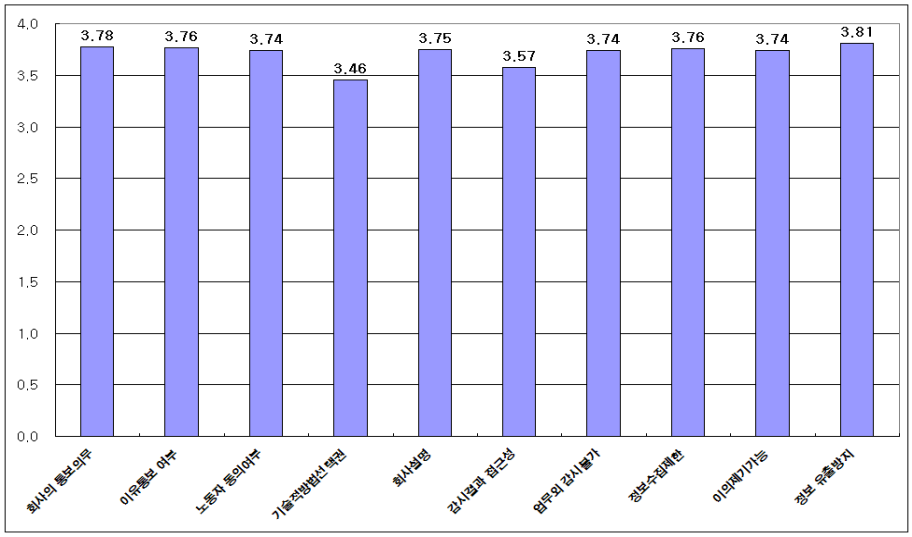
전체적으로 보았을 때 평균이 3.71로 모든 항목에서 매우 높은 수준의 동의가 이루어지고 있음을 알 수 있다. 가장 높은 점수를 얻은 항목은 3.81점을 얻은 전자기술로 인해 얻게 된 정보가 노동자의 동의 없이 유출되어서는 안 된다는 것이었다. 그 다음으로, 회사가 전자감시기술을 이용하여 노동자를 감시하고 있다는 사실을 통보해 주어야할 의무는 3.78점, 전자감시기술 도입의 이유를 통보해야 한다는 것과 전자기술로 인해 얻는 정보가 제한적이어야 한다는 것이 동일하게 3.76점으로 나타났다. 회사가 전자기술의 종류와 내용을 설명해주어야 한다는 것이 3.75점으로 나타났으며, 전자감시기술을 도입할 때 노동자의 동의를 얻어야 한다는 것, 전자기술을 업무외 감시가 불가능하게 해야 한다는 점, 전자기술로 인해 부적절한 정보가 수집되는 것에 대해 이의제기가 가능해야 한다는 것이 3.74점으로 나타났다. 그 외 전자기술에 대한 노동자의 기록접근권은 3.57점이었으며, 가장 낮은 점수는 도입되는 전자기술의 기술적 방법 선택권이었는데 3.46점이었다.

<표 4-53> 전자기술로 인한 노동자 감시규제의 내용 동의 평균치

| | 평균 | 사례수 |
|---|---|---|
| 회사의 통보의무 | 3.78 | 198 |
| 이유통보 여부 | 3.76 | 199 |
| 노동자 동의여부 | 3.74 | 199 |
| 기술적방법선택권 | 3.46 | 199 |
| 회사설명 | 3.75 | 198 |
| 감시결과 접근성 | 3.57 | 199 |
| 업무외 감시불가 | 3.74 | 198 |
| 정보수집제한 | 3.76 | 198 |
| 이의제기가능 | 3.74 | 198 |
| 정보 유출방지 | 3.81 | 198 |

* 4점 척도 (1점 거의없음, 2점 약간 있음, 3점 큰 편, 4점 매우 큼)

<그림 4-53> 전자기술로 인한 노동자 감시규제의 내용 동의 정도




* 4점 척도 (1점 거의 없음, 2점 약간 있음, 3점 큰 편, 4점 매우 큼)

## 3. 요약 및 함의

본 조사에서는 204명의 노동자를 대상으로 전자기술 사용실태, 전자기술 감시에 대한 인식, 전자감시에 대한 규제의 필요성과 향후 대안을 알아보기 위해 설문지를 분석하였다.

조사대상자는 평균 2.36개의 전자기술에 노출되고 있다고 응답했으며 현재 활용되고 있는 기술 중 가장 많은 것이 인터넷이용모니터링이었고 그 뒤를 전자신분증, ERP, CCTV, 컴퓨터 하드디스크 모니터링, 전화송수신 내역기록 등의 순으로 나타났으며 RFID와 지문 및 생체인식이 가장 낮게 나타났다. 한편 설문지에 나열된 전자기술 중 현재 사업장에서 사용하고 있는지를 '모르겠다'는 비율이 가장 높았던 것은 전화송수신내역 기록여부(35.2%)였고 컴퓨터 하드디스크 모니터링(30.6%), ERP(24.7%), 인터넷 사용모니터링(18.1%), RFID(17.7%), 지문 및 생체 인

식체계 사용여부(10.8%), CCTV(6.3%), 전자신분증(5.3%)의 순으로 나타나 각 기술의 활용여부를 제대로 인식하고 있지 못한 응답자가 다수 존재하고 전자기술유형에 따른 불확실성의 정도가 상이한 것으로 나타났다. 특히 많은 노동자들이 활용하고 있는 전화 및 컴퓨터 하드디스크 모니터링이 실제 노동자 감시에 활용되고 있는지를 알고 있지 못한 비율이 상대적으로 높은 것으로 나타나 전자감시에 대한 불확실성이 일상에서 높은 것으로 풀이된다.

전체적으로 현재 직장에서 사용되고 있는 전자기술의 사용목적, 수집된 정보의 내용, 수집된 정보의 활용방안에 대해 상당수의 노동자가 알고 있지 못한 것으로 나타났다. 현재의 직장에서 사용되고 있는 전자기술의 목적에 대해서는 46.0%가 모른다고 하였고 특히 학력간 차이가 심하여 중졸이하 학력을 가진 노동자는 중졸이상 학력의 노동자보다 전자기술의 목적에 대해 상대적으로 인지도가 떨어지고 있는 것으로 나타났다. 전자기술이 수집하고 있는 정보의 내용을 모르는 응답자도 69%에 이르렀고 전체 응답자의 74.6%는 수집된 정보가 어떻게 활용되고 있는지를 모르고 있는 것으로 나타났다.

노동자가 전자기술사용에 대해 느끼는 불안감은 전자기술별로 차이가 나는 것으로 보인다. 불안감의 정도를 1-4점의 범위로 볼 때 지문 및 생체인식이 3.75점으로 가장 높았으며 그 다음으로 RFID 3.54점, CCTV(3.38점), 전화송수신 내역 모니터링(3.28점), ERP(3.19점), 출입카드(3.07점), 하드 디스크 모니터링(2.91점), 인터넷 모니터링(2.82점) 순으로 불안하게 느끼고 있었다.

현재 직장에 설치된 전자기술이 노동자를 관찰, 감시하기 위한 목적이라고 인식한 노동자는 '잘 모르겠다'는 응답자를 제외하고는 26.1%였고 업무효율성 및 생산성 향상이 목적이라고 본 응답자는 73.9%로 나타났다. 전체적으로 업무와 생산성 향상을 위해 전자기술이 도입되었다고 보고 있지만 4명 중 1명은 노동자의 감시가 주요 목적이라고 보고 있는 것으로 나타났다. 직장에서 사용되고 있는 전자기술이 도입될 때 노동자 개인이나 노동자의 대표기구에 전자기술의 설치여부와 장소활용방안 등을 고지한 비율은 약 20-30%에 불과하며 대부분은 아무말 없이 설치했거나 설치 후 에 통보한 것으로 나타났다.

전자기술을 직장에서 사용하는 이유에 대해서는 그 동안 노-사간의  상이한

인식이 존재한 것으로 알려져 있는데 경영층은 업무의 효율성을 위해 노동자는 노동통제 및 사생활침해라고 맞서 왔다. 본 설문지를 통하여 확인할 수 있었던 사실은 노동자는 전자기술사용으로 인해 노동통제강화(1-4점 범위에서 3.12점)가 가장 심하다고 인식하고 있으며 사생활치매(3.11점), 노사간 불신 증대(2.98점), 인사상 불이익 발생(2.87점), 노동조합활동저해(2.87점), 스트레스 등의 건강악화(2.79점) 순으로 나타났다. 한편 생산성향상(2.6점), 회사보안향상(2.8점), 업무효율성 향상(2.6점), 관리비용절감(2.5점), 안전향상 및 산업재해예방(2.3점), 인사평가합리화(2.0점)는 노동자에게 불리한 효과에 비하면 그 점수가 저조한 것으로 나타났다.

전자기술 설치시 노동자나 노동자대표기구의 참여가 저조한 가운데 전자기술 설치 및 활용시 노동자가 참여해야 한다고 응답한 비율은 매우 높게 나타났다. '경영진의 고유 권한'이므로 노동자가 참여하지 않아야 한다는 2.6%에 불과하였고 적극적인 노동자의 참여(66.5%)나 최소한의 설명이 필요하다(21.1%)는 응답이 높게 나와 노동자의 참여의지가 높았다. 또한 전자기술을 활용한 회사의 노동자 관찰 및 감시에 대한 규제가 필요하고(67.0%), 전자감시에 대한 규제를 담당하는 제도적 장치가 필요하다는 응답이 높게(64.0%) 나타났다. 특히 전자감시에 대한 규제의 필요성과 제도적 장치의 필요성은 중졸이상 학력의 응답자가 중졸이하보다 더 많이 느끼고 있었다. 노사간의 신뢰가 별로 없다고 응답한 노동자는 신뢰가 높은 응답자에 비해 전자감시 규제의 필요성을 더 느끼고 있었다.

회사의 노동자를 대상으로 하는 전자감시규제를 위한 방안으로 회사에서 직접적으로 효력을 가질 수 있는 노-사간의 합의문(4점 만점에서 3.26점)이 가장 주요한 규제방안으로 나타났고 그 뒤를 정부법안(3.17점)으로 나타났으며 회사 내 업무규정에 포함시키자는 방안(3.07점)은 지지가 상대적으로 낮은 것으로 나타났다.

전자감시규제를 위해서 포함되어야 할 내용을 10개의 항목으로 구성한 결과 전체적으로 평균점수가 3.71로 높게 나타나 설문지에서 제시한 규제의 내용 - 회사에 감시여부 통보, 전자기술 도입이유 설명, 전자감시시스템의 도입 및 설치에 관한 노동자 동의, 노동자의 전자시스템 기술 선택권, 회사의 전자감시종류, 방법, 감시시기 및 기간에 대한 설명, 노동자의 전자감시 기록 접근권, 비업무장소외 감

시 불가, 비업무 관련 노동자 정보수집 제한, 부적절한 감시 자료나 해석에 관한 이의제기 및 규정 마련, 노동자 동의 없는 감시자료 유출방지 - 이 모두 필요하다고 인식하고 있다.

조사를 통해서 드러난 바, 현재 직장에서 사용되고 있는 전자기술의 존재, 설치목적 및 활용방식에 대해 감시의 대상이 될 수 있는 노동자가 제대로 인지하고 있지 못한 가운데 노동자의 참여가 보장된 전자감시 규제를 요구하고 있는 것으로 나타났다. 전자기술의 활용이 노동자의 근무조건, 사생활침해, 건강악화 등의 부정적인 효과를 가져 올 소지가 업무의 효율성보다 높으므로 전자기술 활용에 대해서는 규제가 필요하다고 보고 있다.

이러한 규제는 노사가 합의하거나 정부차원에서 이루어지는 규제방식이어야 하고 규제의 내용은 전자기술 설치 논의부터 전자감시 자료의 정보활용 등 포괄적인 내용을 요구하고 있는 것으로 나타났다.

# 5장. 국제 기준과 해외 제도의 사례

## 1. 개요

서구 선진국에서 시민사회 차원의 개인 프라이버시(Privacy)를 보호하기 위한 입법논의는 1970년대에 들어 등장하기 시작한다.(Clarke 1999) 이처럼, 서구 사회에서 개인 사생활 보호에 대한 정책적 관심이 높아지게 된 주된 배경은 George Orwell이 예언하였던 "빅브라더(Big Brother)"감시체제의 도래를 현실적으로 가능하게 만드는 컴퓨터 기술의 눈부신 발달에서 찾을 수 있다. 1980년대에 들어서 정부기관이나 민간기업에 의해 시민들의 개인정보와 사생활 그리고 통신권 등을 침해하는 것을 방지하는 국제적 준칙이 마련되는 한편, 서구 선진국들에서는 각국의 여건에 맞추어 개인 프라이버시를 보호하기 위한 다양한 입법이 추진되었다.

그런데, 시민들의 사생활을 보호하기 위한 관련 입법 논의는 컴퓨터기술이 산업현장에 기본적인 생산수단으로 폭넓게 도입되면서 노동자들의 직무수행과 일상활동에 대한 사용자의 감시수단으로 활용됨에 따라 사업장의 새로운 감시기제에 대한 제도적 규제장치의 마련으로 이어지게 되었다. 국제적인 수준에서도 1980년의 OECD에 의해 「프라이버시의 보호와 개인데이타의 국제적 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data」가 제정되어 선진국을 중심으로 시민들의 프라이버시 보호을 위한 입법이 활발하게 진행되었으며, 뒤이어 1990년대에 들어 국제노동기구(ILO)를 주도하여 산업현장의「노동자의 개인정보 보호를 위한 행동준칙(ILO Code of Practice for Protection of Workers' Personal Data)」가 공포되었던 것이다.

지난 1990년대 이후 정보통신기술(Information-Communication Technology,

ICT)의 급속한 발달에 힘입어 소위 정보사회(information society)로 진입하고 있는 서구 선진국에서는 한편으로 사업장수준의 전자감시(electronic surveillance 또는 electronic monitoring)가 매우 일반화되고 있으며, 다른 한편으로는 이같이 확산되는 노동감시를 규제하기 위한 제도적 장치의 입법조치가 잇따르고 있다. 사업장의 전자감시실태에 대한 상세한 기업조사자료가 존재하는 미국(AMA 2001)을 중심으로 그 추세와 동향을 살펴보면, 1997-2001년 사이에 전화통화・음성메일・컴퓨터파일・이메일・비디오 녹화 등에 대해 감시활동을 실시하고 있는 기업들의 비중이 35.3%에서 70.8%(인터넷접속 감시 포함시 77.1%)로 두배로 증가하였다.[4] 2005년에 시행된 동일 조사(AMA 2005)에 따르면, 미국 기업들은 컴퓨터사용(36%), 컴퓨터파일(50%), 이메일(55%), 인터넷 사용(66%), 전화사용(51%), 음성메일(15%), 비디오녹화(51%) 등에 있어 전체 또는 일부 종업원들에 대한 감시활동을 행하고 있는 것으로 나타났다. 이같이 사업장감시의 증가추세를 반영하듯 미국에서만 전자감시의 대상규모가 1990년대 초반 약 2천만명에서 2005년에 4천만명으로 늘어난 것으로 추산되기도 한다.(Wen & Gershuny 2005)[5] 또한, 호주의 경우에도 전체 기업의 80%가 종업원들에 대한 다양한 감시활동을 수행하는 것으로 조사되고 있다.(OVPC 2003) 이처럼 미국과 호주 등의 서구 선진국에서 사업장감시가 크게 늘어남에 따라 자연히 전자감시의 적법성을 둘러싼 사용자와 노동/시민단체 그리고 법조계간의 논란[6]이 지속되는 가운데, 그 감시활동에 따른 사회적

4) 사업장 전자감시가 이처럼 급속하게 확산되는 배경에는 감시장치의 가격 하락과 성능 향상 및 소형화, 노동자들의 정보통신기술 활용 빈도 증대, 전자감시효과에 대한 사용자들의 과잉믿음과 편의성 등이 주요하게 작용하는 것으로 지적되고 있다.(Kizza & Ssanyu 2005)

5) 온라인 노동인구(Online working population, 컴퓨터를 이용하는 노동인구를 지칭)를 기준으로 할 경우, 2001년 현재 미국에서는 전체 온라인 노동인구 4,000만명의 35%인 1,400만명이, 전세적으로 1억명 중 27%인 2,700만명이 전자통신감시를 받고 있는 것으로 추산하기도 한다.(Schulman 2001)

6) Cripps(2004)에 따르면, 전자감시를 옹호하는 입장의 근거로는 사용자의 재산권 보호와 법적 의무 준수(예: 산업안전 환경 유지, 성희롱 방지), 생산성 향상과 비용절감의 효과적 수단 등이 주장되는 반면, 반대론자의 경우에는 노동자의 사생활/프라이버시와 인격적 존엄성에 대한 침해, 사용자의 부당사용 가능성, 노동강도와 스트레스 증대 및 조직관계 훼손 등을 주요 논거로 지적하고 있다. 이와 관련하여 임상훈(2005)를 참조할 것. 또한, Clarke(1999)는 이같은 사업장감시의 논란을 두고, 노동자의 프라이버시는 단순히 권리의 개념으러 접근하기 보다는 여러 당사자들간의 이해관계문제로 이해해야 한다는 정의를 제시하고 있기도 한다.

우려가 점증함에 따라 국제적으로나 각국별로 관련 규제제도의 도입이 점차 늘어나고 있는 것이다.

이 장에서는 우리나라에서 사업장감시와 관련된 향후 제도의 설계를 위한 벤치마킹(bench-marking)연구의 일환으로써 국제기구들과 서구 국가들에 의해 도입-운용되고 있는 사업장 감시[7]을 규율하는 제도적 장치를 살펴보기로 한다. 다음의 2절에서는 OECD와 ILO에서 마련한 국제적 준칙을 정리-소개하고, 3절에서 EU국가들과 미국·캐나다·호주를 중심으로 제도화되어 있는 사업장감시 관련 입법사례를 차례로 검토하고자 한다. 소결의 4절에서는 사업장감시에 대한 국제기준과 해외 입법사례 검토를 통해 도출되는 정책적 시사점을 정리-제시할 것이다.

## 2. 사업장감시 관련 국제기준(Global Standards)

정보통신기술의 발달이 시민사회와 산업현장에서의 프라이버시와 인권에 악영향을 줄 수 있는 상황을 대처하기 위해 여러 국제기구들이 각국에서의 관련 입법을 유도-권장하기 위한 상위규범(Hypernorm)을 마련-제시해오고 있다.(Hartman & Bucci 1998) 사업장의 노동감시는 인권의 기본요소에 해당되는 프라이버시 또는 사생활의 일부를 침해하는 것인 만큼, 시민의 사생활을 보호하려는 보다 근원적인 국제규범에서 출발하여 그 세부영역이라 할 수 있는 산업현장에서의 프라이버시 침해를 낳은 감시활동의 규율에 관한 국제적인 행동준칙으로 발전해오는 것을 살펴볼 수 있다

사생활/프라이버시의 보호에 대한 가장 기본적인 국제규범은 국제연합(United Nations, UN)이 채택-유지해오고 있는 국제권리장전(International Bill of

7) 여기서 사업장감시는 Jankanish(1993)의 정의에 따라 "노동자들의 직무수행과 일상활동에 관한 정보를 컴퓨터 등의 정보통신기기를 활용하여 수집·저장·분석·기록하는 행위"를 지칭하는 것으로 정의한다. 사업장감시는 그 대상이 되는 노동자의 프라이버시범주를 중심으로 살펴보면 노동자의 신체·개인행동·의사소통행위·신상정보 등을 포괄하는 것으로 이해될 수 있다.(Clarke 1999)

Rights)에서 찾아볼 수 있다.(Coleman 2005) UN의 국제권리장전은 총회 결의를 통해 도입된 다음의 3개 협정서로 구성되고 있다: 세계인권헌장(Universal Declaration of Human Rights, UDHR), 경제-사회-문화권리에 관한 국제협약(International Covenant on Economic, Social and Cultural Rights, CESCR), 시민-정치권리에 관한 국제협약(Intenational Covenant on Civil and Political Rights, CCPR). 세계인권헌장(UDHR)은 1948년 12월에, 그리고 남은 두개의 국제협약(CESCR과 CCPR)은 1966년 12월에 각각 UN 총회의 결의를 거쳐 채택되어 세계 각국의 인권을 신장-보호하기 위한 보편적인 도덕규준으로 자리매김 되어 왔다. 이후, 이들 국제권리장전은 1993년 오스트리아 비엔나에서 개최된『세계인권대회(World Conference on Human Rights』에 참석한 171개국의 대표들에 의해 재인준이 이루어지기도 하였다.(Coleman 2005)

UN의 국제권리장전 중 세계인권헌장(UDHR)과 시민-정치권리에 관한 국제협약(CCPR)에서 개인사생활에 관한 규범준칙을 제시하고 있다. 우선, 세계인권헌장의 제12조에서는 다음과 같이 프라이버시의 보호를 명시하고 있다:

> "누구도 자신의 프라이버시와 가족, 가정생활 또는 통신활동에 대한 자의적 간섭이나, 자신의 명예와 평판에 대한 공격에 시달려서는 아니된다. 모든 사람은 그러한 간섭과 공격으로부터 법의 보호를 받을 권리를 갖고 있다. (No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the process of the law against such interference or attacks)"

역시, 시민-정치권리에 관한 국제협약의 제17조에서도 다음의 유사한 규정을 담고 있다:

> "1. 시민은 자신의 프라이버시와 가족, 가정생활 또는 통신활동에 대한 자의적 또는 불법적인 간섭이나, 자신의 명예와 평판에 대한 불법적인 공격에 시달려서는 아니된다. (No one shall be subjected to arbitrary or

unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.

2. 모든 사람은 그러한 간섭과 공격으로부터 법의 보호를 받을 권리를 갖고 있다. (Everyone has the right to the process of the law against such interference or attacks)"

대동소이하게 프라이버시의 법적인 보호를 강조하고 있는 세계인권헌장과 시민-정치권리에 관한 국제협약은 그 효력에 있어 일정한 차이를 갖고 있다. 세계인권헌장이 단순히 국제적인 차원에서의 인권 신장을 희망하는 선언서의 의미를 가지는 반면, 시민-정치권리에 관한 국제협약은 법적인 강제력을 갖는 국제협정으로서 인준국가가 반드시 협약조항을 반영하는 국내법을 입법하도록 하는 구속력을 행사하고 있는 것이다. 2003년말 현재 151개국이 시민-정치권리에 관한 국제협약을 체결하고 있어 상기 17조에서 명시하고 있는 프라이버시 보호를 위한 기본적인 국제규범이 대다수의 나라에서 수용-준수되고 있는 것을 알 수 있다.

UN의 권리장전이 전 세계 국가들을 대상으로 프라이버시 보호에 대한 기본적인 준칙을 제시한 것이라면, OECD는 선진국들을 중심으로 보다 강화된 프라이버시에 관한 국제기준을 마련하고 있다. OECD는 컴퓨터통신기술의 발달에 따른 개인프라이버시의 침해 우려가 높아지고 회원 국가들의 상이한 법제에 의한 정보교류 장애가 발생하는 등의 문제점을 대처-해소하기 위해 1978년에 관련 지침을 마련하기 위한 전문가그룹을 구``하였다. OECD는 전문가그룹이 준비한 방안에 대한 협의를 거쳐 1980년 9월에 프라이버시의 보호와 개인 데이터의 국제적 유통에 관한 가이드라인(C」 delines on the Protection of Privacy and Transborder Flows of Personal Data) 을 확정-채택하였다. 이 지침은 5부 22항목으로 구성되어 있으며, 그 가운데 제2부의 7조에서 14조에 이르기까지 다음과 같이 개인 프라이버시와 자유를 보호하기 위한 8가지 기본원칙을 밝히고 있다:

7조. 수집제한의 원칙 (Collection Limitation Principle)

개인 정보의 수집에 대한 제한이 있어야 하며, 그러한 개인정보는 적법하

고, 공정한 수단에 의해 수집되어야 하고, 적절한 경우에도 정보주체의 인지 또는 동의를 얻어 수집되어야 한다.

8조. 정보질의 원칙 (Data Quality Principle)

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

9조. 목적 명확화의 원칙 (Purpose Specification Principle)

개인정보를 수집되는 목적은 수집 당시에 명확하게 제시되어야 하며, 이후의 정보이용은 당초의 목적의 성취를 위한 것으로 제한되거나, 그 목적에 어긋하지 않은 여타의 상황에 이루어지거나, 그 목적이 변경될 때에는 새로운 목적이 명확히 제시되는 조건하에서 가능하도록 한다.

10조. 이용제한의 원칙 (Use Limitation Principle)

개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 9조에 따라 명시된 목적 이외의 용도로 공개되거나 이용되어서는 안된다.

11조. 안전성 확보의 원칙 (Security Safeguards Principle)

개인정보는 분실, 불법적인 접근, 파손, 사용, 수정, 공개과 같은 위험에 대비하는 합리적인 안전장치에 의해 보호되어야 한다.

12조. 공개성의 원칙 (Openness Principle)

개인정보에 관련된 개발, 운용 및 정책에 대한 공개의 일반적인 정책이 수립되어 있어야 한다. 개인정보의 존재, 특성, 주요 이용목적과 함께 정보관리자의 신원과 통상적인 위치를 손쉽게 확인할 수 있는 방법이 마련되어 있어야 한다.

13조. 개인참가의 원칙 (Individual Participation Principle)

개인은 (a) 정보관리자로부터 자신과 관련된 정보 또는 그 정보의 존재여부를 제공-확인할 수 있어야 하며, (b) 자신과 관련된 정보에 대해 충분히 인지가능한 형태로 적절한 방법에 의해 과도하지 않은 수준에서 적절한 시간 내에 알려지도록 하며, (c) (a)와 (b)의 조건에 따른 정보 열람요구가 거부될 경우 그 사유가 제공되어야 하며, 그러한 거부에 이의제기할 수 있어야 하고, (d) 자신과 관련된 정보수집을 문제삼을 수 있고, 그 같은 이의제기가 수용될 경우에는 그 정보는 삭제·정정·보완되어야 한다.

14조. 책임성의 원칙 (Accountability Principle)

정보 관리자는 위에서 제시한 원칙들이 준수될 수 있도록 필요한 제반조치를 취할 책임을 지고 있다.

이 OECD 가이드라인의 제4부(19조)에는 상기 원칙들을 회원국들이 수용-준수 할 수 있도록 강제하기 위한 필요조치로서 관련 국내법의 입법, 행동준칙 등에 의한 자발적 규율의 촉진-지원, 개인 권리행사의 적정한 수단 제공, 상기 원칙 관련 조치의 불응에 대한 제재와 교정의 수단 제공, 정보주체에 대한 불공정한 차별금지 등을 강구하도록 요구하고 있다. 이에 따라, 대략 OECD 회원국의 절반에서 이 가이드라인에 부합하는 프라이버시보호 입법이 이루어진 것으로 보고되고 있다(OECD 1998)[8] 이처럼, OECD 가이드라인에 따라 관련 개인정보 보호제도를 도입한 회원국가로는 오스트리아, 캐나다, 덴마크, 프랑스, 독일, 룩셈부르크, 노르웨이, 스웨덴, 미국, 벨기에, 아이슬란드, 네덜란드, 스페인, 스위스 등을 꼽을 수 있다.

이후, OECD는 개인정보 보로와 관련된 전문기구인 정보-컴퓨터-통신정책위원회(Committee For Information, Computer and Communication Policy, CICCP)를 설치하여 정보통신기술의 지속적인 발달에 따른 추가적인 대책을 수립하거나

8) OECD(1998)에 따르면, 공공-민간부문 모두에 대해서든 혹은 공공부문에 제한되어서든 총 34개 국가가 프라이버시 보호 입법을 도입한 것으로 집계되고 있다.

정책지침을 만들어 오고 있다. OECD에 의한 후속 조치의 대표적인 사례로 인터넷이라는 새로운 정보공간이 전세계적으로 확산되는 것에 대응하여 CICCP 산하에 정보안전과 프라이버시(Information Security and Privacy)에 관한 전문가그룹이 구성되어 인터넷과 관련된 "프라이버시 가이드라인"의 필요조치를 마련하였으며, 그 결과 1998년에 회원국 장관회의를 거쳐 「글로벌 네트워크에서의 프라이버시 보호선언(Ministerial Declaration of the Protection of Privacy on Global Networks)」이 채택-공표되기도 하였다.

UN의 권리장전과 OECD의 가이드라인이 시민사회 차원의 개인프라이버시문제에 대한 보호원칙을 밝힌 것에 비해 국제노동기구(ILO)는 노동자집단을 대상으로 하는 개인정보와 프라이버시의 보호지침을 마련-제시하고 있다. 정보통신기술의 발달에 따른 사업장 수준의 노동자감시활동에 대한 우려가 증대하는 데에 대응하여 ILO은 1990년대에 들어 독자적인 규제지침을 마련하기 위한 본격적인 노력을 기울였다.[9] 이같은 ILO의 노력은 1990년대 중반에 결실을 보게 되어「노동자의 개인정보 보호를 위한 행동강령(ILO Code of Practice for Protection of Workers' Personal Data)」라는 독자적인 가이드라인을 만들 수 있게 되었다. 구체적으로, 1995년 11월 ILO의 집행위원회의 결정에 따라 노·사·정을 각각 대표하는 총 24인으로 구성되는 전문가회의가 1996년 10월에 개최되어 노동자 프라이버시를 보호하기 위한 지침서를 작성하여 같은 11월 집행위원회의 승인을 얻어 ILO의 공식적인 행위준칙으로 채택됨으로써 회원국가에게 전파-권고하기에 이르게 되었던 것이다.

ILO의「노동자의 개인정보 보호를 위한 행동강령」은 총 13개 장으로 구성되

9) 1980년대까지 노동자의 프라이버시라는 문제에 대한 ILO의 논의는 주로 개인정보 보호라는 차원에서 진행되어 관련된 몇몇 결의안이 제출되었다. 그러나 기술발달의 발달과 더불어 프라이버시에 대한 우려가 늘면서, 제 75차(1988) ILO 총회 당시 ILO 사무총장이 제출한 인권보고서에서 이 문제에 대한 보다 깊은 관심을 표명했다. 그는 개인정보와 현대적인 전자장비들이 노동자들의 움직임을 통제하고 감시하는데 부적절하고 사용되거나 남용될 가능성으로부터 노동자들을 보호하는 것이 노동기준설정에서의 중요 문제로서 제기될 것으로 지적하였다. 노동자프라이버시에 대한 ILO의 정책적인 관심은 1991년과 1993년 각각에 발간된 Conditions of Work Digest 시리즈 연구서에서 확인되는 바, 노동자 프라이버시에 대한 ILO 차원의 집중적인 연구프로젝트를 진행한 결과 보고서를 게재하는 것으로 1부의 개인정보의 보호(Protection of Personal Data), 2부의 사업장 감시(Monitoring and Surveillance in the Workplace). 3부의 작업장 테스트(Testing in the Workplace)로 구성되어 있었다.

어 있으며, 그 전문은 [부록 1]에서 수록하고 있다. 주요 내용을 살펴보면, 4장에서 행동강령의 적용대상을 공공부문과 민간부문을 포괄하는 것으로 명시하고 있고, 5장에서는 노동자의 개인정보 보호에 관한 13개 항목의 일반원칙을 제시하고 있다. 6장에서부터 13장까지는 개인정보의 수집(6장), 보안(7장), 보관(8장), 이용(9장), 전송(10장). 개인 권리(11장), 집단적 권리(12장), 고용알선기관(13장)에 대한 세부 지침을 서술하고 있다. 주요 내용을 간추려 보면 다음과 같다:

① 사용자는 노동자 정보를 반드시 작업과 관련한 범주에서 본인에게 직접 얻어야 하며,

② 사용자는 노동자의 정치·종교적 신념 및 성생활에 관한 정보를 얻으려 해서는 안되며,

③ 노동자는 프라이버시에 관한 권리를 포기하지 말아야 하며,

④ 사용자가 특정 노동자를 감시할 경우 본인에게 그 사유와 방법 그리고 시간을 통보해야 하고 비밀감시는 형사범죄 용의자에게만 해당하며,

⑤ 개인정보의 사용 기간 등은 투명하고 명확하게 노동자에게 미리 사전 고지하며,

⑥ 검열된 자료에 대하여 해당 노동자에게 열람권이 보장되는 등 인간적인 방식으로 동기를 유발시키는 요소로서 전자감시가 이루어져야 한다.

그런데, ILO의 「노동자의 개인정보 보호를 위한 행동강령」은 회원국들에 대해 관련 입법이나 정책을 강제하는 구속력(binding force)을 가지지 못하고, 다만 각국에서 관련 법안·규제·단체협약·취업규칙·정책 및 기업차원의 경영수단을 마련함에 있어 참조되는 권고지침으로 활용되고 있다.

## 3. 해외 주요국의 사업장감시 관련 입법 사례

### 1) EU 국가 사례

유럽 국가들은 일찍이 인권 및 프라이버시의 보호를 위한 통일적인 규범을 형성하여 왔다. 1950년에 유럽국가들이 제정한「유럽 인권헌장(European Convention on Human Rights)」의 7조와 8조에서 개인 및 가정생활과 개인정보를 보호받을 권리의 하나로서 포함시켰으며, 이 인권 조항은 이후 유럽연합(European Union, EU)에 의한 관련 입법지침의 주요 근거로 제시되고 있다. 또한, 1981년에는 당시 유럽평의회(Council of Europe)이 "개인정보의 자동처리에 있어 개인 보호에 관한 협약 (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data)"을 체결하여 유럽지역내 회원국가들로 하여금 관련 제도를 입법하게 함과 동시에 이후 시민과 노동자에 대한 감시활동을 규제하는 제도를 마련함에 있어 EU와 비유럽국가들의 준거지침으로 활용되었다. 실제, 상기 협약에 의거하여 EU 통합이전(1992년)까지 유럽공동체(European Community)는 다음과 같이 개인정보 보호를 위한 여러 보고서를 작성-제출하기도 하였다:

- "사회보험에 사용되는 개인정보 보호에 관한 보고서"(1986년)
- "고용관계에 사용되는 개인정보 보호에 관한 보고서"(1989년)

1992년에 Maastricht협정을 통해 유럽연합(1999년)으로 발전적인 통합을 성사시킨 당시 유럽공동체(European Community)는 1995년 10월에 개인의 정보 및 프라이버시 보호를 위한 중요한 정책결정을 낳게 되는 바, 다름 아닌 "개인정보처리에 있어 개인 보호와 개인정보의 자유이동에 관한 EU 일반지침(European Union Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 95/46/EC)"을 제정-공표하였던 것이다. 이 지침은 EU 회원국들의 관련 입법 및 정책집행을 강제하는

구속력을 갖고 있어 그 이후 각국에서는 개인정보/프라이버시의 보호를 위한 법률 제정 또는 정비가 활발하게 이루어지게 되었다. 개인정보와 관련하여 이 EU지침은 다음의 7개 일반원칙을 제시하고 있으며, 그 상세한 내용은 [부록]을 참조하기 바란다.

① 필요성(Finality): 개인 정보는 명시된 특정의 합당한 목적에 한해서 수집될 수 있다.

② 합목적성(Legitimacy): 개인 정보는 제한된 목적을 위해서만 처리-이용될 수 있다.

③ 투명성(Transparency): 개인 정보의 이용-처리에 대해 정보주체에게 반드시 통지하여야 한다.

④ 적절성(Proportionality): 개인 정보는 본래의 수집-이용 목적에 적절-부합하여야 하며, 과도해서는 아니된다.

⑤ 기밀성(Confidentiality)과 안전성: 개인정보의 수집과 이용에 있어 기밀과 안정이 보장되는 기술적·조직적 수단이 강구되어야 한다.

⑥ 통제성(Control): 개인 정보의 수집과 이용에 관한 통제력을 행사하는 정보보호기관(Data Protection Authorities)을 설치-운용하여야 한다.

⑦ 인지성(Awareness): 정보 주체는 이 지침의 원칙과 그 적용에 대해 충분히 숙지할 수 있어야 한다.

1995년의 개인정보 보호 EU지침을 발전시켜, 1997년 12월과 2002년 7월에는 각각 통신업종과 전자통신업종의 특수성을 고려하여 이들 산업부문을 대상으로 하는 추가적인 지침을 다음과 같이 제정-공표하기도 하였다:

- “통신업종에 있어 개인정보의 처리와 프라이버시에 관한 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)”

- “전자통신업종에 있어 개인정보의 처리와 프라이버시에 관한 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)”

2000년대에 EU는 정보통신기술의 급속한 발달과 더불어 노동자들에 대한 사업장감시가 사회적으로 주목을 받게 됨에 따라 기존의 95년 EU지침을 고용관계에 적용하기 위한 활발한 연구와 정책협의가 진행되고 있는 바, 주요 성과물을 예시하면 다음과 같다:

- 2001년 1월: “종업원 평가자료에 관한 정보보호 작업그룹의 권고서(EC, Data Protection Working Party, Recommendation 1/2001 on Employee Evaluation Data)”
- 2001년 8월: “고용관계에서의 개인정보 처리에 관한 정보보호 작업그룹의 의견서(EC, Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context)”
- 2002년 5월: “작업장 전자통신 감시에 관한 정보보호 작업그룹의 연구보고서(EC, Data Protection Working Party, Working Document on the Surveillance of Electronic Communications in the Workplace)
- 2002년 11월: “비디오감시의 수단에 의한 개인정보 처리에 관한 정보보호 작업그룹의 연구보고서(EC, Data Protection Working Party, Working Document on the Processing of Personal Data by means of Video Surveillance)
- 2004년 4월: “비디오감시의 수단에 의한 개인정보 처리에 관한 EU의 의견서(EU report Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance)”
- 2005년 1월: “RFID 기술과 관련된 정보보호이슈에 관한 정보보호 작업그룹의 연구보고서(EC, Data Protection Working Party, Working Document on Data Protection Issues Related to RFID Technology)"

아울러, EU 집행위원회는 노동자의 개인정보 보호를 위한 지침을 마련하기 위해 2001년 8월에 1단계의 사회적 정책협의(consultation of social partners)를 개시하였으며, 여기에는 유럽연합 차원의 노동단체인 ETUC, CEC, EUROCADRES와 사용자단체인 UNICE, NEAPME, BDI가 참석하고 있다. 2002년 10월에 2단계의 사회적 정책협의가 개최되었으나, 노동자의 개인정보를 보호하기 위한 지침의 도입을 지지하는 노동단체들과 반대하는 사용자단체들 간에 입장차이가 적지 않아 그 지침 제정에 관한 사회적 합의를 이루는 데에는 다소간 시간이 걸릴 것으로 전망되고 있다.

이상에서 살펴본 EU차원의 여러 지침(Directives)과 관련 정책 권고는 회원국들에게 개인 프라이시의 보호와 사업장감시의 규제를 제도화하는 입법 준거로 작용해오고 있다. 그런데, 이 같은 EU 지침이 대체로 잘 준수되고 있는 가운데 [표 1]에서 예시하는 바와 같이 EU 국가들에서 도입-시행하고 있는 노동자 프라이버시의 보호 입법은 다소간 차이를 보이고 있기도 하다.(Hednrickx 2001) 이들 EU 국가에서 노동자 프라이버시를 보호하기 위한 법률체계로는 헌법, 시민법(Civil Code)·형법(Criminal Code)과 같은 일반법, 프라이버시 관련 특별법 그리고 노동관계법 및 정책적 행위준칙으로 구성되어 있다. 그러면, 이 같은 법률체계에 맞추어 노동자 프라이버시 보호를 위한 EU국가들의 입법사례를 간추려 살펴보기 한다.[10)]

우선, 일부의 EU국가들은 헌법에 개인의 인격과 사생활 보호와 관련 조항을 명시하여 노동자 프라이버시 보호를 위한 입법근거를 제시하고 있다. [표 1]에서 보여주듯이, 헌법에 이같이 프라이버시 조항을 포함하고 있는 국가로는 벨기에(22조), 독일(1조와 2조), 그리스(18조), 스페인(18조), 네덜란드(10조), 포르투갈(26조, 35조, 54조), 핀란드(10조) 등을 열거할 수 있다. 이 가운데 포르투갈의 헌법 규정은 노동자의 프라이버시 권리에 대해 구체적으로 명시하고 있어 시민 프라이버시의 일반적인 권리조항을 포함하고 있는 다른 EU국가들과 비교하여 보다 강력한 보호입법의 근거를 갖고 있는 것으로 평가되고 있다. 또한, 영국의 경우에는 불문

10) 노동자 프라이버시 관련 EU국가의 입법례에 대한 소개는 주로 Hendrickx(2001)를 참조하여 작성한 것임을 밝혀둔다.

법의 전통에 따라 헌법이 존재치 않은 가운데 헌법에 준하는 입법효력을 가지는 “인권법(Human Right Act)"가 2000년에 발효되어 개인프라이버시 권리를 명확히 밝히고 있다.

둘째, 모든 EU국가들은 개인정보 보호에 관한 EU지침(95/46/EC)에 따라 개인정보 또는 프라이버시 보호를 위한 특별법을 제정 또는 개정하여 시행하고 있는 것으로 확인된다. 이 중 일부 국가(예: 벨기에, 덴마크, 프랑스, 아일랜드, 이태리, 네덜란드, 포르투갈, 핀란드, 영국 등)에서는 상기 지침의 제7원칙에 따라 개인정보 및 프라이버시 보호의 정책기능을 수행하는 감독위원회를 설치-운영하고 있으며, 이들 감독위원회의 주관하에 개인정보 일반 또는 고용관계의 프라이버시에 대한 행위준칙(Code of Practice)를 제정-공표하기도 하였다. 이에 더하여 일부 국가에서는 추가적인 보호의 법률규정을 갖추고 있는 바, 이를테면 덴마크의 경우에는 1996년에 “의료정보법(Medical Data Act)"을 제정하여 반드시 노조 또는 종업원대표와의 사전합의를 거쳐 종업원의 보건의료정보를 수집할 수 있도록 하고 있으며, 독일・포르투갈(통신법, Telecommunications Act) 그리고 영국(통신규제지침 Telecommunications Regulations)에서는 통신이용의 기밀보장과 감시규제를 별도 제도화하고 있다. 또한, 덴마크와 스웨덴에서는 비디오감시 또는 카메라감시를 규제하는 법률을 제정-시행하고 있기도 하다.

셋째, 소수의 EU국가에서 개인정보 보호 또는 사업장감시 규제를 위한 별도의 특별법을 제정하여 운영하고 있다. 특히, 핀란드에서는 2000년에 “노동생활에서의 개인정보 보호에 관한 법(Act on Data Protection in Working Life)”이 입법-발효되어 유럽국가 중에서는 사업장 감시를 규율하는 가장 구체적인 법률규정을 갖추게 되었으며, 이러한 입법사례를 좇아 스웨덴이 유사법안(“Bill on Personal Integrity in Working Life”)을 심의중인 것으로 알려지고 있다. 한편, 영국에서도 2000년에 “조사권 규제법(Regulation of Investigatory Powers Act)을 제정하여 사용자의 사업장감시에 대한 합법적인 실시 요건을 상세하게 규정하기도 하였다.

넷째, 노동관계법을 통해 사용자의 감시활동을 제도적으로 규제하는 국가는 소수로 제한되며, 대표적인 예로는 프랑스(Labour Code 121-8항과 122-45항), 이태리(Workers’ Statute 4조), 스페인(Employee Statute) 등을 꼽을 수 있다. 특히,

스페인의 경우에는 추가적인 정부조례(Royal Legislative Decree 5/2000)에 의해 사용자의 노동자 감시행위를 처벌하는 벌칙을 규정하고 있다. 이처럼, 노동관계법에서 사업장 감시의 규제를 명시하는 나라는 드물지만, 대부분의 EU국가(예: 벨기에, 독일, 그리스, 네덜란드, 오스트리아, 핀란드, 스웨덴 등)는 사업장 수준의 종업원평의회(Works Council)를 제도화하고 있어 이들 종업원평의회에게 사용자의 감시장비 설치에 대한 사전 협의와 현장의 감시활동에 대한 노동자들의 고충처리를 수행할 수 있는 권한을 부여하고 있다. 이같이 EU국가 대다수에는 사업장감시 문제를 집단적 노사관계의 교섭-협의사안으로 제도화함으로써 노동자들에 의한 자주적인 보호기제를 제공하고 있는 것이다.

마지막으로는, 일부의 EU국가가 형법(Criminal Code)과 시민법(Civil Code)에 의거하여 사용자의 프라이버시 침해를 규율하고 있기도 하다. 노동자 프라이버시 보호를 위해 형사법을 활용하는 나라로는 덴마크와 이태리를 꼽을 수 있는 한편, 프랑스에서는 형법과 시민법 모두가 인용되고 있다. 아울러, EU국가에서는 노동법원(예: 독일) 또는 일반법원에서 사용자감시활동에 대한 판례가 상당히 축적되어왔으며, 그 가운데 대륙의 EU국가에서는 노동자보호를 강조하는 판례가 지배적인 반면, 영국에서는 사용자의 사업장감시활동에 대한 정당성을 인정하는 판례가 다소 많아 일정한 차이를 보이는 것으로 평가되기도 한다.(Hendrickx 2001)

<표 5-1> 노동자 프라이버시에 대한 EU국가들의 입법사례

| 국가명 | 노동자 프라이버시 관련 입법 내용 |
|---|---|
| 벨기에 | -헌법 22조, 프라이버시 권리 명기<br>-Act on Data Protection(1998년 개정- 도청금지), 프라이버시감독관 설치<br>-노동자의 사전동의 없는 통신감시에 대한 형사 제재<br>-고용관계에서의 프라이버시 보호의 행위준칙 제정 |
| 덴마크 | -Works Council Act, 사업장감시 관련 노사협의 의무화<br>-Processing of Personal Data Act(2000년), 정보보호감독관 설치<br>-Medical Data Act(1996) 노조와의 사전합의후 보건의료정보 수집가능<br>-Camera Surveillance Act (2000년 개정)<br>-형법(Criminal Code), 전자감시 규제 |

| | |
|---|---|
| 독일 | -헌법 1-2조, 인격권 · 프라이버시 · 정보보호 규정 포함(연방법원판례)<br>-Federal Data Protection Act(2001년 개정) 공공부문과 민간부문 적용<br>-Telecommunications Act의 5조(기밀유지 및 정보보호)<br>-Works Constitution Act 87조, 사업장감시 관련 노사협의 의무화<br>-사업장 직무상 통신감시에 대한 노동법원의 사용자 귀책 인정 판례 |
| 그리스 | -개정헌법(2001년)에서 프라이버시 및 인격권 관련 조항 명기<br>-Data Protection Act(2001년 개정)<br>-사용자의 종업원프라이버시 위반에 대해 시민법(Civil Code) 57-60조에 의거, 처벌<br>-노동관계법, Works Council의 사업장감시 관련 노사협의권 부여 |
| 스페인 | -헌법 18조 4항, 프라이버시권리 보호 명기<br>-Organic Act on Protection of Personal Data(1999년) 공공-민간부문적용<br>-Royal Legislative Decree 5/2000 사용자의 노동자 감시행위 처벌<br>-종업원헌장(Employee Statute, 1995년)에서 노동자의 프라이버시와 인격권 보호 규정 포함 |
| 프랑스 | -Act on Computer & Freedom(1978년- 개정검토중), 프라이버시 보호의 고용관계 행위준칙 제정, 국가정보보호관(CNIL) 설치<br>-시민법 9조 프라이버시권리 명시, 형법 '악의적' 도청행위 처벌<br>-Labour Code 종업원정보 평가목적 사용/사전동의 요건, 고용프라이버시 조항 명기, Works Council의 사업장감시 관련 노사협의권 부여<br>-근무시간 개인통신의 프라이버시 존중/사용자감시 불법 판례 |
| 아일랜드 | -Data Protection Act(2002년 개정), 정보보호감독관의 행위준칙 공표 |
| 이태리 | -Act on Protection of Individuals & Personal Data(1996년) 국가감독관<br>-노동자헌장 4조 노동자감시장비 사용제한, 8조 노동자의 개인신상 탐문 불법 명시 |
| 네덜란드 | -형법, 사용자의 도청행위 엄격 금지<br>-헌법 10조, 프라이버시권리 보호 명기<br>-Works Councils Act, 사업장감시 관련 노사협의 의무화<br>-Personal Data Act(2000년 개정), 프라이버시 보호의 고용관계행위준칙 제정, 정보보호감독관 설치 |
| 오스트리아 | -Data Protection Act(2000년 개정) 정보보호원칙 명시<br>-Works Constitution Act 91조, 사업장감시 관련 노사협의 의무화 |
| 포르투갈 | -헌법(1976년) 26조 인격권과 사생활 보호, 35조 컴퓨터자료 사용 관련 프라이버시 명기, 54조 노동자평의회의 사업장감시 협의권리 부여 (공공-민간부문 공동 적용)<br>-Data Protection Act(1998년), Telecommunications Act, Private Security Act 사용자의 통신/비디오감시행위 불법 간주, 정보보호감독관 설치<br>-Telecommunications Act, 업무통신기록의 노동자 사전동의 필요 |
| 핀란드 | -헌법 10조, 프라이버시권리 보호 명기 |

| | |
|---|---|
| | -Personal Data Act(1999년), Act on Data Protection in Working Life (또는 Employment Privacy Act, 2000년 제정) Data Protection Ombudsman<br>-Co-operation Act, 사업장감시 관련 노사협의 의무화 |
| 스웨덴 | -Personal Data Act(1998년 개정), Personal Integrity in Working Life법안 심의 중<br>-Act on Codetermination at Work, Works Council 프라이버시협의권 부여<br>-Act on Public Camera Surveillance(1980년), 사업장 준용 |
| 영국 | -Human Right Act(2000년 발효)에 의한 개인프라이버시 권리 보호<br>-Data Protection Act(1998년-정보보호원칙 명시), 노동자감시의 사전동의 요건 강화, 정보감독관(Information Commissioner) 행위준칙 공표(2000년)<br>-Telecommunications Regulations(2000년) 동의없이 감시가능요건 제한<br>-Regulation of Investigatory Powers Act(2000년) 사업상 감시의 제한 허용 |

* 요주의정보(sensitive data, 병력·범죄 기록 등 지칭) 관련 노동자프라이버시에 관한 입법사례 생략하였으며 상세 내용은 Hendrickx(2001)을 참조할 것.

### 2) 미국의 사례

미국에서는 사업장에서 노동자들의 사생활이나 프라이버시를 보호하기 위해 입법된 별도의 법률은 존재하지 않는다.(고세일 2005) 다만, 시민의 사생활 보호를 위해 일반적으로 제정되어 있는 헌법, 관습법(Common Laws), 연방차원의 관계법령 그리고 주단위의 법률 등의 관련조항들이 사업장에서 발생하는 노동자의 감시 또는 사생활침해 문제에 대한 사법적인 심판준거로 해석-활용되고 있다. 따라서, 노동자의 프라이버시 보호를 위한 미국의 법률 체계는 매우 복잡하고 산만할 뿐 아니라 노동자의 인격권을 강조하고 있는 유럽국가에 비해 사용자의 재산권을 옹호하는 법논리가 우세하게 작용하고 있는 것으로 평가되고 있다.(Kovatch 2000)

우선, 미국의 4차 수정헌법(Fourth Amendment)에서는 정부기관이 시민들을 대상으로 부적절한 검색과 압류를 금지하는 조항을 담고 있는 바, 이 조항에 의거하여 정부기구와 공공기관의 종사자들에 대한 사용자 또는 관리자의 무단 감시활동을 불법으로 판정하는 판례들이 형성됨으로써 특히 공공부문 노동자들의 프라이버시를 보호하는 근거로 자리잡고 있다.(Scott 2001)[11] 민간부문에 대해서는 별

도의 성문법이 부재하기 때문에 그동안 관습법(Common Law)이 주된 사법적 심판근거로 활용되고 있는데, 여러 판례를 통해서 종업원이 문제행동을 범하는 경우에는 사업장내 화장실 또는 탈의실 등의 개인적 공간에 대해 감시할 수 있으며 심지어 적법한 직무행위에 대해서도 회사 소유의 컴퓨터설비를 이용하는 경우에 회사의 감시활동은 노동자의 프라이버시를 침해하지 않는 것으로 인정해오고 있다.(Kovatch 2000; Scott 2001)[12] 다만, 사용자의 감시활동이 노동자들의 노동조합 관련 활동 또는 근로조건 개선의 집단적 논의 및 상호부조활동 등을 대상으로 이루어질 경우에는 연방노동관계법(National Labor Relations Act)에서 규정하는 부당노동행위(unfair labor practice)로 인정되어 규제하는 판례와 행정해석이 대체로 이루어지고 있다.[13]

미국에서 정보통신기술을 이용한 감시활동으로부터 시민들의 개인프라이버시를 보호하려는 취지에서 1986년에 연방 전자통신프라이버시법(National Electronic Privacy Communication Act, EPCA)이 제정되었다. 특히, EPCA에서는 "의도적으로 전자통신을 감시하거나 제3자로 하여금 감시하도록 하는 행위를 불법으로 간주(2511조항)"하고 있으며, 동법 위반시에는 불법감시로 인정되는 기간에 대해 하루 최소 $200에서 최고 $10,000의 벌금을 부과할 수 있도록 규정되어 있다. 그런데, EPCA에는 그 현실 적용에 있어 여러 유보 또는 면책조항을 담고 있어 실제 사용자의 사업장감시를 거의 규제하지 못하는 결과를 낳는 것으로 평가되기도 한다.(Stanley & Steinhardt 2003; Tribbey 1999)

EPCA에서 사용자의 감시활동에 대해 명시적으로 인정하는 면책요건으로는

---

11) 노동자 프라이버시 보호판례의 대표적인 사건으로는 연방법원의 1987년 O'Connor v. Ortega 심판사건을 들 수 있는데, 공공병원의 정신과의사인 Ortega씨의 사무실과 자료서류를 병원 사용자가 무단으로 수색한 것에 대해 연방법원은 수정헌법을 위반한 것으로 판결하여 이후 공공부문의 유사 사업장감시사건에 대한 준거가 되었다.

12) 이같은 관습법 판례로는 K-Mart v. Trott (1984년), Simpson v. Commonwealth of Pennsylvania Unemployment Compensation Bd. of Review (1982년) Smyth v. the Pillisbury Co. (1996년); Bourke v. NIssan Motor Corp. (1993년), United States v. Simons (1998년), TBG Ins. Service Corp. v. Superior Ct. (2002년) 등을 예시할 수 있다.

13) 노조활동 관련 종업원에 대한 감시활동을 부당노동행위로 간주한 대표적인 판례 및 행정해석사건으로는 NLRB v. Unbelievable Inc. (1995년)과 NLRB의 Timekeeping System Inc. 심판사건(1997년)을 꼽을 수 있다.

사전동의의 면책(consent exempt)와 회사자산 이용면책(business use exemption)을 들 수 있는데, 전자는 동법 2511조(2)(d)에 언급되어 있는 것으로 종업원의 사전 동의가 있을 경우를 지칭하며, 후자는 역시 동법 2511조(2)(a)(i)에서 회사 소유 자산을 종업원이 이용하는 경우를 뜻하고 있다. 이에 더하여, EPCA는 종업원들의 사적 대화에 대한 사용자의 감시활동을 문제삼고 있으나 직무상의 대화와 이메일 통신에 대한 감시활동은 적법한 것으로 용인하고 있으며, 또한 통신 또는 정보 전송과정에 대한 사용자의 감시활동이 위법으로 규제되지만 통신 이후 보관되어 있는 정보 또는 자료에 대한 검색-감시활동을 적법한 것으로 인정하고 있기도 하다.

이 같이 현행 연방전자통신프라이버시법이 사용자 편향의 단서조항으로 인해 노동자들에 대한 사업장감시를 제대로 규율하지 못하고 있다는 노동계와 시민단체들의 반발이 계속되는 가운데, 민주당 주도의 대체입법이 지난 1990년대 초부터 시도되기도 하였으나 공화당이 지배하는 국회에서 매번 좌절되었다.[14] 그 가운데, 1996년에 제정된 "건강보험이동성과 책임성법(Health Insurance Portability and Accountability Act)"에서는 종업원들의 병력 및 의료정보에 대한 프라이버시 기준을 보다 엄격하게 제한하는 규정을 도입하고 있으며, 특히 종업원의 사전 허가 요건을 의무화하고 위반 벌칙규정(예: 징역1-10년, 벌금 5만-25만불)을 대폭 강화함으로써 의료/보건 신상정보에 한해 EPCA에 비해 한층 엄격한 규제 장치가 마련되기도 하였다.[15]

이상의 연방차원 법률에 더하여, 13개 주에서는 별도의 프라이버시 보호 법률을 제도화하고 있는 것으로 알려지며, 특히 Connecticut와 Florida주에서는 2003년에 각각 ECPA 수준 이상으로 사용자의 감시활동에 대한 규제를 강화하는 "전자

14) 1991년에 민주당의 주도하에 사용자의 감시활동에 대한 규제와 벌칙을 강화하는 "소비자-노동자 프라이버시법(The Privacy for Customers and Workers Act)"의 입법이 시도되었으나 사용자 단체와 공화당의 반대로 실패하였으며, 2000년에 다시금 민주당이 사용자의 감시방법, 감시수단, 수집정보, 감시빈도 등에 대한 종업원에의 사전통보를 의무화하는(단, 종업원의 불법/위험행위 간여 또는 사용자의 감시행위 적정결과 예상시에는 사전통보 불필요) "전자감시 사전공지법(The Notice of Electronic Monitoring Act)"의 입법을 시도하였으나, 역시 공화당의 반대로 무산되었다. 이런 가운데, 9.11 테러사건이후 오히려 전국적인 감시체제를 도입하려는 "종합정보경고체제(Total Information Awareness)"프로젝트가 국방성에 의해 추진되고 있기도 하다.(Stanley & Steinhardt 2003)

15) Geist(2002)에 따르면, 최근의 미국 법원판례가 작업장 프라이버시를 보호하기 위해 ECPA를 폭넓게 해석하는 경향이 증대하는 것으로 평가하기도 한다.

감시법 (Electronic Monitoring Act)"과 "통신안전법(Security of Cummunication Act)법을 제정하였다.[16]

### 3) 캐나다 사례

캐나다에서는 프라이버시보호의 입법체계가 연방정부과 주정부의 이원화된 구조를 보이고 있다. 우선, 연방차원에는 개인 사생활보호를 위한 법률로서 "프라이버시법(Privacy Act)"과 "개인정보보화와 전자문서법(Personal Information Protection and Electronic Documents Act, PIPEDA)"이 존재하고 있다. 전자의 프라이버시법은 1983년 7월에 발효되었으며, 150여개의 연방정부기관에 대해 시민과 해당 기관종사자들의 개인정보를 수집·사용·공개하는 것을 제한하는 법률적 규제장치로 기능하고 있다. 또한, 이 법에 의거하여 프라이버시감독관(Privacy Commissioner)이 설치되어 캐나다 연방차원의 사생활 침해 관련 정책 및 고충사건을 처리하고 있다.[17]

최근 2004년 1월에 발효된 PIPEDA는 민간기업 부문에 있어 고객과 소속 종업원들의 프라이버시를 보호하려는 취지에서 입법-기능하고 있다. 이 법에서는 노동자 대상의 사업장감시에 대한 강화된 규제조항이 포함되어 있는 바, 우선 종업원의 동의 없이 사용자가 감시활동을 수행할 수 있는 적정사유 또는 타당한 목적(reasonableness clause or appropriate purpose)을 크게 제한하고 있으며, 사업장 내 프라이버시문제를 전담 감독하는 "프라이버시위원(Privacy Officer)"제도를 도입하였고, 수집목적 공표-정보주체 사전동의-목적제한적 수집활동정보 등과 같은

16) 캘리포니아주에서는 2001년에 주의회에서 종업원의 사전동의 없는 사용자의 감시활동을 불법화하는 SB147법을 제정하였으나, 사용자단체의 로비를 받은 당시 Gray Davis 주지사의 비토권 행사로 인해 무산되기도 하였다.

17) 일반 시민이나 기관소속 종업원은 자신의 사생활침해 고충문제에 대해 공공기관의 경우에는 '프라이버시법"의 29조, 민간부문 기업체의 경우에는 PIPEDA의 11조에 의거하여 프라이버시감독관에게 진정-제소할 수 있다. 제소된 사건에 대해 프라이버시감독관은 조사와 당사자 청문회 등을 실시하여 해당 사건의 해결을 위한 조정-중재를 수행한다. 캐나다의 대부분 주에서는 이와 유사한 프라이버시감독관 또는 옴부즈만(Ombudsman)을 두고 있다.

정보수집의 원칙을 제시하고 있는 것이다. 다만, 캐나다의 특수한 입법구조에 따라 PIPEDA는 주법에 의해 관장되는 민간부문의 노동자집단에 대해서는 그 법적 효력을 갖지 않는 것으로 되어 있다.

이 밖에도, Radiocommunication Act, Telecommunications Act, Bank Act 등과 같이 특정 업종부문을 대상으로 프라이버시 보호규정을 담고 있는 연방차원의 법률이 존재하고 있기도 하다. 또한, 미국의 관습법을 대신하여 캐나다에서는 형법(Criminal Code)가 사생활침해에 대한 형사상의 처벌 근거(제 183조와 184조)를 제공하고 있으며, 이같이 형법에 의한 감시행위 처벌의 경우에는 미국에서와 같이 종업원의 사전동의와 사용자직무와 관련된 면책조건을 부여하고 있다고 한다.(Geist 2002)

각 주는 독자적으로 공공기관의 프라이버시 침해를 규율하는 법률이 제정되어 있고 관련 감독기관을 설치-운영하고 있다. 다만, 연방의 PEPEDA와 같이 주 차원에서 민간부문에서의 프라이버시문제를 다루는 법률은 British Columbia, Alerta, 그리고 Quebec 주에만 제정되어 있다. 또한, Ontario주의 정보-프라이버시 위원회(Information and Privacy Commission)는 정례적으로 의견서를 공표하여 시민사회와 산업현장에서의 감시행동을 규율하는 주 차원의 행위준칙을 제시하고 있는 것이 특기할 만하다. 특히 이 위원회는 1992년에 사업장 감시의 3개 원칙(① 비밀감시를 금지하고, ② 가시적 감시의 경우에도 엄격한 기준에 따라 수행되어야 하며, ③ 직무와 관련없는 개인정보의 수집을 허용치 않는다)를 발표하였고, 2001년에는 “사업장 밖에서의 프라이버스와 개인기밀을 보호하기 위한 가이드라인(Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside of the Office)”를 작성-공표하기도 하였다.

### 4) 호주의 사례

호주는 미국과 캐나다와 같이 연방국가이므로 개인 프라이버시 보호를 위한 입법체계가 연방정부-주정부의 이원구조를 갖고 있다. 연방차원에서 프라이버시의

보호입법으로 처음 등장한 것은 1979년에 제정된 "연방통신(도청)법(Common-wealth Telecommunications (Interception) Act)"으로서 통신부문의 감시활동을 규제하였다. 호주에서 체계적으로 시민들의 프라이버시를 보호하기 위해 제도화된 규제장치는 1988년에 입법된 "연방프라이버시법(Federal Privacy Act)"에서 찾을 수 있다. 이 법에는 다음의 11개 항목에 대한 '정보프라이버시원칙(Information Privacy Principles, IPPs)'[18]을 밝히고 있다:

① 개인정보의 수집 방법과 목적 (Manner and purpose of collection of personal information)

② 특정 개인의 사적 정보 취득 (Solicitation of personal information from individual concerned)

③ 개인정보 취득 일반 (Solicitation of personal information generally)

④ 개인정보의 보관과 안전 (Storage and security of personal information)

⑤ 정보관리자의 관리기록에 관한 정보 (Information relating to records kept by record-keeper)

⑥ 개인정보 기록의 접근 (Access to records containing personal information)

⑦ 개인정보 기록의 수정 (Alteration of records containing personal information)

⑧ 사용전 개인정보 정확성 등의 정보관리자 점검 (Record-keeper to check accuracy es. of personal information before use)

⑨ 적정 목적에 따른 개인정보의 사용 (Personal information to be used only for relevant purpose)

⑩ 개인정보의 사용 제한 (Limits on use of personal information)

⑪ 개인정보의 공개 제한 (Limits on disclosure of personal information)

---

18) 호주 정보프라이버시원칙(IPPs)의 상세내용에 대해서는 http://www.privacy.gov.au/publications/ipps.html를 참조할 것.

이상의 정보프라이버시원칙(IPPs)는 연방프라이버시법이 정부 및 공공기관에 제한적으로 적용된 것이므로 이들 공공부문의 종사자에 대한 감시활동을 규제하는 제도적 행위준칙으로 활용되었다. 그런데, 2000년에 연방프라이버시법이 연간 3백만 호주달러 이상의 매출실적을 올린 민간기업들에까지 확대 적용되도록 개정됨으로써 민간기업에서의 사업장감시로부터 노동자의 프라이버시를 보호할 수 있는 길이 열리게 되었다. 2001년 12월에 발표된 "연방프라이버시수정(민간부문)법(Federal Privacy Amendment (Private Sector) Act)"에는 별도의 '국가프라이버시원칙(National Privacy Principles, NPPs)[19]를 다음과 같은 항목을 중심으로 제정-공표하였다:

① 정보 수집 (Collection)
② 정보 사용과 공개 (Use and disclosure)
③ 정보 질 (Data quality)
④ 정보 안전 (Data security)
⑤ 정보관리의 공개성 (Openness)
⑥ 정보의 접근과 수정 (Access and correction)
⑦ 정보 확인절차 (Identifiers)
⑧ 정보의 익명성 (Anonymity)
⑨ 국가간 정보교류 (Transborder data flows)
⑩ 요주의 정보 (Sesitive data)

또한, 연방프라이버시법은 1988년부터 연방정부의 '인권-동등기회위원회(Human Rights & Equal Opportunities Commission)의 산하에 프라이버시감독관(Federal Privacy Commissioner)직제[20]를 설치-운영하도록 하였던 바, 이 감독관

19) 호주 국가프라이버시원칙(NPPs)의 상세내용에 대해서는 http://www.privacy.gov.au/publications/npps01. html를 참조할 것.

20) 호주의 연방프라이버시감독관은 캐나다의 감독관과 유사하게 연방 공공기관에서 발생한 프라이버시 침해의 진정사건을 심사-조정-중재 기능을 수행하고 있다. 호주와 캐나다 이외

은 핵심수행 기능의 하나로서 개인프라이버시 관련 행위준칙 및 정책가이드라인을 제정-공표해오고 있다. 실제, 연방프라이버시감독관은 1998년에 개인정보의 공정 처리를 위한 국가원칙(National Principles for the Fair Handling of Personal Information)'을 제정-공표하였으며, 또한 2000년에는 '작업장 이메일·웹브라우저·프라이버시(Workplace E-mail, Web Browsing and Privacy)'[21]에 관한 가이드라인을 제시하기도 하였다.

각 주에서는 독자적인 프라이버시 보호입법을 마련하여 사업장감시에 대한 정책적인 규제를 다양하게 시행하고 있다. 호주의 주정부 가운데 노동자 프라이버시를 보호하기 위한 가장 강력한 규제장치를 입법하고 있는 New South Wales주를 중심으로 살펴보면, 1998년에 작업장 비디오감시를 규제하는 "작업장비디오감시법(Workplace Video Surveillance Act, WVSA)"((부록 3) 원문 참조)을 제정-시행한 데에 이어, 2004년에는 WVSA의 입법 이후 인터넷과 이메일의 감시활동을 둘러싼 사회적 우려가 제기됨에 따라 2005년 5월에 동법을 대체하여 컴퓨터감시 등을 포괄하는 새로운 "작업장감시법(Workplace Surveillance Act)"을 제정하였다.(Smythe, Shailer & Stein 2004) 작업장감시법은 5부[22]로 구성되어 있으며, 주요 내용으로는 최근에 활용되는 비디오카메라·컴퓨터(이메일과 인터넷 포함)·위치추적장치 등의 모든 전자감시활동이 노동자의 사전 승인 없이는 허용되지 않고(단, 종업원의 불법 또는 비리행동이 분명하게 의심되는 경우에만 사전동의 없이 감시행위가 허용됨), 사업장내 개인공간(예: 화장실, 탈의실, 휴게실 등)에 대한 감시와 비밀스런 감시활동(Covert surveillance)를 금지하고 있으며, 인터넷과 이메일에 대해서는 종업원들의 사전 동의를 없이 폐쇄할 수 없다는 등의 강화된 규제조항이 담겨져 있다.

---

에 프라이버시감독관제를 운영하고 있는 나라로는 뉴질랜드와 홍콩을 꼽을 수 있다.

21) 이 가이드라인은 연방정부 산하의 공공부문에 적용되었으며, 주요 내용으로는 (a) 명확한 금지행위 명시, (b) 수집자료 및 사용권한 위임자의 상세 정보 제공, (c) 네트워크 안전성의 필요 강조, (d) 모니터링방법 및 갈등해결기제의 명시, (e) 정기 점검 등을 포함하고 있다.

22) 뉴사우스웨일즈의 작업장감시법은 다음의 목차로 구성되고 있다: 1부 전문, 2부 종업원의 작업장감시에 대한 사전통보, 3부 금지된 감시활동, 4부 작업장의 종업원에 대한 비밀 감시, 5부 기타사항. 이 법의 원문에 대해서는 http://www.parliament.nsw.gov.au/prod/parlment/NSWBills.nsf/0/을 참조할 것.

호주의 Victoria주는 New South Wales주에 비하면 다소 미온적이기는 하나, 1990년대 말부터 프라이버시 보호를 위한 여러 주법의 입법활동을 활발하게 전개해오고 있다. 우선 Victoria 주의회는 1999년에 "감시장치법Surveillance Device Act)"을 제정한 데에 이어, 2000년년에는 "정보프라이버시법(Information Privacy Act)"을 입법하여 주 차원의 전자감시에 대한 규제를 강화하고 있다. 사업장 감시와 관련해서는 2003년 4월에 주프라이버시감독관이 주법개혁위원회에 작업장 프라이시의 보호를 위한 입법방안을 제출함으로써 작업장감시에 대한 규제장치의 제도화논의가 현재 진행되고 있기도 하다.(OVPC 2003)[23]

## 4. 소결 : 정책적 시사점

이 장에서는 사업장감시로부터 노동자의 프라이버시를 보호하기 위해 제정되어 있는 국제기준(International Standards)과 서구 국가의 입법사례를 살펴보았다. 프라이버시 보호에 관한 해외 제도적 규범의 역사적인 발전과정은 한마디로 시민권적 영역으로부터 노동권의 영역으로 심화되어온 것으로 파악될 수 있다.[24] 다시 말해, 시민들의 기본 인권이라 할 수 있는 사생활(프라이버시)과 인격권의 일반적인 보호로부터 사회구성원의 다수를 차지하는 노동자집단에 대한 사업장감시로부터의 보호로 진전된 것을 국제기준이 UN권리장전-OECD가이드라인-ILO 행위준칙으로 심화-발전되어온 궤적에서, 그리고 서구국가들에 있어 입법사례의 최근 변화추세를 통해 확인해볼 수 있다.

노동자 프라이버시의 보호에 있어 그 규제 장치를 거의 갖추고 있지 못한 우리나라의 입장에서는 관련 제도를 도입-정비하는 것이 시급히 요청되는 바, 이상

23) 빅토리아주 프라이버시감독관이 제출안 작업장프라이버시 보호방안의 상세 내용에 대해서는 OVPC(2003)를 참조할 것.

24) 다른 한편으로, 서구 국가에서 프라이버시 보호입법의 발전과정은 국가권력(공공부문)으로부터의 시민인격권 보호로부터 기업권력(민간부문)으로부터 노동자 인격권의 보호로 확장되는 소위 수평효과(Horizontal Effect)로 이해할 수도 있다.(Hendrickx 2001)

에서 살펴본 국제기준과 서구 선진국 입법사례를 통해 얻게 되는 몇 가지 정책적 시사점을 정리-제시하고자 한다. 우선, 우리나라 역시 UN와 ILO 그리고 OECD의 회원국인 만큼 이들 기구에서 제정-공포한 여러 국제기준에 맞추어 서둘러 국내의 관련 제도를 입법 또는 정비하는 것이 요망된다. 이는 우리나라의 국제적인 위상을 비추어 볼 때나 국내 사업장에서 무방비로 침해받고 있는 노동자 프라이버시의 문제 심각성을 고려할 때, 그리고 날로 발전하는 정보통신의 감시기술을 감안할 경우, 정부가 이제라도 국제규범에 부합하는 제도정비를 통해 노동인권의 보호를 위한 정책적인 노력을 경주해야 할 것으로 요망된다.

둘째, 해외의 입법사례를 살펴보건대 노동자의 프라이버시를 보호하기 위한 입법기술적 접근으로는 특별법을 제정하는 방법이 손쉽고 효과적일 것으로 판단되며, 국내의 낙후한 프라이버시 보호제도 실정을 고려해서 시민 프라이버시 또는 개인정보보호를 위한 포괄적인 특별법(예: 개인정보 보호법)과 사업장 수준의 노동자 프라이버시를 보호하기 위한 노동관련 특별법(예: 사업장감시 규제법)을 동시적으로 또는 단계적으로 입법 추진할 필요가 있다. 이때, 다수의 EU국가와 호주·캐나다에서 설치-운영되고 있는 프라이버시보호위원회(Commission) 또는 프라이버시감독관(Ombudsman)제를 관련 법률의 입법시에 포함시켜 도입하는 것이 요망되며, 보다 적극적으로는 (EU국가들의 사례에서 보여주듯이) 사업장 수준에서 노조 또는 종업원대표에게 프라이버시감독권을 부여-수행하거나 프라이버시 관련문제를 노사협의회의 의무협의 의제로 포함시키는 방안도 검토해볼 수도 있을 것이다.

셋째, 해외 입법사례 및 관련 판례에서 역시 드러나듯이, 사업장감시는 노사간에 이해상충될 수 있는 사안인 만큼 그 합법적 경계(Legitimate Boundary)를 제도적으로나 규범적으로 잘 확립하는 것이 바람직하며, 이를 위해서는 사용자의 재산권과 노동자의 인격권·사생활을 균형되게 보호할 수 있는 정책접근의 시각이 요구된다. 따라서, 사업장 프라이버시의 제도적 규제장치를 입법하는 과정에서 노사간의 소모적인 갈등을 최소화하기 위해서는 Clarke(1999)가 제시하는 다음의 전략요소들을 잘 고려하여 입법추진의 전략적 로드맵을 강구하는 것이 바람직하겠다:

<프라이버시 입법의 전략적 고려 요소>

① 일반 원칙 수립

② 모든 조직에 상기 원칙 적용

③ 제도/규범 준수거부에 대한 효과적 제재방법 강구

④ 산업별-기술별 세부 행동규범 수립

⑤ 기업-산업차원의 갈등해결기제 마련

⑥ 원칙-규범-제재(사법/준사법)장치를 포괄하는 종합적인 framework 확립

마지막으로, 사업장에서의 프라이버시문제는 노사 간의 집단적인 이해 갈등을 불가피하게 초래할 수 있는 성격의 사안이라는 점을 고려하여, 최근 EU 집행위원회 주도하에 추진되고 있는 사회적대화의 좋은 선례를 참조하여 우리나라에서도 노사정간의 사회적 정책협의절차를 거쳐 노사 간의 이해 조화와 올바른 노동 프라이버시 질서를 도모할 수 있는 규범적 정책원칙과 관련 제도의 제정을 추진하는 것이 요망된다.

# 6장. 법적 규제 개선방향

## 1. 전자 노동감시의 법적 평가

### 1) 전자 노동감시를 둘러싼 노사간의 권리관계[25)]

사용자는 사용자의 재산권과 영업의 자유 또는 사용자에게 주어진 시설관리권 또는 노무지휘권에 기초하여 효율적인 경영과 안전 관리 또는 생산현장 관리·통제를 위한 감시카메라 등에 의한 전자 노동감시를 정당화한다. 이에 대하여 근로자들은 인격권과 행복추구권, 사생활의 권리(프라이버시권)를 침해당하고 노동3권의 행사를 무력화하는 데 이용되는 전자 노동감시를 부당하다고 한다. 즉, 사용자는 직업의 자유(헌법 제15조)와 재산권 보장(제23조)에 기초한 노무지휘권과 시설관리권을 기초로 사업장의 전자 노동감시를 정당화하고, 이에 대하여 근로자는 인간의 존엄성(헌법 제10조), 사생활의 자유(제17조), 통신비밀의 자유(제18조), 신체의 자유(제12조), 양심의 자유(제19조), 근로권(제32조), 근로3권(제33조) 등의 헌법상 기본적 인권을 근거로 또는 근로기준법상 강제근로의 금지(근기법 제6조)를 근거로 사업장의 전자 노동감시를 부정적으로 보고 있다.

---

25) 하경효, 새로운 근로감시기술의 도입에 따른 법적 문제, 노동법학 제18호, 한국노동법학회편, 2004.6, 106-111면; 김승환(2001), 노동현장에서의 "CTV 설치와 노동자의 인권" (노동자 감시 문제와 대용 CCTV문제 해결을 위한 토론회 발표문), 노동자감시 반대·대용 CCTV철거를 위한 전북공동대책위, 2001.9.12; 박훈(2001), 대용 손해배상 청구 사건에서의 핵심적인 쟁점과 이에 관련한 문제에 대하여, 위 토론회 자료집, 2001.9.12 참조.

### (1) 근로자의 권리

헌법 제10조는 모든 국민은 인간으로서 존엄과 가치를 가지며 행복을 추구할 권리를 가진다고 규정함으로써 인간의 존엄과 가치와 행복추구권을 인정하고 있다. 인간으로서의 존엄과 가치는 우리 헌법의 최고 구성원리이면서 동시에 주관적 권리로서의 법적 성격을 갖는 기본권이고[26] 모든 기본권의 이념적 출발점이 되고 있다. 헌법재판소도 인간의 존엄과 가치의 기본권성을 인정하고 있다.[27] 따라서 근로자도 당연히 인간의 존엄과 가치를 행복추구권과 함께 주관적 권리로서 향유할 수 있다.

인간으로서의 존엄과 가치의 헌법적 의미는 인간은 동물이나 물적 재화와 구별된다는 것(인간성)과 인간을 단순한 객체나 수단으로 전락시킬 수 없다는 것(주체성)을 뜻한다.[28] 따라서 인간의 존엄과 가치에는 일반적 인격권으로서 예를 들어 당사자의 동의 없이는 사진이나 카메라에 강제적으로 찍히거나 이를 신문 잡지 등에 게재 당하지 않을 자유인 초상권 또는 자신의 행동을 감시당하지 않을 권리 등이 일반적으로 인정되고 있으며, 일반적 행동의 자유권으로서 자신이 싫어하는 것을 중지할 권리와 이를 요구할 권리가 내재되어 있는 것으로 해석되고 있다.

또 헌법 제17조는 모든 국민은 사생활의 비밀과 자유를 침해받지 않는다고 규정하고 있는데 일반적으로 이를 프라이버시권[29]이라 부르고 헌법 제10조와 관

26) 헌법학에서는 헌법 제10조의 인간의 존엄과 가치가 기타의 기본권을 파생시키는 주 기본권 내지 포괄적 기본권으로서 인정될 수 있는지, 인간의 존엄과 가치가 헌법 제10조 자체만에 의하여 독자적인 기본권의 성격을 갖는지 아니면 헌법 제37조제1항과의 상호관계에서 기본권성이 인정되는 것인지 여부에 대하여 이견이 있다. 계희열, 헌법학(중) , 박영사, 2002, 192면; 김철수, 헌법학신론 , 박영사, 2003, 262면; 허영, 한국헌법론 , 박영사, 2003, 317면 이하 참조.

27) 헌법재판소 2002.7.18, 2000헌마327 결정, 헌법재판소 2001.7.19, 2000헌마546 결정 등. 헌법재판소는 인간으로서의 존엄과 가치의 구체적인 권리성을 인정하고 인격권으로 해석한다. 즉, "모든 기본권 보장의 종국적 목적(기본이념)이라 할 수 있는 인간의 본질이며 고유한 가치인 개인의 인격권…"(헌법재판소 1990.9.1. 89헌마82결정) 또는 "모든 권리의 출발점인 동시에 그 구심점을 이루는 인격권…"(헌법재판소 1991.9.16. 89헌마163결정)이라고 한다.

28) 김승환, 앞의 글, 참조.

29) 인권사(人權史)에서 비교적 늦게 등장하기 시작한 인권들로는 망명권, 평화적 생존권, 일조

련성 속에서 논의를 전개하고 있다. 이러한 프라이버시권은 한마디로 "개인, 집단, 기관들이 자신에 대한 정보가 언제, 어떻게 어느 범위까지 타인에게 전달되는가를 스스로 결정해야 한다는 요구"로 정의될 수 있다. 이 헌법 제17조의 사생활의 비밀과 자유는 헌법 제18조의 통신의 자유와 함께 사업장의 전자 노동감시와 관련하여 근로자에게 중요한 의미를 가지는 기본권이다.

한편, 헌법상 기본권(인권)은 공권력에 대해서만이 아니라 사인(私人)에 대해서도, 특히 경제적 또는 사회적 힘을 가진 자에 대해서도 간접적으로 그 효력이 인정된다. 따라서 전자 노동감시와 관련된 위의 헌법상 기본권은 다른 사법상 법률관계와 마찬가지로 근로관계에도 간접적으로 기본권의 효력이 인정된다. 때문에 사용자는 근로자와의 관계에서 헌법상 기본권을 존중할 의무가 있다.[30]

또 헌법 제10조의 인간의 존엄과 가치로부터 또는 이와 함께 헌법 제37조제1항을 비롯한 인간의 존엄성의 실현을 목적으로 하는 제반 기본권으로부터 헌법상 인격권 개념을 도출할 수 있으며, 이로부터 원칙적으로 사법상의 인격권 개념도 인정된다. 이에 따라 오늘날 생명, 신체, 건강, 자유 외에 프라이버시, 명예 등도 일반적인 인격권의 내용으로서 불법행위의 보호를 받을 수 있다.

이러한 헌법상 인격권 또는 사법상 인격권은 근로관계에 있어서 근로자에게

권(日照權), 초상권, 환경권, 프라이버시권, 문화유산에 대한 권리, 개발에 대한 권리, 장애인의 권리, 어린이의 권리 등이다. 이 중 정보사회에서 특히 중요성을 띠는 인권은 프라이버시권이다. 초기에 학자들(Samuel D. Warren, Louis D. Brandeis, Thomas M. Cooley)은 프라이버시권을 "혼자 있을 수 있는 권리"(right to be let alone)라고 말하였다. 이는 자기에 관한 정보를 말하지 않을 수 있는 권리, 드러내지 않을 수 있는 권리, 이를 침해할 때에는 방어를 하고 침해의 중지를 요구할 수 있는 권리라는 뜻을 가지고 있다. 적극적으로 무엇인가를 요구하는 권리가 아니라는 점에서 프라이버시권은 소극적 권리의 뜻으로 이해되었다. 그러나 컴퓨터를 이용한 개인정보의 대량수집·처리·유통이 가능해진 정보사회에 들어서면서 상황이 본질적으로 달라졌다. 개인은 자신에 관한 정보를 누가 어떻게 수집·활용하고 있는지를 알아야 한다는 문제가 발생하였다. 이 때부터(1960년대) 학자들(William M. Beaney, Alan F. Westin)은 프라이버시권을 "자기에 관한 정보의 흐름을 통제하는 개인의 권리"(individual's right to control the circulation of information relating to himself)로 이해하기 시작하였다. 미국 연방대법원은 1965년에 '그리스울드 사건(Griswold v. Connecticut, 381 U. S. 479)에서 프라이버시권을 "자기에 관한 정보를 선택적으로 개시(開示)하는 권리" 내지는 "자기에 관한 정보의 흐름을 콘트롤하는 권리"라고 해석함으로써 이러한 학설을 뒷받침하였다.(김승환, 앞의 글 참조)

30) 하경효, 근로관계에 있어서 근로자의 양심의 자유와 자기책임, 노동법에 있어서 권리와 책임 (김형배교수화갑기념논문집), 박영사, 1994, 171면; 하경효, 새로운 근로감시기술의 도입에 따른 법적 문제, 노동법학 제18호, 한국노동법학회편, 2004.6, 107면.

도 인정된다. 따라서 근로관계에 있어서 사용자는 근로자의 인격권 또는 인격적 이익을 존중하고 침해하지 않도록 하는 부작위 의무를 진다. 이는 근로계약상 사용자의 부수적 의무에는 근로자의 인격적 이익을 침해해서는 안 될 의무가 포함되며, 사용자가 전자 노동감시 장비에 의한 감시활동에 의하여 발생하게 될 근로자의 인격적 이익의 침해를 사전에 방지할 의무를 지고 있다는 것을 의미한다.

또 전자 노동감시를 받고 있는 근로자의 근로는 경우에 따라 "근로자의 정신 또는 신체상의 자유를 부당하게 구속하는 수단으로써 근로자의 자유의사에 반하는 강제근로"에 해당할 수도 있다. 근로기준법 제6조는 이러한 강제근로를 금지하고 있다.

### (2) 사용자의 권리

사용자는 헌법 제15조의 직업의 자유의 내용으로서의 직업행사의 내용인 영업의 자유와 헌법 제23조에서 보장하는 재산권의 주체이다. 또 사용자는 사법영역에서도 이러한 헌법상의 기본권을 기초로 하여 자유로운 계약을 체결하고 이를 통해 획득한 근로자에 대한 노무지휘권을 행사하거나 또는 기업의 유·무형 자산에 대하여 소유권에 기초한 기업시설관리권을 행사할 수 있다.

따라서 사용자는 이러한 영업의 자유와 노무지휘권의 행사의 일환으로서 생산성향상이나 기타 경영상 목적을 실현하기 위해 근로자에 의해 수행되는 작업과정을 통제하고 감시하는데 이해관계를 가지고 있다. 또한 기업시설의 단순한 보안관리를 위해 정문이나 기업건물 내·외부에 감시카메라를 설치할 수도 있다.[31]

이와 같이 사용자의 노무지휘권이나 시설관리권도 근로자의 인격권과 마찬가지로 보호할 가치 있는 권리이다. 그러나 이러한 사용자의 권리행사가 구체적인 근로관계에서 노동통제·감시의 형태를 취한다면, 근로자와 사용자간의 이해관계의 충돌은 피할 수 없게 된다.(하경효, 2004, 110면)

---

31) 하경효, 앞의 논문(2004), 109면.

### (3) 사용자의 인격적 이익의 존중의무와 이익형량의 필요성

근로계약 체결 당시 또는 그에 기하여 실제로 노동력을 제공하는 과정에서 근로자의 인격보호는 그 존중 및 침해금지라는 사용자의 계약상 부수적 의무 안에 포섭될 수 있다. 예컨대 사용자가 사업장에서 근로자의 신체적 완전성을 보호하고 침해하지 않을 의무를 부담하는 것은 사용자의 보호 및 주의 의무로부터 도출되며, 사용자의 이러한 주의 의무로부터 근로자의 인격권을 침해하지 않을 의무도 도출된다.

이와 같이 사용자에게 부수적 의무의 구체적 내용으로서 인격권 침해금지의무가 부과되는 이상, 적어도 근로자 인격권의 핵심이라고 할 수 있는 인간의 존엄성을 본질적으로 침해하는 행위는 근로자의 동의여부를 불문하고 허용되지 않는다. 다만, 근로관계에서 정신적 고통을 발생시키는 사용자의 모든 행위가 언제나 그리고 무조건 근로자의 인격적 이익을 침해하는 것은 아니다. 그러한 근로자의 인격적 이익의 침해여부는 사용자의 계약상의 권리로서의 지시권 또는 감독권과의 이익형량을 거친 후에만 판단될 수 있다. 따라서 사업장의 전자 노동감시와 관련한 법적 판단은 필수적으로 사용자와 근로자간 이익형량을 요구하게 된다.

## 2) 전자 노동감시의 정당성 판단기준

### (1) 감시의 대상, 목적 및 중요성에 대한 이익형량

사업장에서 전자적 장비에 의한 전자 노동감시의 허용 여부를 판단함에 있어서 먼저 이를 둘러싼 사용자와 근로자의 각각 보호할 가치가 있는 이익을 서로 비교·형량하여야 한다. 이익형량을 위해서는 양 당사자의 이해관계상황을 특정하여야 한다. 이를 위해서는 첫째, 법적으로 평가되어야 할 사업장 감시의 대상이 무엇인지 확정해야 하고, 둘째, 감시장비의 구체적 목적을 고려해야 하고, 셋째, 그 이해관계 상황 각각의 중요성을 평가해야 한다. 사업장 감시가 근로계약상 근

로자에게 부담지워진 노무제공의무와 밀접하게 관련될수록 감시장치에 의한 침해가 허용될 여지가 그 만큼 더 커질 수 있지만, 반대로 감시수단이 근로자의 사적 생활영역에서의 인권 내지 인격적 이익과 더 많은 관련성을 맺게 된다면 그러한 통제는 그 만큼 허용되지 않는 것으로 이해해야 한다.

참고로, EU의 보고서[32]에 의하면 "근로자들은 매일 아침 회사에 들어서면서부터 자신의 개인정보를 보호받을 권리를 포기하지 않는다. 회사에서 타인들과 인간관계를 넓혀나감에 따라 프라이버시 보호에 대한 적절한 수준의 기대를 하게 된다. 하지만 근로자의 권리는 사용자의 합법적인 권리와 요구, 특히 회사를 어느 정도 효율적으로 운영할 권리와 무엇보다 근로자의 행동에 의한 피해를 입는 것으로부터 보호받을 권리 사이에 균형을 이뤄야 한다. 이러한 사용자의 권리와 이익은 근로자의 프라이버시를 제한하는 적절한 제도를 정당화하는 합법적 근거가 된다. 사용자가 근로자의 범죄행위의 피해자가 되는 경우가 그런 예에 해당한다.

이렇게 다양한 권리와 요구들의 균형을 이루기 위해선 여러 가지 원칙들이 필요하다. 감시행위가 사용자의 요구를 만족시키기에 편리하다는 단순한 사실만으로 사용자의 행위가 정당화되지는 않는다는 것을 명심해야한다. 감시는 이 보고서에 제시된 여러 원칙들의 검토를 거쳐 수행되어야 한다."고 하여, 사용자의 이익과 근로자 이익 사이의 이익형량이 필요하다는 점을 강조하고 있다. 구체적인 평가기준으로서는 "①감시행위가 근로자에게 투명한가? ②전자통신감시가 필요한가? 전통적인 감시방법으로는 똑같은 결과를 얻을 수 없는가? ③개인정보의 처리가 근로자에게 공정하게 여겨지는가? ④결합되는 이해관계 사이에 균형이 유지되는가?"를 제시하고 있다.

### (2) 근로자의 수인 의무와 사용자의 사전통지 의무

감시의 대상, 목적 및 중요성에 대한 이익형량을 통해서 사업장 감시를 둘러싼 근로관계 양 당사자의 이익 중 어느 쪽이 더욱 큰 이익을 가지는지를 비교·

32) EU, 회사에서의 전자통신 감시에 관한 특별조사위원회 보고서 (2002.5.29) 참조. 이 자료는 노동자감시근절연대모임(http://www.gamsi.net)에서 작성하였음.

형량하는 판단이 이루어지게 된다. 만약 근로자의 인격적 이익 또는 프라이버시 보호이익이 더 크다고 판단되면 일단 전자 노동감시는 허용될 수 없다. 반대로 사용자의 통제이익이 더 크다고 판단되면 관련 근로자는 이러한 통제장비의 설치와 운영을 수인할 의무를 부담하게 된다. 다만 여기에서도 양 당사자의 상충하는 이익을 가능한 한 조정하여 적정한 균형을 유지하도록 하는 원칙이 함께 고려되어야 한다. 따라서 사업장 감시에 대한 사용자의 이익이 일견 크다고 하더라도 그러한 감시장비의 설치는 그러한 목적달성을 위한 최소한의 정도에 머물러야 한다.

이익형량의 결과에 따라 사용자에 의한 사업장 감시가 허용될 수 있다고 판단되는 경우에도 원칙적으로 사업장 감시를 위한 기계장치의 설치 및 이를 통한 감시는 관련 근로자에게 사전에 통지되어야 한다. 따라서 사전통지 없는 감시장비의 설치(예컨대 몰래카메라 또는 전화도청 등)는 단순한 도난방지와 같은 업무상 필요성이 인정되는 경우라고 하더라도 근로자의 존엄성이나 인격권을 침해하는 행위로서 허용될 수 없다. 물론 업무상 필요에 의해 감시장비의 설치를 결정한 사용자가 이 사실을 근로자에게 사전에 통지했다고 해서 그러한 사용자의 잠시활동이 바로 정당화되는 것은 아니다. 이 경우에도 여전히 그 허용여부는 근로관계 당사자간의 이익형량을 통해서 결정되어야 한다. 따라서 이익형량을 통해 전자장비에 의한 사업장 감시에 대한 사용자의 이익이 보다 중대한 것으로 판단된다면 근로자가 이에 동의하지 않더라도 사용자는 사전 통지만으로도 그러한 조치를 정당하게 시행할 수 있다.

### (3) 근로자의 동의

당사자 간에 이익형량을 통해 근로자 측의 불이익이 더 크고 근로자의 인격권이 침해될 가능성이 있어서 그 자체로서는 사용자측의 감시장비 설치가 허용될 수 없는 경우라고 하더라도 근로자가 이에 개별적으로 동의했다면 사용자의 감시행위가 정당화되는지 문제된다. 원칙적으로 근로자가 자신의 인격적 행위에 대한 침해행위에 대해 동의하였다면 그것이 인간의 존엄과 가치를 극단적으로 해하는 것이 아닌 한 사업장 감시는 허용된다.

원칙적으로 허용되는 근로자의 동의는 자유로운 의사에 기한 것임을 요한다. 이러한 동의방식에 대해서는 그 진정성, 즉 근로자의 자유의사의 존재에 대해 엄격하게 평가하여야 한다. 서면상 동의의 진정성을 형식적으로 인정하여 근로자의 인격권 침해 소지가 존재함에도 불구하고 근로자가 이에 동의하였다는 이유만으로 당해 감시가 무조건 허용된다고 판단할 수는 없다. 결국 사업장 감시의 허용여부를 최종적으로 판단함에 있어서는 서면동의의 구체적 양태를 고려하여야 한다. 따라서 통일된 양식의 근로계약서에 의한 근로자의 동의가 유효한 것으로 인정받기 위해서는 당해 근로자에게 시행될 감시의 종류와 목적 등이 사전에 설명되어야 한다.

## 2. 전자 노동감시 규제에 관한 법제 현황

우리나라에는 일반인을 대상으로 한 전자적 장치에 의한 사생활의 감시에 관한 규제뿐만 아니라 근로자를 대상으로 한 사업장의 전자 노동감시의 규제에 관한 일반법도 존재하지 않는다. 그나마 관련 특별법으로 우편물, 전자메일, 전화통화의 감[illegible]·감청의 제[illegible] 이로부터 획득한 통신내용 및 개인정보의 공[illegible]를 금[illegible]하는 통신비밀보호법, 정보통신망 이[illegible]촉진 및 정보보호 등에 관한 법률 및 위치정보의 보호 및 이용 등에 관한 법률 (2005.1.27, 법률 제7372호) 등이 있지만, 전자적 감시장비에 의한 일반인의 사생활이나 전자 노동감시 자체를 규율하는 법으로서는 미흡하다고 하지 않을 수 없다. 위 법들은 주로 정보통신서비스제공자와 이용자와의 관계만을 규율하고 있으며, 개인정보보호나 감시규제 등에 관해서는 거의 규율하고 있지 않다. 따라서 아직까지는 헌법상 인간의 존엄과 가치, 사생활의 보호 및 통신의 자유 등의 기본권의 해석론에 의하여 해결할 수밖에 없으며, 새로운 입법이 요구되는 이유가 여기에 있다.

### 1) 헌법

우리 헌법은 앞에서 본 바와 같이 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.”(제10조)고 하여 인간의 존엄과 가치 및 행복추구권을 기본권중 기본권으로 규정하고 있으며, “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다. 모든 국민은 통신의 비밀을 침해받지 아니한다”고 하여 사생활의 자유(제17조)와 통신비밀의 자유(제18조)를 보장하고 있다. 또 헌법에 명시되지 않은 기본권도 헌법에 열거되지 아니한 이유로 경시되지 않는다는 일반적 기본권도 규정하고 있다(헌법 제17조). 이와 같이 사업장에서의 전자 노동감시는 헌법상 인간의 존엄과 가치, 행복추구권, 사생활의 자유 및 통신비밀의 자유에 대한 기본권침해 문제와 직접적으로 관련된다.

뿐만 아니라 사업장에서의 전자 노동감시에 대해서는 헌법상 신체의 자유(제12조), 양심의 자유(제19조), 근로권(제32조) 및 근로3권(제33조) 등의 기본권 침해를 야기하기도 한다. 따라서 사업장에서의 전자 노동감시가 이상의 헌법상 기본권 침해문제를 야기하는 경우에 근로자는 기본권의 제3자적 효력을 근거로 사용자의 불법행위를 다툴 수 있으며, 감시의 배제와 손해배상을 청구할 수 있다.

### 2) 노동관계법

우리 근로기준법은 사업장에서의 전자 노동감시에 의한 근로자의 인격적 이익의 보호에 관한 직접적인 규정을 두고 있지 않다. 다만 근로기준법 제6조가 근로자의 신체 또는 정신상의 자유를 부당하게 구속하는 강제근로를 금지하고 있으며, 제101조에서 사업장의 부속기숙사에서 기숙하는 근로자의 사생활의 자유를 침해하지 못하도록 규정하고 있을 뿐이다.

또 법의 성격상 직접적인 규정을 두고 있지는 않지만, 사업장에서의 전자 노동감시 장비를 이용하여 사용자가 조합활동을 감시하거나 노동조합에 관한 정보

를 수집하는 경우에는 노동조합및노동관계조정법상 부당노동행위에 해당한다(동법 제81조제4호 참조).

### 3) 정보·통신 관련법

현재 우리나라 법률 중 감시를 일반적으로 규율하는 정보통신 관련법은 존재하지 않으며, 특정한 경우에 통신비밀보호법이 적용될 수 있으나 이를 통한 전자노동감시의 규제는 실효성을 거둘 수가 없을 것으로 보인다.

통신비밀보호법의 관련 규정으로는 법 제2조(정의), 제3조(통신 및 대화비밀의 보호), 제4조(불법검열에 의한 우편물의 내용과 불법감청에 의한 전기통신내용의 증거사용금지), 제14조(타인간의 비밀대화 침해금지), 제16조(벌칙) 등이 있다.

통신비밀보호법에 의하면 "누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다"고 규정하고 있으며(동법 제3조), 이 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자는 10연 이하의 징역과 5년 이하의 자격정지에 처하도록 하고 있다(동법 제16조). 동법에서 "전기통신"이란 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(동법 제2조제1호), "감청"이란 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다(동법 제2조제7호).

통신비밀보호법은 제한적으로 프라이버시권을 보호하고 있을 뿐이다. 위 법률의 규정에 의하여 작업장에서 사사로운 이메일을 열람하는 것, 전화통화 내용을 청취하는 것, 노동조합 사무실을 감청하는 것 등에 대해서는 처벌할 수가 있다. 그러나 위 법률은 '통신'과 '타인간의 대화'를 보호하고 있으나 무단으로 다른 사

람을 감시하여 촬영하거나 작업 속도를 전자적인 장치로 감시하는 것에 있어서는 이를 처벌 대상으로 삼지 않아 제한적으로만 프라이버시권을 보호하고 있다. 따라서 감시카메라를 설치하여 작업장 모습을 촬영하는 것은 통신비밀보호법에 저촉에 되지 않으나 작업장에서 일하는 근로자들간의 대화를 녹음한다면 이는 타인간의 대화를 녹음하는 것으로 처벌대상이 된다.

위와 같은 법률을 개정하여 법률명도 '사생활비밀보호법'으로 정하고 당사자가 원하지 않는 모든 촬영과 감청, 녹음을 제한하고 그 벌칙도 강화하는 쪽으로 입법 개정하는 것이 바람직하다.[33]

또, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「위치정보의 보호 및 이용 등에 관한 법률」(제정 2005.1.27, 법률 제7372호)이 제정되어 있다. 정보통신망이용촉진법은 '개인정보'를 "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 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다"고 규정하고 있다(동법 제2조제1항제6호). 동법은 정보통신서비스제공자 등으로 하여금 개인정보를 일정한 허용범위를 벗어나 이용하거나 제3자에게 제공하는 것을 금지하고 개인정보 보호를 위해 필요한 조치를 강구하도록 명령하고(동법 제24조 및 제28조), "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니된다"고 하여 개인정보의 침해금지 주체를 제3자에까지 확대하고 있다(동법 제49조).

위치정보보호법 에 의하면, "누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니된다. 다만, 제29조의 규정에 의한 긴급구조기관의 긴급구조 또는 경보발송 요청이 있거나 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다."고 규정하고 있다(동법 제15조 제1항). 또 위치정보사업자 등은 위치정보의 보호조치를 취하여야 하고(동법 제16조), "위치정보사업자등과 그 종업원이거나 종업원이었던 자는 직무상 알게 된 위치정보를 누설·변조·훼손 또는 공개하여

33) 박훈, 앞의 글 참조.

서는 아니된다."(동법 제17조). 특히 위치정보보호법은 위치정보사업자가 개인위치정보를 수집하고자 하는 경우에는 미리 일정한 사항을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻도록 하고 있다(동법 제18조). 또 위치기반서비스사업자가 개인위치정보를 이용하여 서비스를 제공하고자 하는 경우에는 미리 일정한 사항을 이용약관에 명시한 후 개인위치 정보주체의 동의를 얻어야 한다(동법 제19조).

### 4) 외국에서의 법적 규제

#### (1) 프랑스

프랑스 노동법은 "어느 누구도 개인의 권리를 제한할 수 없다. 이를 제한하기 위해서는 그 제한이 정당하고 적절한 범위 내여야 한다"라고 규정하여 프라이버시권을 침해하는 사용자에 대해 법적 조치를 취할 수 있도록 하고 있다. 특히 근로자에게 알리지 않은 방법으로 근로자의 개인정보를 수집하는 것을 금지하고(L.121-8항), 노동조합 활동에 관한 감시를 엄격히 금지하고 있다(L.122-45항). 사용자는 은밀한 감시로 알아낸 노동조합 활동 사실을 근거로 근로자를 해고하거나 징계할 수 없다. 또한 근로자의 프라이버시를 침해하는 행위가 적법하려면 매우 엄격한 판단을 거쳐야 한다. 프라이버시 침해행위가 적법하기 위해서는 문제되는 프라이버시 침해행위가 근로자가 수행하는 업무와 관련성이 있어야 하고, 그 방법은 목적에 합당한 것이어야 한다. 따라서 근로자가 동의를 하였다거나 침해적인 감시행위를 묵인했다는 사실만으로 프라이버시권의 침해가 정당화될 수는 없다.

1991년 통신비밀법에 의하면 사용자는 사법부의 영장에 의하지 않고는 작업장에서 근로자의 개인적인 통신에 접근할 수 없다. 프랑스 대법원은 근로자에게는 프라이버시권이 있고 이것은 사업자가 근로자에 의해 송수신된 개인적 메시지의 내용에 접근할 수 없다는 의미라고 판시한 바 있다. 프랑스 민법 제9조는 사업장에서 비밀스런 감시 도구의 사용을 금지하는 것으로 해석된다. 나아가 사용자는

위법하게 수집한 정보를 가지고 근로자를 징계하거나 해고할 수 없다. 안전 목적으로 감시가 적법하게 이루어지는 경우에도 안전 문제와 무관한 모든 말과 행동을 감시하는 경우에는 위법이다.

프랑스에서 근로자 프라이버시권을 보호하는 기관은 '국립정보자유위원회'이다. 국립정보자유위원회는 정보프라이버시법(1978)에 의해 설립되었는데 작업장 프라이버시 문제에 대해 법률적으로 구속력이 있는 의견제시와 권고를 하고 있다. 특히 공공부문 사용자가 전자적인 사업장 감시 시스템을 설치하고자 하는 경우 국립정보자유위원회의 사전 승인을 얻어야 한다. 근로자 11명 이상의 사업장에서는 '근로자위원회'가 근로자 프라이버시 보호의 책임을 맡는다. 사용자는 새로운 기술을 도입하거나 감시도구를 비롯해 근로자의 활동을 통제할 수 있는 수단을 도입할 경우 미리 근로자위원회에 알리고 협의를 해야 한다. 만약 사용자의 대응이 부적절하거나 합의하지 못할 경우 근로자는 노사심판소에 조정신청을 할 수 있고 심판소는 가처분 결정이나 금전배상을 명할 수 있다.

### (2) 독일

독일의 경영조직법(Betriebsverfassungsgesets) 제87조 제1항 제6호는 사용자가 근로자의 행동과 업적의 감시를 예정한 기술적 장치의 도입과 그 이용에 관한 조치를 하기 위해서는 사업장평의회(Betriebsrat)와의 공동결정(Mitbestmmung)을 거쳐야 한다고 규정하여 기술적 장치를 이용한 근로자의 감시로 인하여 기본법(독일 헌법)상의 '인간의 존엄', '인격의 자유로운 발현의 권리' 등의 기본권에 기초한 근로자의 인격적 자유가 침해되는 것을 방지하기 위한 집단적 규율절차를 마련하고 있다. 독일의 사업장조직법 규정의 해석상 직접 근로자의 행동과 업적의 감시를 목적으로 하여 기술적 장치를 사용하려는 경우는 물론이고 사용자가 어떠한 기술적 장치를 이용하려는 본래의 목적이 직접적으로 근로자의 감시를 위한 것이 아니라고 할지라도 그 부수적인 효과로서 기술적 장치의 이용에 따라 얻게 되는 자료가 사용자에 의하여 근로자의 행동과 업적을 판정하는데 사용될 수 있는 객관적인 가능성이 있는 경우 그 역시 위 법 소정의 공동결정 사항에 해당한다는

것이 독일의 판례와 통설의 견해이다.[34]

이에 따라 독일 연방노동법원은 헌법상의 인격권 조항에 따라 근로자의 프라이버시권을 인정하고 있으며 이는 사업장평의회와 회사의 단체협약에 의해서도 보호되고 있다. 공공부문 근로자는 작업성과를 측정하거나 근로자 행동을 감시할 수 있는 도구를 도입하거나 운영하는 문제를 결정하는데 참여할 권리가 있다. 이메일이나 인터넷 사용을 감시할 수 있는 도구를 도입할 때도 마찬가지이다. 또 경영조직법에 따라 사용자와 사업장평의회는 정보통신기술의 활용으로 근로자의 프라이버시가 침해되는 데 대해 보호 수단을 마련할 의무를 갖는다. 단체교섭에서 근로자 감시에 대해 합의가 이루어지지 않을 경우 사용자와 사업장평의회는 근로자 감시 도구의 도입이 가져올 문제점에 대해 전문가의 도움을 받아 합의해야 한다. 연방노동법원은 그 도구가 직접 근로자의 행동을 감시하기 위한 것이건 결과적으로 그러한 것이건 근로자를 감시하는 도구가 도입될 때는 사용자와 사업장평의회가 공동으로 결정해야 한다고 명시했다.

### (3) 영국

영국은 2000년 8월에 통과된 「조사권한규제법」에 의해 사업자가 통신의 송신자와 수신자 양쪽의 동의를 구하지 않고 전화와 이메일을 감청하는 것을 위법이라고 규정하고 있다. 이외에도 작업장내 프라이버시 보호와 관련하여 데이터보호법 (Data Protection Act, 1984.7.12)은 제2장에서 데이터 보호 원칙을 규정하고 있다. 데이터 보호 원칙은 8가지로 되어 있다. 그 중 제3원칙에 따르면 개인 데이터는 그 목적에 합치되지 않는 태양(態樣)으로 이용되거나 제공되어서는 안 된다. 제4원칙에 따르면 일정한 목적을 위하여 보유되는 개인 데이터는 그 목적에 관하여 적정하고 관련성을 가져야 하며, 과도한 것이어서는 안 된다. 제4원칙에 따라 개인 정보의 지나친 집중이 제한된다. 또 '영국정보보호위원회'에서 마련한 사업자와 근로자의 관계에서 개인정보이용에 관한 실무규정이 있다. 이 실무규정의 주

□□ □□

34) BAG 1975. 10. 6.자 결정, DB 1975, 2223. 김지형, 근로기준법 해설, 청림, 2000, 75-78면에서 재인용.

요 내용으로 ①사업자는 개인정보 수집에 있어서 정당한 사유와 분명한 목적 하에서만 수집하고 사전에 근로자에게 알리고 동의를 구해야 하며 ②근로자는 사업자가 자신의 데이터를 보유하고 있는 것의 데이터 내용, 용도, 의도를 정기적으로 통보받아야 하며(복사본) ③특별히 민감한 데이터는 해당법의 특별한 통제를 받는다(정치적 성향, 종교, 성생활, 민감한 건강 데이터 등) 또한 ④근로자의 범죄기록, 유전자 검사는 특별한 제한을 두며 ⑤사업장 감시는 정당한 사유를 가지고 사전에 통보하며 감시장치는 눈에 보이는 곳에 설치할 것 등에 대해서 규정하고 있다.

### (4) 기타

오스트레일리아의 뉴사우스웨일즈에서는 직장에서의 비디오감시에 대한 규제법이 제정되어 시행되고 있다. 이 법은 은밀한 비디오감시의 원칙적인 금지, 공개적인 비디오 감시의 경우 14일 전의 사전 통지와 상시적 고지 등을 내용으로 하고 있다. 또한 법률에 의해 직장에서의 통신비밀이 보호되며, 비밀녹음이 금지된다.

미국에서는 1974년에 「프라이버시법」(Privacy Act)이 제정되었고, 1988년에는 「컴퓨터 연결 및 프라이버시 보호법」(Computer Matching and Privacy Protection Act)으로 개정되었다. 컴퓨터 연결은 연방정부의 지불과오의 발견, 차금(借金)징수의 증대, 사회보장 사기(詐欺)의 색출에 기여함으로써 연방정부의 예산절감을 가져올 수 있다는 것이 그 입법취지이다. 그러나 그러한 장점을 인정한다 하더라도 개인정보가 그 유통에 대한 통제의 기회도 없이 다른 목적을 위하여 사용될 수 있다는 점에서 강한 비판을 받고 있다.

벨기에와 덴마크는 근로자 의료정보와 의료검진에 대해 특별보호규정을 두고 있다. 핀란드에는 노사관계에서의 프라이버시 보호에 관한 특별입법이 제정되어 있다. 이탈리아에는 근로자에 대한 감시와 모니터링을 제한하는 특별규정이 있다. 근로자의 이메일 내용에 사업자가 접근하기 위해서는 사법부의 명령이 있어야 한다. 네덜란드는 노동법에서 노동조합에 정보를 제공하고 동의를 받아야 한다고 규정하고 있다. 스웨덴은 카메라 감시장비를 도입할 경우 노동조합 대표와 협의해야

한다는 법률규정이 있으며 근로자의 작업수행을 감시할 때는 당사자에게 알려야 하고 사전에 의무적으로 노동조합 대표의 의견을 들어야 한다. 노르웨이의 경우도 직장을 감시하는 경우는 이를 단체협약사항으로 노동조합의 대표에게 알리고 협의를 거쳐야 한다.

## 3. 전자 노동감시 관련 법제 개선방향

### 1) 전자 노동감시 규제입법의 필요성과 입법체계

앞에서 본 바와 같이 정보기술의 발달에 따라 사업장에서 전자적 기술을 이용한 감시장비를 도입하여 근로자를 통제하거나 감시하는 것이 일반화되고 있다. 이로 인하여 근로자의 인권침해 사례가 빈발하고 있으며 앞으로 더욱 심각하게 전개될 것으로 보인다. 그러나 현재 우리나라 노동관계법은 이에 관하여 직접적인 규율을 하지 않고 있으며, 근로자의 인격적 이익을 보호하기 위한 일반적인 입법도 없는 실정이다. 그리하여 구체적인 문제해결은 헌법상 기본권 해석론이나 미흡한 실정법에 의지한 해석론에 의하여 해결되고 있는 상황이다. 그러므로 사업장에서의 전자 노동감시에 의한 근로자의 인격적 이익을 보호하기 위해서는 무분별한 전자 노동감시 장비의 도입과 이용을 규제하기 위한 보다 구체적인 입법적 조치가 필요하다.

사업장의 전자 노동감시를 규제하기 위한 '입법체계'에 관해서는 다음과 같이 생각할 수 있다. 먼저 ①사업장 감시에 관한 특별법을 제정하는 방안과 ②사업장을 포함한 일반적인 감시를 규율한 법을 제정하고 거기에서 사업장 감시를 규율하는 방안이 있을 수 있다. 첫째 방안은 사업장에 한정하는 프라이버시보호법을 만드는 것인데, 사업장의 특수성을 고려한 세분화된 법률을 만들 수 있다는 장점이 있으나 현재 프라이버시 일반에 대한 관련법이 없는 상황에서 사업장에 대해

서만 특별법을 만드는 데는 한계가 있을 수 있다. 오늘날 정보기술발달에 따른 전자적 감시 문제가 사업장의 근로자뿐만 아니라 일반인의 프라이버시권에 대한 심각한 위협이 되고 있다는 점을 감안한다면, 감시에 관한 일반 법률을 제정하고 그 법의 적용범위에 사업장 감시도 포함하되, 노사관계에 특수한 문제에 대해서는 따로 특별규정을 두거나 특별법을 제정한 방안이 일단 합리적이라고 생각된다.

둘째, 노동관계법 특히 근로기준법에 근로자의 개인정보, 사생활 및 인격권의 보호에 관한 근거규정을 명시적으로 둘 필요가 있다. 또 근로자의 인격권을 침해할 가능성이 있는 작업방식이나 감시장비의 도입과 관련된 사항을 근로기준법의 취업규칙의 필요적 기재사항 또는 노사협의회 의결사항으로 함으로써, 전자 노동감시가 전자 노동감시에 대한 규제입법과 함께 단체협약, 노사협의 및 취업규칙에 의하여 통제되도록 할 필요가 있다. 구체적으로 전자 노동감시 문제를 헌법과 노동관계법 및 관련 규제입법에 근거하여 회사와 근로자(노동조합)간 단체협약 내지 노사협정을 통해서 전자 노동감시 장비의 도입과 이용에 관한 규정 및 근로자의 프라이버시 보호에 관한 규정을 둠으로써 규범력을 획득할 수 있다.

### 2) 전자 노동감시 규제입법의 기본원칙

#### (1) 사회적 기준의 설정

전자적 장비를 이용한 사업장 감시로 인한 근로자의 피해를 구제하고, 이러한 기술들의 오·남용 사례를 사전에 차단하기 위하여 법제화를 통한 사회적 기준이 설정되어야 한다. 전자 노동감시 규제의 사회적 기준으로는 먼저 전자 노동감시는 근로자의 존엄과 가치 및 프라이버시의 침해가능성이 높기 때문에 이를 금지하는 것을 원칙으로 한다. 다만 사용자의 경영상의 이익과 비교형량하여 부득이 전자 노동감시 장비를 도입하게 되는 경우에도 해당 감시가 근로조건에 미치는 영향을 면밀히 검토하여 우선적으로 근로자의 인격권 내지 인격적 이익 나아가 자기정보 관리통제권이 침해되지 않도록 하여야 한다.

### (2) 전자 노동감시 장비의 도입요건

사용자가 합법적인 전자 노동감시를 행하기 위해서는 구체적으로 다음의 요건을 갖추어야 한다.

첫째, 사용자는 전자적 장비에 의한 감시기법을 도입함에 있어서 사전에 다른 방법이 없다는 '보충성'을 근로자에게 객관적인 방법으로 제시하여야 한다. 둘째, 사용자는 도입방법에 있어서 일방적 도입이 아닌 공개적이고 투명한 방법 즉, 장비의 장단점을 투명하게 근로자에게 공개하여야 하며, 근로자의 사전 동의 또는 노동조합과의 교섭을 통하여 민주적인 절차를 거쳐 도입방안을 제시하여야 한다. 셋째, 사용자는 사업장 감시장비를 도입할 경우 극히 제한적으로 도입하여야 한다. 예를 들어 근로자가 전혀 없는 무인 자동화공장, 위험시설에 대한 통제·감시, 근로자가 없는 지하공간의 시설물관리를 위한 조치 등을 위하여 제한적으로 도입하여야 하며, 근로자의 산업재해예방을 위한 통제·감시장비를 설치하는 경우에도 우선적으로 안전설비를 모두 갖춘 후에 근로자와 단체가 인정하고 동의한 범위 내에서 최종적으로 선택하여야 하며 근로자의 인격권을 보호할 수 있는 방안이 강구되어야 한다.

### (3) 자기정보 관리통제권의 보장

개인은 자기정보에 관하여 누가, 무엇을, 언제, 어떻게 알았고, 이를 저장했으며, 이 저장된 개인정보가 자기에게 유리한 것인지 불리한 것인지를 알 수 있어야 한다. 근로자의 경우에도 이와 같은 개인정보에 대한 자기결정권이 보장되어야 사업장에서 불안감 없이 근로를 제공할 수 있다.

자기정보 관리통제권이란 정보기술의 발달에 따라 자기정보가 광범위하게 수집·처리·관리·재가공 되어 자기정보의 침해로 인하여 피해를 받게 되는 현상이 늘어가고 있으므로 자기정보 전반에 대하여 자신에 관한 정보를 직접 관리하고 통제할 수 있는 권리를 말한다.[35] 법원은 자기정보 관리통제권에 대하여 "헌

35) 성낙인, 통신에서의 기본권보호 , 공법연구 , 제30집 제2호, 43~44쪽.

법 제10조 및 제17조의 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것"이라고 판시하고 있다.[36]

전자 노동감시 장치를 설치할 때에는 인권침해 종류의 기록금지, 개인정보수집방법의 제한, 개인의 의사에 반하는 입력의 금지, 개인정보의 무제한 축적의 금지, 자기 파일에 대한 접근권의 보장, 개인정보의 정정권의 보장, 개인정보에 대한 남용의 금지 등이 요망된다. 그리고 이러한 기본 틀을 내용으로 하여 자기정보관리통제권이 보장되어져야 한다. 동시에 보다 더 적극적으로 통제와 감시에 대하여 반대를 주장하고 철회를 요구·관철할 수 있는 권리가 보장되어야 한다.

### (4) 전자 노동감시 장비 도입에 대한 개별적 동의 또는 집단적 합의

사업장 감시장비의 설치는 새로운 기술의 도입에 의한 노동통제·감시의 문제이고 한편에서는 근로조건의 결정과 밀접한 관련이 있는 문제이므로 개별 근로자의 동의와 근로자 단체와의 집단적 합의가 필요하다. 특히 전자 노동감시 장비를 도입하는 경우에 정보독점권에 의해 발생하는 정보의 왜곡현상을 극복하기 위해서는 최소한의 개별적 동의 또는 집단적 합의의 절차적 과정이 선행되어야 한다.

먼저 근로자의 동의는 동등한 지위에서 자유로운 의사에 기하여 행해져야 한다. 동의의 형식에는 구두동의와 서면동의가 있으나, 근로자의 자유의사의 진정성을 담보하는 데에는 서면동의가 바람직하다. 동의에서 가장 중요한 것은 근로자가 정확한 판단을 할 수 있도록 동의의 내용을 명확하게 제시하여야 한다. 사용자가 일방적으로 설명과 서면을 제시하는 것, 예를 들어 경영상 목적의 당위성만을 제시하거나 고용불안을 조장하는 행위, 통제·감시의 궁극적인 목적을 우회적으로 표현하는 행위, 근무시간 중 서면동의를 요구하는 경우 등은 동의의 과정에서 근로자의 자유로운 판단을 흐리게 할 개연성이 있다. 또 대등하고 자유로운 결정은

36) 대법원 1998. 7. 28. 선고96다 42789판결.

합의의 한 형태, 즉 비강압적·비강제적 결정 또는 자발적·임의적 동의를 뜻한다.

근로자의 개별적 동의만으로는 노사당사자간의 실질적으로 대등한 지위를 확보하는 데는 한계가 있기 때문에 개별적 동의보다는 현실적으로 집단적 동의가 대등적 결정의 실현에 더 적합할 수 있다. 구체적으로 전자 노동감시 도입 문제는 근로조건에 중대한 영향을 미치므로 단체교섭 사항이 된다. 따라서 사용자는 전자 노동감시와 관련하여 단체교섭에 응할 의무와 교섭의 과정에서 합의형성을 위하여 성실하게 노력할 의무가 있다. 단체교섭에서는 실질적인 근로자의 개인정보와 인권이 충분히 보호될 수 있는 세부적 내용을 다루어야 한다. 또 근참법 제19조 제10호는 신기술·기술의 도입 시 노사가 협의하도록 하고 있다. 우리나라 노사협의회의 법적 기능에 한계가 있기는 하지만 노동조합이 없는 경우에는 전자 노동감시의 도입과 관련하여 노사협의회를 활용하는 것도 집단적 동의의 한 방법이라고 할 수 있다.

### 3) 전자 노동감시 규제입법의 구체적 방향[37]

#### (1) 전자 노동감시의 규제

가) 기본원칙

사업장의 전자 노동감시는 헌법상 근로자의 존엄과 가치, 프라이버시권 및 인

37) 권주노총, 「노동자 감시 규제와 노동자 개인정보 보호에 관한 입법 제안」, 2003.7; 이은우, 「해외 입법사례와 반감시입법제안」 "첨단기술에 의한 노동자감시, 어떻게 대응할 것인가" 토론회 발표자료(노동자감시근절을위한연대모임 주최), 2001.11.1; EU, 「회사에서의 전자통신 감시에 관한 특별조사위원회 보고서」, 2002.5.29; EU, 「개인정보의 처리와 자유로운 유통에 관한 개인정보보호지침」 (Directive 95/46/EC), 1995; ILO, 「근로자의 개인정보보호에 관한 행동강령」, 1996.10 (http://www.ilo.org/public/english/support/publ/pdf/protect.pdf); OECD, 「프라이버시보호와 개인정보의 국제적 유통에 관한 가이드라인」(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), 1980 등 참조.

격권을 침해하고, 근로조건에 영향을 미치며, 또는 노동3권을 제약할 위험성이 높다는 점을 전자 노동감시 규제입법의 기본원칙으로 확인할 필요가 있다. 이러한 기본원칙은 법률해석의 원칙이 된다. 따라서 인간의 존엄성, 사상・행동・신체・양심의 자유를 억압하고 노동3권을 침해할 가능성이 있는 모든 전자 노동감시는 원칙적으로 금지되며, 예외적으로 그것이 허용되는 경우에도 헌법상의 기본권과 근로자의 인격적 이익을 침해하는 방식으로 이루어져서는 안 된다는 점을 천명하여야 한다. 근로자들은 사업장에서 노동을 제공하는 과정에서도 자신의 개인정보와 프라이버시를 보호받을 권리가 포기되어서는 안 되기 때문이다.

나) 구체적 규제기준

근로자에 대한 전자 노동감시는 원칙적으로 허용되어서는 안 된다. 다만 특별한 경우에 예외적으로 허용될 수 있는데, 이 경우에도 ①감시가 행해지고 있다는 점에 대한 명시적이고 계속적인 고지와 표시가 있어야 하고, ②감시의 결과물에 대한 근로자의 열람 및 정정이 허용되어야 하며, ③감시의 결과물에 대하여 접근할 수 있는 자, 보관 및 폐기의 주기, 보안대책 등이 마련되고 공표되어야 하며, ④어떤 경우에도 감시는 인격권을 침해하지 않는 범위 내에서 가장 침해가 적은 방법으로 이루어져야 하며, ⑤감시의 결과물은 근로자에 대한 평가의 자료나 불리한 평가의 자료로 이용되어서는 안 된다. 그리고 감시장치를 도입할 경우에는 사전에 노동조합에 통지하고, 노동조합과의 단체협약을 통하여 동의를 얻어서 도입하여야 한다.

사업장에서의 전자 노동감시 장비의 도입과 이용에 관하여 근로자와 사용자의 이익형량이 이루어져 전자 노동감시가 허용될 수 있다고 하더라도 사용자의 감시행위가 당연히 정당화되지는 않는다. 근로자와 사용자의 다양한 권리와 요구들의 균형을 이루기 위해서는 여러 가지 원칙들이 필요하다. 감시는 이러한 원칙들의 검토를 거쳐 수행되어야 한다.[38]

EU의 지침[39]은 감시활동의 합법성을 획득하는 데 필요한 「 이메일과 인터넷 」

38) EU, 회사에서의 전자통신 감시에 관한 특별조사위원회 보고서 (2002.5.29)의 '서문' 참조.

감시에 적용되는 일반적 원칙, 을 밝히고 있다. 이를 기초로 전자 노동감시의 기본 원칙을 재구성하면 다음과 같다.

①필요성 : 사용자는 감시행위를 시작하기 전에 어떤 형태의 감시활동이 특별한 목적을 위해 절대적으로 필요한지 점검해야 한다.

②합목적성 : 사용자는 적정하고 합법적인 목적을 가지고 정보를 수집해야 하며, 그러한 목적에 부합하지 않는 경우에는 정보수집을 즉시 금지하여야 한다. 특히 통신시스템의 안전을 위해 수집한 정보는 다른 목적(예를 들어 근로자의 감시)으로 쓰여서는 안 된다(일관성 원칙).

③투명성 : 사용자는 감시행위를 항상 공개해야 하며, 법령이 정하는 예외적인 경우를 제외하고는 비공개 감시가 허용되지 않는다. 특정한 범죄행위가 명백하거나 사용자가 작업장에서의 위법행위를 적발하는 것이 법적으로 허용되어 있는 경우에 해당한다. 감시행위의 투명성을 확보하기 위해서는, 사용자는 감시와 관련하여 그 허용범위 등에 관하여 근로자에게 명확한 설명과 모든 정보를 제공하고(정보주체에 대한 고지의무), 사용자가 감시정책을 입안하기 전에 근로자대표와 협의하고, 근로자가 정보보호 규정(정보의 범위와 목적 등)을 항상 확인할 수 있게 하고, 근로자는 사용자가 수집한 자신에 관계된 개인정보에 접근할 권리를 갖는다. 또한 정보가 부정확하고 불완전한 경우에 근로자는 정보의 수정, 삭제, 접근금지에 대한 요구를 할 수 있다.

④합법성 : 정보의 처리는 합법적인 목적(경쟁사에 영업비밀이 유출되는 것과 같은 영업상의 비밀보호)을 가지고 수행되어야 한다.

⑤적정성 : 감시과정에서 얻은 개인정보는 특정한 목적을 달성하는데 있어 적정해야 하고 과도하지 않아야 한다.

⑥정보의 보존과 정확성 : 사용자에 의해 합법적으로 저장된 정보는 정확해야하고 필요 이상으로 오랫동안 보존되어서는 안 된다.

⑦안전성 : 사용자는 보존하고 있는 개인정보가 외부로부터 안전함을 보장할 적절할 기술적인 대책을 강구하여야 한다.

39) EU, 개인정보의 처리와 자유로운 유통에 관한 개인정보보호지침 (Directive 95/46/EC, 1995)

다) 전자 노동감시 시스템 도입시의 근로자와 근로자대표의 동의

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

동의는 개별적인 동의와 집단적인 동의로 나누어 근로조건과 관련된 것은 집단적 동의가 필요한 것으로 하고, 개별 근로자의 인격적 이익과 관련되는 것에 대해서는 개인적인 동의까지 받아야 하는 것으로 한다. 특히 후자의 경우에 노동조합 등 근로자대표의 집단적 동의로 근로자의 동의를 대체할 수 없다. 프라이버시권 등과 같은 개인의 인격권은 스스로 포기하지 않는 한 노동조합 등에 의하여 포기될 수 없기 때문이다.

참고로, ILO 행동강령(1996)은 a)근로자의 개인정보를 처리하는 자동 시스템의 채택 및 변경에 관하여, b)사업장 안의 전자 근로자 감시 시스템의 채택에 앞서, c)근로자의 개인정보에 대한 설문조사 및 검사를 해석하고 관리하는 방법과 내용, 목적에 대하여 근로자대표는 통지를 받고 조언할 수 있도록 하고 있다(행동강령 12.2).

라) 전자 노동감시의 유형별 규제

**CCTV를 통한 감시**

CCTV를 통한 감시는 도난 또는 위험 방지를 위해서만 허용될 수 있다. CCTV의 설치는 근로조건과 밀접한 관련이 있으므로 노동조합의 동의를 얻어야 한다. 이 경우에도 CCTV 감시는 근로자의 작업모습을 직접 촬영하는 방식으로 이루어져서는 안 된다. 한편 CCTV를 촬영하고 있을 때에는 “CCTV 촬영중”이라는 표시가 크고 선명하게 보이도록 하고, 촬영된 녹화분에 대해서는 당사자의 열람 및 정정이 가능해야 한다. 그리고 촬영된 녹화분의 보호관리에도 만전을 기해야 한다.

참고로, 1995년에 호주 뉴사우스웨일즈 프라이버시위원회가 제정한 작업장의

공개적인 비디오 감시에 대한 가이드라인 은, “비디오감시는 직장내 개인의 프라이버시에 대한 중대한 위협이다. 직장에서 비디오감시를 사용할 때는 회사의 사업상 이익과 근로자의 프라이버시 사이에 균형을 꾀하는 것이 중요하다. 회사가 비디오감시 장비를 설치할 때는 높은 수준의 규제를 받아야 한다.”고 하면서, 그 결정 과정은 다음의 내용을 고려하도록 하고 있다.

①(금지된 사용) 개별 근로자의 작업수행을 모니터링하기 위한 목적을 위한 비디오감시, 노동관계법원에서 허용하지 않는 공개적인 비디오감시, 화장실・샤워룸・탈의실에서의 비디오감시 및 노동관계법원이 허용하지 않는 락카룸과 직원 휴게실에서의 비디오감시는 허용되지 않는다.

②(협의) 회사는 비디오감시 기기를 설치할 때 근로자와 근로자 대표와 협의해야 한다. 이러한 협의의 영향을 받는 근로자들은 회사로부터 감시정책, 절차와 그 목적에 대한 문서를 제공받아야 한다.

③(고지) 초기에 근로자와 협의가 끝나면 비디오감시의 영역은 명확하게 표시되어야 한다. 이 표시들은 근로자들과 감시행위의 공중에게 고지하려는 목적과 더불어 불법적이고 부적절한 감시행위를 제지하기 위한 목적을 충족시킨다. 표시는 감시영역, 감시목적, 감시시간 및 감시책임자를 고지해야 한다.

④(정당한 감시) 카메라를 설치하고 12개월 안에, 회사는 비디오 감시가 본래의 목적을 달성하는데 효과적이라는 것을 증명해야 한다. 카메라는 오직 그 초기 목적을 달성하는 데 효과적이고 그 감시가 계속 실재적으로 정당함을 보여줄 수 있는 경우에만 유지해야 한다.

⑤(카메라 가동 시간) 비디오 감시는 카메라가 특정한 목적에 비추어 정당하게 사용되는 시간 동안에만 가동될 수 있다.

⑥(감시 카메라의 위치) 카메라는 명확하고 분명한 보안 위험이 있는 장소에만 설치될 수 있다. 카메라는 작업 기능의 직접적인 수행에 관여되어 있지 않은 근로자를 감시하는 장소에 설치되어서는 안 된다.

⑦(감시의 수행) 감시카메라는 윤리적으로만 가동되어야 한다. 카메라는 개

인을 확대하거나 이유없이 개인의 활동을 염탐하는데 사용되어서는 안 된다. 카메라는 그 목적에 적합하지 않은 기능을 위해 사용되어서는 안 된다. 회사는 카메라 조작자가 적절하지 않은 방법으로 감시를 행하는 것을 발견하였을 경우 적절한 징계 행위를 취해야만 한다.

⑧(테이프에 대한 접근, 보존 등) 테이프에 대한 접근은 감시를 본래 목적 내에서 제한적으로 기록을 사용하는 개인에게 한정되어야만 한다. 테이프에 대한 접근이 있었던 경우는 모두 기록되어야만 한다. 특별한 탐문의 목적이 없는 한 테이프는 최대 7일 동안 보존된 후에 삭제되거나 파괴된다. 법에서 보장하는 접근 이외에 직장에 대한 제3자는 테이프 기록에 접근할 수 없다. 감시카메라에 잡힌 화면으로 인해 근로자가 경고나 어떤 징계에 처하게 될 경우, 사고 당시의 비디오테이프에 대한 근로자나 근로자대표의 접근을 경고, 징계나 법적 처분이 내려진 후 14일 내에 허용해야 한다.

⑨(예외) 회사가 이 강령으로부터 특별한 예외를 적용하려면, 직장의 어떠한 특별한 상황이 직장에 일반적으로 적용되는 원칙으로부터 예외가 될 수 있는지 합리적인 설명을 제공할 수 있어야만 한다. 이러한 예외의 적용은 프라이버시 위원회에 의해 승인 또는 거부될 수 있다.

⑩(협력 사항) 회사는 비디오 감시를 수행하는 담당자를 임명한다. 자문적 판정을 하는 프라이버시 위원회에 대해 강령의 시행과 관련해 이의를 제기할 수 있다.

### 이메일 감시

현행법상 근로자의 동의 없는 이메일에 대한 감시는 허용되지 않는다. 근로자의 이메일을 사용자가 서버에 저장하는 경우에도 이메일에 대한 접근은 허용되지 않는다. 근로자의 이메일 사용과 관련한 어떤 기록이나 추적도 허용되지 않는다. 근로자는 회사 내에서 이메일을 이용할 자유가 있으며, 이를 시스템의 운용을 위하여 불가피한 경우가 아니라면 제한할 수 없다.

근로자의 이메일이 업무를 내용으로 하는 것인 경우에는 회사의 업무수행의 절차로서 이메일을 열람, 저장할 수 있으나, 이 경우에도 해당 이메일에 근로자의 개인정보가 포함되어 있는 경우에는 개인정보처리에 대한 원칙에 의하여 처리되어야 한다.

참고로, EU의 보고서[40]에 의하면, 이메일이나 전통적 방식의 편지 모두 동등한 보호의 대상이 되어야 하며, 업무영역에서의 전자통신도 '사생활'과 '통신'의 개념에 포함시키고 있다. 이 보고서는 EU지침(Directive 95/46/EC, 1995)에 따른 합법성을 다음과 같이 판단하고 있다.

①개인정보가 담긴 이메일은 보호되며, 사용자는 이 정보를 처리할 정당한 근거가 있어야 한다. 근로자는 자유로운 상황에서 동의할 수 있어야 하고 충분히 정보가 제공되어야 하며, 일반적으로 합법적 수단으로써 근로자의 동의에만 근거해서 개인정보를 처리해서도 안 된다. 정보가 공개되는 제3자나 통제자의 정당한 이해관계가 걸려있을 때는 이메일 감시가 합법화되지만, 이 경우에도 통신비밀 권리에 해당하는 근로자의 기본적 권리와 자유를 침해해선 안 된다.

②동의란 근로자가 정말로 자유롭게 선택할 수 있어야 하고, 어떤 손해 없이도 그 동의를 파기할 수 있어야 한다.

③근로자에게 순전히 개인적인 용도로 메일계정이 부여되거나 웹메일에 접근할 수 있도록 허용되었을 경우에 사용자가 이 계정을 열람하는 것은 아주 제한적인 조건에서만 정당화될 수 있다.

또 기업이 근로자에게 제공해야하는 최소한의 정보로는, ①근로자에게 순수한 개인용 메일계정을 가질 권리가 부여되는지, 작업장에서 웹메일 계정의 사용이 허락되는지, 사용자가 개인용도로 쓸 웹메일 계정의 사용을 권유했는지 여부, ②근로자가 예기치 않게 부재중일 때 메일의 내용에 접근하기 위한 설비, 접근을 하려는 목적, ③메시지의 백업 화일이 있을 때, 그것의 보존기간, ④이메일이 서버에서 틀림없이 지워졌다는 증거, ⑤안전문제, ⑥정책형성과정에서 근로자 대표의 참여 등이다.

### 인터넷 이용 감시

근로자가 인터넷을 이용하여 의사를 주고받는 경우에는 통신비밀보호법에 의하여 보호되지만, 그 외의 경우에는 현행법상 근로자의 인터넷 이용감시에 대한 규율이 없다. 근로자의 노동조합 활동을 방해하기 위하여 사용자가 인터넷 이용을

40) EU, 회사에서의 전자통신 감시에 관한 특별조사위원회 보고서 , 2002.5.29.

감시하는 경우에는 부당노동행위에 해당한다.

근로자의 인터넷 이용에 대한 차단·감시는 허용되지 않는다. 근로자의 인터넷 이용의 자유도 원칙적으로 제한되어서는 안 된다. 다만 당해 인터넷의 이용이 범죄행위를 구성하는 경우에는 사용자는 근로자의 해당 인터넷 이용을 차단할 수 있다. 이 경우에도 사전에 인터넷 이용을 차단해야 하며, 근로자의 인터넷 이용을 감시해서는 안 된다.

인터넷을 차단할 경우에는 차단하는 인터넷 웹사이트의 목록 등을 공개하여야 하며, 근로자의 이의 신청을 허용해야 한다. 근로자의 인터넷 이용에 대한 로그기록 등은 사용자에 의하여 접근, 열람되어서는 안되며, 부득이하게 컴퓨터 시스템의 운영과정에서 자연적으로 근로자의 인터넷 로그기록을 사용자가 서버에 저장하고 있는 경우에도 그 로그기록은 엄격하게 비밀로서 관리되어야 하고, 적절한 주기에 따라 삭제되어야 한다. 특히 근로자가 인터넷을 이용하여 노동조합과 관련된 활동을 하는 경우, 이것이 정당한 범위 내에서 노동조합활동으로 행해지는 경우에는 제한되거나 이를 이유로 불이익한 처우를 받아서는 안 된다.

참고로, 위 EU보고서는 업무시 인터넷의 개인적 사용에 대하여 "사용자가 근로자의 인터넷 사용의 총괄적으로 금지하는 것은 근로자가 일상생활 속에서 인터넷으로부터 얼마나 많은 도움을 받는지가 전혀 고려되지 않기 때문에 비현실적"이라고 한다. 인터넷 감시에 관해서는 다음과 같은 원칙을 제시하고 있다.

> ①인터넷의 개인적 사용을 감시하는 것보다는 가능한 범위 내에서 자동접근경고를 한다거나 몇 개의 사이트를 차단하는 등 기술적으로 접근을 제한하는 방식에 의존하여야 한다.
>
> ②인터넷의 의심스러운 사용을 적발하는 즉시 고지하는 것이 문제를 최소화한다.
>
> ③인터넷의 오용은 대부분 방문한 사이트의 내용을 검사할 필요도 없이 적발할 수 있다. 예를 들어, 사용시간을 체크하고 가장 자주 방문하는 사이트를 체크하는 것은 사용자가 자신의 장비가 오용되고 있는지 여부를 확인하기에 충분하다.

④근로자의 인터넷 사용을 점검할 때 사용자는 검색엔진이나 링크, 배너광고, 오타 등으로 인해 의도치 않게 사이트를 방문할 수도 있다는 사실을 고려하여 쉽게 결론을 내려서는 안 된다. 어떤 경우든 근로자에게 사용자가 주장하는 오용에 대해 사실을 알려야 하고, 이에 대해 이의를 제기할 수 있는 기회를 주어야 한다.

또, 회사의 인터넷 이용정책과 관련하여 다음과 같은 방식을 추천하고 있다.

①투명성의 원칙을 준수하여야 한다.

②사용자는 근로자가 복사하거나 검색할 수 없는 자료에 대해 충분히 고지하고 인터넷의 개인적 사용이 허용되는 조건에 대해 명확히 제시하여야 한다.

③근로자는 인터넷의 오용을 감시하고 특정한 사이트를 차단하는 시스템에 대해 고지받아야 한다. 감시가 개인이나 회사의 영역과 관련이 있는지, 사용자가 특정한 환경에서 방문한 사이트를 보고, 기록하는지 등 감시의 범위가 정해져야 한다.

④위반사실의 조사와 정책수행과정에서의 근로자 대표가 참여하여야 한다.

**기타 컴퓨터 감시**

근로자의 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 근로자 컴퓨터의 내용 중에서 근로자의 업무와 관련된 부분에 대해서 분리하여 당사자의 사전동의를 얻어 근로자의 컴퓨터 내용을 열람할 수 있다.

**위치추적 또는 생체정보를 이용한 감시**

어떠한 방법으로도 개별 근로자의 위치가 파악되는 장치나 기구 등의 이용은

허용되지 않는다. 다만, 위험방지를 위하여 필요한 경우로서 다른 방법이 없는 경우에는 당사자의 동의를 얻어 위치추적을 할 수 있다. 생체정보를 이용한 감시도 위험방지를 위하여 필요한 경우로서 다른 방법이 없는 경우에 당사자의 동의를 얻어서만 허용된다. 어떠한 경우에도 근로자에 대한 유전자 검사 기타 생체정보를 이용한 검사는 허용되지 않는다.

**스마트카드 또는 ID카드**

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

### (2) 근로자 개인정보 보호

가) 일반원칙

사용자가 근로자를 채용할 경우, 취업 중인 경우 또는 합법적인 전자 노동감시에 의하는 경우에 개인정보보호 원칙이 준수되어야 한다. 그 내용은 주로 ILO의 행동강령, OECD의 가이드라인 및 EU지침을 통해서 살펴볼 수 있다. 즉, 개인정보 수집시 당사자의 동의, 개인정보 수집시 목적의 특정, 특정 목적 외 사용금지, 유통의 금지, 가공의 금지, 개인정보의 제3자에 대한 제공의 금지, 개인정보주체의 개인정보에 대한 열람, 정정청구권과 삭제권, 개인정보 수집에 대한 거부권과 이로 인한 불이익 취급 금지, 퇴직 시 개인정보에 대하여 문서보존연한에 개인정보의 최소화 관「 」 등이 그것이다.

먼저, ILO의 「 」 근로자 개인정보보호에 관한 행동강령 에 의한 "개인정보보호의 일반원칙"은 다음과 같다.[41]

41) ILO, 근로자의 개인정보보호에 관한 행동강령 (1996) 참조.

①개인정보는 반드시 적법하고 공정하게 그리고 오직 근로자의 고용과 직접 관련한 이유로만 처리되어야 한다.

②개인정보는 원칙적으로 반드시 수집할 당시의 원래 목적과 동일한 목적으로만 사용되어야 한다.

③만일 개인정보가 처음 수집될 당시의 목적과 다른 목적으로 처리되는 경우, 사용자는 반드시 원래의 목적과 모순된 목적으로 사용되지 않을 것임을 보장해야 하며, 상황 변화로 인해 발생할 수 있는 오해를 방지하는 데 필요한 대책을 반드시 수립해야 한다.

④자동정보시스템의 보안이나 적절한 운영을 보장하기 위해 기술적이거나 관리적인 차원의 대책을 수립할 때 수집된 개인정보는 근로자의 행동을 통제하는 데에 사용될 수 없다.

⑤어떤 근로자에 대한 결정이 그 근로자에 대한 자동처리된 개인정보에만 의존해서 이루어지면 안 된다.

⑥전자감시로 수집된 개인정보가 직무수행평가의 유일한 요소가 되어서는 안 된다.

⑦사용자는 수집된 개인정보의 종류와 양을 가능한 한 줄이기 위하여 그리고 근로자의 프라이버시권을 보호하는 방법을 개선하기 위하여 자신의 정보처리업무에 대하여 정기적인 평가를 행하여야 한다.

⑧근로자와 그 대표는 모든 정보수집 과정, 그 과정을 제어하는 규칙 그리고 자신의 권리에 대해 통지 받아야 한다.

⑨개인정보를 처리하는 사람은 정보수집과 자신의 역할을 이해하기 위해 정기적으로 훈련받아야 한다.

⑩개인정보의 처리는 고용이나 취업에서 불법적인 차별효과를 주어서는 안 된다.

⑪사용자, 근로자와 그 대표는 개인정보를 보호해야 하고 근로자의 프라이버시권에 대한 정책을 개발하도록 협력해야 한다.

⑫사용자, 근로자대표, 고용알선기관, 근로 등 개인정보에 접근할 수 있는 모든 사람은 자신의 의무이행과 비밀유지의 의무를 지켜야 한다.

⑬근로자는 프라이버시권을 포기할 수 없다.

또, OECD는 다음과 같은 프라이버시 보호와 개인정보의 국제적 유통에 관한 가이드라인을 마련하고 있다.[42] 이 지침은 각 국의 프라이버시 입법과 사적 분야의 프라이버시 규약에 반영되었다.

①수집제한의 원칙(Collection Limitation Principle) : 개인정보의 수집은 원칙적으로 제한되어야 하며, 개인정보를 수집할 때는 적법하고 공정한 수단에 의해야 하며 적절한 상황에서 정보주체에게 알리거나 동의를 구해야 한다.

②정보정확성의 원칙(Data Quality Principle) : 개인정보는 사용 목적에 부합해야 하고, 사용 목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태로 유지되어야 한다.

③목적특정화의 원칙(Purpose Specification Principle) : 개인정보를 수집할 때는 그 수집 목적이 특정되어 제시되어야 하고 이후 이를 사용할 때는 애초 목적과 모순되지 않아야 하며 사용 목적이 변하는 각각의 경우에 다시 명시되어야 한다.

④사용제한의 원칙(Use Limitation Principle) : 개인정보는 정보주체의 동의가 있거나 법률 규정에 의하지 않고는 수집 당시 특정된 목적 이외의 용도로 공개되거나 사용되어서는 안 된다.

⑤보안확보의 원칙(Security Safeguards Principle) : 개인정보의 유출, 권한 이외의 접근·파괴·사용·수정, 누출 위험에 대비하여 합리적인 보안 장치를 마련해야 한다.

⑥공개의 원칙(Openness Principle) : 개인정보의 작성, 사용 및 정책에 관해서는 일반적인 공개정책을 취하여야 한다. 개인정보의 존재와 특성, 주요 사용 목적과 함께 정보 관리자의 신원과 주소를 쉽게 알 수 있는 수단이 마련되어야 한다.

⑦개인참여의 원칙(Individual Participation Principle) : 정보주체인 개인은 정보관리자에게 자신과 관련된 정보가 있는지 없는지 존재를 확인하고, 합리적인 시간 안에 과도하지 않은 비용과 합리적인 방식, 그리고 쉽게 알아

42) OECD, 프라이버시 보호와 개인정보의 국제적 유통에 관한 가이드라인 (1980).

볼 수 있는 형태로 자기 정보를 열람할 수 있어야 하며, 자신의 정보에 대해 이의를 제기하고 삭제·정정·보완·수정을 청구할 수 있어야 한다.

⑧책임의 원칙(Accountability Principle) : 정보 관리자는 위의 원칙들이 지켜지도록 필요한 제반조치를 취할 책임을 진다.

또, EU 지침[43]에서 규정하고 있는 개인정보보호지침은 다음과 같다.

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

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

③근로자의 개인정보는 수집의 목적에 비추어 적절한 범위 내에서 수집되어야 하며, 과다하게 수집되어서는 안 된다.

④근로자의 개인정보는 정확하여야 하며, 근로자는 개인정보의 오류를 수정할 권리가 있다.

⑤근로자의 개인정보는 안전하게 보관되어야 한다.

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

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

나) 개인정보의 수집

「 」

ILO의 행동강령 은 근로자 개인정보 수집에 있어서 다음과 같은 원칙을 규정하고 있다(행동강령 6).

「 」

43) EU, 개인정보의 처리와 자유로운 유통에 관한 개인정보보호지침 (Directive 95/46/EC, 1995)

①원칙적으로 모든 정보는 반드시 근로자 개인에게서 획득되어야 한다.

②만약 개인정보를 제3자로부터 획득해야할 필요가 있을 경우, 근로자는 반드시 사전에 이를 통보 받아야 하고 이에 대한 명백한 동의 의사를 전달할 수 있어야 한다. 사업자는 반드시 처리 목적, 사업자가 사용하려는 출처와 수단 뿐 아니라 수집 정보의 유형 그리고 만약에 동의 거부가 있다면 그 결과를 명시해야 한다.

③만약 어떤 근로자가 사업자나 다른 어떤 사람 혹은 조직에게 자신의 정보를 수집하거나 노출시킬 권한을 위임하는 계약서에 대한 서명을 요구받을 때에는, 계약서가 평이한 용어로 작성되어야 하고 구체적이어야 하며, 단체나 기관이 명시되어야 하고, 문제의 신상정보가 드러나 있어야 하며, 개인정보가 어떤 목적으로 수집되는지와 계약서의 유효 기간이 명시되어 있어야 한다.

④사업자가 근로자의 개인정보 사용에 대한 동의를 얻었을 경우, 사업자는 정보를 수집하거나 조사하는 사람과 기관이 언제나 조사 목적을 염두에 두고 그 재현에서 실수나 오해가 없도록 보장해야 한다.

⑤사업자는 근로자의 다음 정보를 수집할 수 없다 : 성생활, 정치적인, 종교적인 또는 그 외의 믿음·신앙, 전과. 사업자는 이 정보들을 고용 결정에 직접 관련이 있고 적법한 경우에 한해서만 수집할 수 있다.

⑥사업자는 법이나 단체협약에 의하여 강제되거나 허락된 경우가 아니면 특정 노동단체에서의 지위나 근로자 조합 활동에 관한 정보를 수집할 수 없다.

⑦개인의료정보는 적법하고 의료상의 기밀과 작업현장의 건강과 안전에 대한 일반원칙에 따라 △근로자가 특정 직업에 맞는지 결정하기 위해서 △작업현장의 건강과 안전을 위한 요구조건을 만족시키기 위해서 △사회보장혜택을 위한 자격을 심사하고 그 혜택 수락여부를 결정하기 위해서 필요한 경우가 아니면 수집될 수 없다.

⑧근로자가 이 강령에 어긋나는 요구를 받았을 때 근로자가 부정확하거나 불완전한 답을 한 경우, 근로자는 고용 관계가 종료되거나 다른 규율상의 처분을 받지 않아야 한다.

⑨개인정보 요청에 대한 근로자의 잘못된 이해로 제공된 개인정보 혹은 관

계없거나 범위를 넘어서는 개인정보는 처리될 수 없다.

⑩거짓말 탐지기, 사실 증명 장비와 기타 유사한 검사 절차는 사용될 수 없다.

⑪인성테스트 또는 유사한 검사절차는 이 강령 규정에 따라야 하며, 근로자는 검사를 거부할 수 있음을 명시해야 한다.

⑫유전자검사는 금지되거나 법적으로 명확히 인정된 경우에만 한정되어야 한다.

⑬약물검사는 국가의 제정법과 관습법 또는 국제법 표준에 따라 이루어져야 한다. ILO는 사업장에서의 알코올과 약물 관련 사안의 처리에 대한 행동 강령과 "사업장에서의 약물과 알코올 검사에 대한 규범"을 가지고 있다.

⑭근로자를 감시할 때에는 사전에 감시의 목적과 예정시간, 사용되는 방법과 기술, 수집되는 정보를 알려야만 한다. 또한 사업자는 근로자의 프라이버시 침해를 최소화해야만 한다. 비밀스런 감시는 국가의 법에 의하거나 범죄행위 또는 그에 준하는 심각한 행위가 의심될 때에만 허용된다. 지속적인 감시는 건강과 안전 또는 재산의 보호를 위해 필요할 때에만 허락된다.

다) 개인정보의 보관

ILO의 「 」 행동강령 은 근로자 개인정보의 보관에 있어서 다음과 같은 원칙을 규정하고 있다(행동강령 8).

①개인정보의 보관은 개인정보 수집에 관한 원칙에 따른 방법으로 수집된 개인정보에 대해서만 보관을 허용해야 한다.

②비밀이 보장되어야 하는 개인 의료정보는 의료 기밀 규정에 따라 인사담당자에게만 보관되어야 하며 다른 모든 개인정보와 분리하여 다루어야 한다.

③사용자는 전반적인 정보와 정기적으로 검토되는 개별 근로자의 개인정보 항목과 그 처리에 대한 정보를 제공해야 한다.

④사용자는 저장된 개인정보가 정확하고 최신의 것이며 완전하다는 것을 정기적으로 보장해야 한다.

⑤개인정보를 수집할 당시의 특정한 필요성이 계속적으로 존재하는 동안에만 그 정보를 보관할 수 있다. 단, 다음의 경우는 예외로 한다.

(a) 근로자가 특정 기간 동안 구직자 명단에 올라 있기를 원할 때

(b) 국가의 법으로 개인정보가 요구될 때

(c) 현재 존재하거나 과거에 존재했던 고용 관계와 관련한 법적 증명 절차를 위하여 사용자 또는 근로자가 개인정보를 요구할 때

⑥개인정보를 다음과 같은 방법으로 보관하고 작성하여야 한다.

(a) 근로자가 이해할 수 있어야 한다.

(b) 근로자의 특성을 거론하며 그 근로자에 대한 차별을 유발해서는 안된다.

라) 개인정보의 처리

개인정보의 처리는 다음의 원칙에 따라 이루어져야 한다.

①수집시의 동의의 원칙

②목적의 특정, 명시의 원칙

③직무수행과 관련된 정보의 최소수집의 원칙.

특히 이 경우 근로자로부터 취득할 수 있는 개인정보의 범위는 당해 고용계약 하에서 근로자의 직무의 수행에 필요한 정보로 제한되어야 한다. 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 된다. 인종에 관한 정보도 민감한 정보로서 수집되어서는 안된다. 질병에 관한 정보는 당해업무 수행과 관련이 있는 범위 내에서만 수집되어야 하며, 이용되어야 한다. 업무와 관련이 없는 질병에 관

한 정보를 취득하기 위한 신체검사도 허용되지 않는다. 질병에 관한 정보에 대해서는 근로자의 열람권과 항변권, 정정권이 인정되어야 한다. 그리고 근로자의 개인정보는 항상 최신성을 유지하여 정정되어야 하며, 내부적으로도 목적 외로 이용되지 않도록 하고, 해당업무를 담당하는 자 외에는 개인정보가 공개되거나 제공되어서는 안 된다. 이때 사용자는 근로자의 개인정보에 접근할 수 있는 업무담당자를 미리 지정해서 통보해야 한다. 근로자의 개인정보에 대한 보안조치는 적절하게 취해져야 한다.

④의료정보의 특별한 보호 : 특히 질병에 관한 정보에 대해서는 근로자의 열람권과 항변권, 정정권이 인정되어야 한다.

⑤정확성, 최신성 유지 : 그리고 근로자의 개인정보는 항상 최신성을 유지하여 정정되어야 한다.

⑥목적외 사용의 금지와 제3자 제공의 금지 : 내부적으로도 목적외로 이용되지 않도록 한다. 어떤 근로자에 대한 결정이 그 근로자에 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.

⑦보안 : 보안이 유지되어야 하며, 안전하게 보관되고, 해당업무를 담당하는 자 외에는 개인정보가 공개되거나 제공되어서는 안될 것이다.

⑧정보의 통합 : 개인정보의 통합은 원칙적으로 금지되며, 최초에 수집한 목적을 넘는 개인정보의 통합은 허용되어서는 안될 것이다.

⑨접근 : 이때 사용자는 근로자의 개인정보에 접근할 수 있는 업무담당자를 미리 지정해서 통보해야 할 것이다.

마) 개인정보의 보안

「 」

ILO의 행동강령 은 근로자 개인정보의 보안과 관련하여, "사용자는 정보의 유실, 정보에 대한 권한 없는 접근과 그 사용, 수정, 유포를 막기 위하여 상황에 따른 적절한 보안 수단을 사용하고 개인정보를 보호할 의무가 있다"(행동강령

7.1)고 규정하고 있다.

바) 개인정보의 교환

ILO의「 행동강령 은 근로자 개인정보의 교환에 있어서 다음과 같은 원칙을 규정하고 있다(행동강령 10).

①개인정보는 다음의 경우를 제외하고 근로자의 명시적 동의 없이 제3자와 교환될 수 없다.

(a) 생명과 건강에 대한 중대하고 절박한 위협을 막기 위해 필요할 때

(b) 법률로 요구되었거나 승인되었을 때

(c) 고용 관계의 관리를 위해 필요할 때

(d) 형법집행을 위해 요구될 때

②근로자의 개인정보는 근로자의 인지와 명시적 동의 없이 상업적 · 영리적 목적으로 교환될 수 없다.

③사용자는 근로자의 개인정보를 교환하는 자에게 그 개인정보는 제공한 목적에 한해서만 사용되어야 함을 고지해야 하며, 이를 이행할 것임을 확인받아야 한다.

④개인정보의 내부적 상호교환은 근로자가 명백히 인지한 사람들에 한해야 한다.

⑤개인정보의 내부이용은 그 개인정보가 특정 작업의 수행에 필요한 경우에 한하여 승인 받은 특정 이용자에게만 허용된다.

⑥근로자의 개인정보를 포함한 자료들의 취합은 원칙적으로 금지된다.

⑦의료기록의 경우 사용자는 특정한 고용의 결정에 관련한 판정만을 제공받을 수 있다. 그 판정은 어떠한 의료정보도 포함할 수 없다. 판정은 제안된 작업에 적합한지를 나타내거나, 일정 종류의 직업, 일시적 혹은 영구적으로 의학적으로 금해야 하는 근무환경을 적시하는 내용이어야 한다.

⑧근로자의 대표와 개인정보를 교환하는 것은 국가의 법률이나 관습법에

따른 단체협약에 따라 이루어져야 한다. 또한, 근로자 대표의 특정한 업무 수행에 필요한 개인정보에만 한정되어야 한다.

사) 자동처리장치를 통한 평가정보의 수집 및 수집된 정보에 의한 평가

자동처리장치를 통하여 근로자의 평가정보를 수집하는 것은 (ⅰ)당해 근로자를 식별할 수 없도록 처리가 되거나, (ii)당해 근로자를 식별할 수 있는 정보로 수집되는 경우에는 주 단위나 월 단위로 통합된 결과로 처리하여 수집되어야 하며, 이와 같이 수집된 정보가 근로자에 대한 평가의 유일한 근거나 주요한 근거가 되어서는 안 된다.

### (3) 개인정보보호와 사업장감시규제에 있어서 개인과 집단의 권리

가) 개인의 권리

ILO의 「행동강령」은 개인정보보호와 사업장감시규제에 있어서 개인의 권리를 다음과 같이 규정하고 있다(행동강령 11).

①근로자는 확보된 자신의 개인정보와 그 개인정보의 처리과정을 정기적으로 고지받을 권리를 가진다.

②개인정보가 자동화된 시스템으로 처리되었거나 근로자별로 특정한 수작업 파일에 보관되었거나 기타 어떤 형태로 근로자의 개인 정보가 보관되었든지 간에 근로자는 자신의 모든 개인정보에 접근할 수 있다.

③근로자가 자신의 개인정보의 처리과정에 대하여 알 권리는 그 근로자의 개인정보를 포함하는 모든 형태의 기록을 검토하고 사본을 소지할 수 있는 권리를 포함한다.

④근로자는 근무시간 중 자신의 개인정보에 대해 접근할 수 있는 권리를

가진다. 만약 근무시간에 이루어지지 못할 때에는 근로자와 사용자의 편의를 고려하여 실시되어야 한다.

⑤근로자는 접근권의 행사를 보조할 근로자 대표나 보조자를 지명할 권리가 있다.

⑥근로자는 자신이 선택한 의료전문가를 통해 자신의 의료 정보에 접근할 권리를 가진다.

⑦사용자는 근로자가 자신의 기록에 접근하거나 복사하는 것에 비용 부담을 지울 수 없다.

⑧사용자는 안전 점검할 때 점검에 현저한 위해가 예상되는 경우에 한하여 점검이 끝날 때까지 근로자가 자신의 개인정보에 접근하는 것을 거부할 수 있다. 그러나 근로자가 자신의 모든 개인정보에 접근하기 전에는 인사에 관한 어떠한 결정도 행할 수 없다.

⑨근로자는 잘못되고 불완전한 개인정보 및 이 강령의 규정에 따르지 않는 개인정보에 대해 삭제 혹은 수정을 요구할 권리를 갖는다.

⑩개인정보를 삭제 혹은 수정할 때, 사용자는 앞서 부정확하고 불완전한 개인정보를 제공받았던 모든 사람에게 삭제 혹은 수정한 사실을 알려야만 한다. 단, 삭제 혹은 수정의 통지가 필요하지 않다는 근로자의 동의가 있을 때에는 알리지 않을 수도 있다.

⑪사용자가 개인정보의 수정을 거절할 때, 근로자는 그 개인정보에 동의하지 않는다는 진술 혹은 그 근거 기록을 제출할 권리를 가진다. 이후에 개인정보가 사용될 때에는 언제나 이 개인정보가 논란이 있음을 알리는 정보와 해당 근로자의 진술이 포함되어야 한다.

⑫사법 기록의 경우 삭제나 수정이 불가능할 때에는 근로자는 자신의 관점을 서술한 진술을 첨부할 권리를 가진다. 이 진술은 포함하지 않아도 된다는 근로자의 동의가 없는 한 모든 개인정보 교환에 포함되어야 한다.

⑬법률, 규칙 조례, 단체협약, 업무규정 혹은 정책에 있어서, 사용자가 법 절차를 이행하지 않을 때 근로자가 배상받을 수 있는 방법을 적시해야 한다. 근로자가 제출하는 어떠한 진정도 받아들이고 답변하는 절차를 마련해야 한다. 진정 절차는 근로자가 이용하기 쉽고 간단해야 한다.

나) 집단적 권리

ILO의「 행동강령」은 개인정보보호와 사업장감시규제에 있어서 개인의 권리를 다음과 같이 규정하고 있다(행동강령 12).

> ①근로자의 개인정보 처리에 관한 모든 협상은 자신에 대한 어떠한 개인정보가 어떠한 조건하에서 어떤 목적으로 사용되어야 하는지 알고 결정할 수 있는 개별 근로자의 권리를 보장하는 것을 목적으로 하는 이 행동 강령의 원칙에 따라야 한다.
>
> ②근로자의 대표는, a)근로자의 개인정보를 처리하는 자동 시스템의 채택 및 변경에 관하여, b)사업장 안의 전자 근로자 감시 시스템의 채택에 앞서, c)근로자의 개인정보에 대한 설문조사 및 검사를 해석하고 관리하는 방법과 내용, 목적에 대하여 통지받고 조언할 수 있다.

### (4) 권리구제 및 실효성 확보방안

전자 노동감시를 규제하는 입법에는 전자 노동감시에 의하여 근로자의 인권이 침해된 경우에는 사용자 및 관계자에 대한 처벌규정을 두고, 피해를 입은 근로자의 권리구제수단이 마련되어야 한다. 또 일반법원에 의한 권리구제방법 이외에 노동위원회 또는 예를 들어 프라이버시위원회 또는 반감시위원회에 의한 권리구제방법을 규정한다.

## 4) 단체협약을 통한 전자 노동감시 규제방안

전자 노동감시의 도입과 이용은 그것이 근로자의 존엄과 가치 및 프라이버시권을 침해하는 경우에 그리고 그것이 사용자의 경영상 이익과 비교형량 하더라도

수용될 수 없는 경우에는 그 자체가 사용자의 불법행위를 구성하여 허용되지 않는다. 따라서 이러한 경우에는 노동조합이 동의하더라도 유효하지 않다. 즉, 근로자의 인권 또는 인격적 이익에 대한 중대한 침해를 초래하는 전자 노동감시 장비의 도입에 관한 사항은 단체교섭 대상문제에 있어서 위법교섭사항이 된다.

그러나 일반적으로 사용자는 경영상 또는 노동통제의 필요에 의하여 전자 노동감시 장비를 도입 또는 설치하고자 하는 경우에 조합원 즉 근로자의 근로조건 유지개선 및 지위향상을 위하여 조직된 단체인 노동조합은 그러한 문제에 대하여 사용자에게 교섭을 요구할 권리가 있다. 현실적으로도 전자 노동감시에 대해서는 개별 근로자의 동의를 요건으로 하지만 약자적 위치에 있는 개별 근로자의 자유의사의 진정성에 한계가 있기 때문에 노동조합을 통해서 진정한 자기결정권을 확보할 필요가 있다. 따라서 전자 노동감시의 규제를 위해서는 입법적 조치와 함께 노동조합과 사용자의 단체협약에 의한 제도적 장치를 활용할 필요가 있다.

단체협약에 의하여 전자 노동감시에 의한 규제를 하는 경우에 다음과 같은 내용을 담을 수 있다.[44]

### (1) 인권보호에 관한 규정

단체협약에 근로자의 인권보호에 관한 총칙 규정을 둘 필요가 있다. 그 내용은 다음과 같다. ①회사는 회사 내에서 조합원의 존엄과 가치를 침해하거나 훼손해서는 안 된다. ②회사는 조합이 조합원에 대한 인권침해 사항의 조사와 시정을 요구할 경우 조사에 응해야 하며 인권침해행위의 중지, 원상회복 등 필요한 조치를 취하고 재발방지 조치를 마련해야 한다. 다만, 조합 또는 조합원이 원할 경우 비공개로 조사를 진행해야 한다. ③회사는 조합의 요구로 조사한 인권침해사항에 대해서는 조사결과와 처리결과를 조합에 통보하여야 한다.

---

44) 민주노총, 2002 인권단협안 자료 참조. 여기서는 자료를 부분적으로 발췌하여 소개한다.

### (2) 개인정보의 보호에 관한 규정

회사는 어떤 기관보다도 근로자들의 개인정보를 가장 많이 수집·관리(주민등록정보, 가족, 병역, 학력, 건강, 소득, 업무 관련 기록 등)하고 있음에도 불구하고, 근로기준법상 블랙리스트 금지(제39조) 규정 외에 별다른 법규나 규정이 없다. 그리하여 그 동안 회사의 고의·과실에 의하여 개인정보가 유출되거나 회사가 이를 악용하는 경우에도 이를 구체적으로 규제할 방법이 없었고, 피해를 받은 근로자가 개별적으로 대응하는 방법밖에는 없었다. 따라서 단체협약은 개인정보의 수집, 보관 및 이용 등에 관하여 상세한 규정을 둘 필요가 있다.

가) 원칙

먼저 "회사는 업무상 취득한 조합원의 성명, 나이, 생년월일, 근속연수, 금융거래, 전 직장, 가족현황, 병역, 정당가입여부, 결혼내역, 성적지향 등 일체의 개인정보를 보호해야 한다"는 원칙을 규정하여야 한다.

나) 개인정보의 수집

근로자의 개인정보 수집에 관해서는 "①회사는 근로자의 개인정보의 수집에 있어서 고용과 직접적으로 관련된 것만을 대상으로 해야 하며 그 목적과 내용, 수집방법, 담당부서와 담당자에 대해 조합과 사전 합의해야 한다. ②회사는 개인정보를 수집할 경우 조합원 본인으로부터 직접 취득해야 하며 개인정보를 제3자로부터 획득해야 할 필요가 있을 경우라 하더라도 해당조합원의 명시적인 동의 없이 취득해서는 아니 된다. ③회사는 사상, 신념, 종교 등 조합원의 권리, 이익, 사생활을  침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. ④회사는 조합원들의 조합활동이나 사내외 단체 활동 및 업무외 사적인 활동에 대한 정보를 수집해서는 안 된다.  등의 규정을 둔다.

사용자가 개인정보를 수집하는 경우에 "조합원은 고용과 직접적으로 관련되

지 않은 사생활을 침해할 수 있는 개인정보에 대해 거부할 권리가 있으며, 회사는 이를 이유로 불이익 처우를 해서는 아니 된다"는 개인정보제공 거부권을 명시하여야 한다.

다) 개인정보의 관리

사용자가 개인정보를 관리함에 있어서 "①회사는 조합원의 개인정보를 관리함에 있어 조합과 사전에 합의하여야 하며 조합원들에게 보관기간과 방법, 처리 및 폐기 방법, 담당부서와 담당자 등을 고지하여야 한다. ②회사는 조합원의 개인정보를 해당 조합원의 동의 없이 담당부서와 담당자를 제외한 회사내외의 제3자에게 제공해서는 아니 된다. ③회사는 조합 또는 해당 조합원이 개인정보의 열람 및 사본복사를 요구할 경우 이에 응해야 하며 비용을 부담한다. ④회사는 개인정보 관리를 위해 별도의 규정을 마련하고 그 내용에 대해 조합과 사전협의(합의)하여야 한다."는 규정을 둔다.

사용자가 개인정보를 수정 또는 폐기하는 경우에도, "①회사는 조합 또는 조합원이 조합과 합의 없이 수집·관리되고 있는 개인정보, 사실과 다른 개인정보, 고용과 직접적으로 관련되지 않은 사생활을 침해할 수 있는 개인정보의 경우에 대해 개인정보의 수정, 폐기를 요구할 경우 이에 응해야 하며 그 결과를 통보해주어야 한다. ②회사는 보관기간이 종료되었을 때는 폐기해야 하며, 해당 조합원에게 통보해주어야 한다. 단, 조합 또는 해당 조합원이 개인정보의 유지를 요구한 경우, 조합과 해당 조합원이 개인정보 유지에 명시적으로 동의하는 경우, 법률에 의해 개인정보의 유지가 요구되는 기간의 경우는 그렇지 아니한다"는 규정을 둔다.

### (3) 전자 노동감시에 관한 규정

가) 원칙

"회사는 조합 또는 조합원을 감시할 목적으로 컴퓨터, 전화, 비디오카메라, 지

문, 홍체, 정맥 등 생체인식기기 및 기타 정보통신·음향·(감지)·영상기술을 이용하여 조합원의 이동, 작업과정을 기록·저장할 설비 및 소프트웨어(이하 "감시장비")를 설치하여서는 아니 된다. 다만, 노동안전, 도난 등 위험·사고방지를 위해 장비를 설치할 경우에는 조합과 사전에 합의하여야 하며 사용 중에는 조합원에게 인지할 수 있는 조치를 취해야 한다."는 규정을 두고, 합의하여야 할 내용으로 "설치목적과 사용기간, 설치방법·장소와 기록내용, 감시장비의 종류와 기술내용, 담당부서와 담당자, 근로자의 접근권과 사용 중지권의 인정" 등을 규정하여야 한다.

또 사생활 보호를 위하여 "회사는 화장실, 탈의실, 세면실, 휴게실, 기숙사 등 사생활을 침해할 수 있는 장소에 감시장비를 설치해 조합원의 사생활을 침해해서는 아니 된다"는 것을 명시한다.

나) 감시장비의 철거

회사는 조합과 사전합의 없이 설치한 감시장비, 설치목적과 사용기간이 만료된 감시장비는 즉시 철거해야 하고 그 결과를 조합에 통보해야 하고, 조합은 이에 대한 실사확인 절차를 하여야 한다.

다) 감시장비에 의한 기록물 관리 및 이용

감시장비에 의하여 수집되거나 만들어진 기록물에 대하여 "①회사는 감시장비에 의한 기록물(이하 '기록물')에 대해서는 보관기간, 처리 및 접근방법, 담당부서와 담당자에 대해 사전에 조합과 합의해야 한다. ②회사는 기록물 관리를 위해 별도의 규정을 마련하고 그 내용에 대해 조합과 사전 협의하여야 한다. ③회사는 기록물을 담당부서와 담당자 외에는 어느 누구에게도 제공해서는 아니 된다. ④회사는 감시장비에 의해 기록된 내용을 조합 또는 해당조합원이 열람을 요구할 경우 이에 따라야 한다."는 규정을 둠으로써 그 악용을 막도록 한다.

또 기록물 수정과 폐기에 대해서도 "①회사는 조합 또는 조합원이 조합과 합

의 없이 수집된 기록물, 사생활을 침해할 수 있는 기록물, 조작되었거나 사실과 다른 기록물에 대해 개인정보의 수정, 폐기를 요구할 경우 이에 응해야 하며 그 결과를 통보해주어야 한다. ②회사는 기록물이 그 목적과 보관기간을 마쳤을 경우에는 복구할 수 없게 폐기하고 이를 조합에 통보하여야 한다. 단, 조합 또는 해당 조합원이 자료의 보관·유지를 요구할 경우, 조합 또는 해당 조합원의 명시적 동의가 있을 경우, 현재 법적 소송의 증거물로 요구되고 있는 경우는 제외한다."는 규정을 둔다.

감시장비에 의한 기록물의 이용과 관련하여 "회사는 감시장비에 의한 기록물의 내용을 임금산정과 인사고과에 반영해서는 아니 된다"는 규정도 필요하다.

# 7장. 결론

## 1) 감시기술에 대한 사회적 개입의 필요성

전자감시 기술의 확장은 이제 이 문제에 대한 사회적 개입의 필요성을 그 어느 때 보다 절실히 요구하고 있다. 전자감시의 시스템화로 감시의 문제는 일터와 작업장 수준을 넘어 인간 활동의 전 영역에 걸쳐 심각한 영향을 미치게 되었기 때문이다. 이제 전자감시 문제의 심각성을 인식하고, 이에 대한 사회적 대응 방안을 모색하기 위한 노력이 본격적으로 이루어져야 할 때인 것이다.

전자감시의 문제는 이미 사회의 다양한 영역에서 심각한 문제로 등장하고 있다. 주민정보, 교육정보, 의료정보, 생체정보 등 정보의 수집, 가공, 활용과 관련된 문제들이 심각한 '사회적 각축'(social contention)의 중심 영역에 진입하였다. 생산현장 뿐 아니라 소비를 포함한 사회적 활동의 제반 영역에서 인간의 활동에 대한 정보가 데이터베이스화되고 전자정보 시스템에 의해 처리되는 상황에서 시스템에 자체에 대한 민주적 통제의 문제는 대단히 중요한 사회적, 인권적 이슈가 될 것이 분명하다. 특히 작업장에서 이루어지는 전자감시의 문제에 대한 올바른 인권적 대응은 정보사회의 성격을 가늠하는 핵심 지표가 되고 있다.

## 2) 국가적 수준의 대응

감시사회에 대한 효과적 대응을 위해서는 기술의 문제에 대한 국가적 차원의 새로운 시각이 무엇보다 절실히 요구되고 있다. 이는 정보기술이 인간의 존엄성, 프라이버시, 건강 등에 미치는 광범위한 차원의 영향에 대하여 국가 정책 차원에

서 새로운 접근이 요구되는 것을 의미한다. 정보기술에 대한 국가의 정책은 경제적 부가가치와 통치적 효율성의 관점이 압도적인 비중을 차지해 왔다. 그러나 통치와 효율성 제고라는 관점의 이면에는 정보감시기술로 인한 인권과 프라이버시 침해의 문제가 도사리고 있음을 간과해서는 안 될 것이다. 인권과 프라이버시 보호를 위한 국가의 정책적 대응 노력이 제대로 이루어지지 않는 상황에서 정보감시기술의 사회적 오·남용 가능성은 막기 어려울 것으로 판단된다.

이러한 상황에서 국가는 사업장 감시를 비롯하여 감시기술의 사회적 부작용 문제를 적극적으로 논의할 수 있는 공론의 장을 제공하고, 이해 당사자들의 참여를 통해 적절한 사회적 합의와 기준을 설정하기 위한 정책적 노력을 기울여야 할 것으로 보인다. 과거의 경험으로 볼 때 국가는 전자감시 기술의 사회적 문제나 부작용에 대해 거의 관심을 기울이지 않았으며, 도리어 이러한 문제들이 제기되는 것에 대해 기본적으로 부정적인 입장을 취해 왔다.

정보기술이 한국경제에서 차지하는 비중과 중요성으로 인해 통치와 산업적 관점에서 관련 산업과 기술의 발전을 육성, 지원하는 것만이 국가의 거의 유일한 관심인 상황에서 정보기술에 대한 민주적 통제는 산업 발전에 부정적 영향을 미치는 것으로 판단될 가능성이 높다. 시민의 일상생활에 중대한 영향을 미치는 기술체계의 도입과 확산의 영향에 대해 사회적 평가가 제대로 이루어지지 않는 상태에서 생산 체제의 효율성과 경쟁력의 기준에 따라 작업장에 투입되는 감시기술은 인간의 자유와 인권을 침해하는 커다란 문제를 드러낼 가능성이 높다.

정보기술에 대한 민주적 통제에 대해 국가가 소극적인 또 하나의 본질적 이유는 국가 스스로 권력의 유지 뿐 아니라 통치 수단으로 체계적인 정보 수집을 요구하고 있기 때문이다. 국가권력에 의해 이루어지는 정보수집, 가공, 활용 행위에 대한 시민적 개입과 민주적 통제의 가능성이 극히 낮은 상황에서 국가가 감시기술에 대한 민주적 통제에 적극적으로 나서는 데에는 커다란 한계가 있었던 것이 사실이다.

그러나 전자감시 기술의 시스템화와 인권 침해 가능성이 점점 커지고 있는 상황에서 민주주의 국가가 이 문제를 간과할 수는 없게 되었다. 전자감시 기술이 작업장 뿐 아니라 생활세계의 전 영역에 걸쳐 그 영향을 확대해 나아감에 따라

감시시스템의 노·남용으로 인한 인권과 프라이버시 침해 문제를 적극적으로 제기하고, 이에 대한 민주적 통제와 법제도적 규제 방향을 본격적으로 모색하지 않는다면 정보기술사회에서 감시 시스템의 통제로부터 인간의 가치와 존엄성을 지키는 것은 더욱 어려워질 것이기 때문이다. 다행히 전자감시의 효과와 영향에 대한 국내외의 많은 연구들은 적절한 윤리 및 법제도적 기준의 설정과 절차적 합리성의 제고, 전자감시 및 정보수집 기술의 작업장 도입에 대한 노사의 동의, 평가, 운영의 투명성 제고를 위한 노동자들의 참여가 촉진될 경우 정보기술이 감시기술로 전환되어 노동인권을 침해하는 위험성이 현저히 감소하는 것을 보여주고 있다. 국가적 수준에서 노동인권 보호를 위한 적극적 개입이 중요하고, 시급한 이유는 바로 여기에 있다.

### 3) 작업장 수준의 대응

전자감시 시스템에 대한 효과적인 대응을 위해 가장 중요한 사회적 주체의 하나는 전자감시 체제의 통제로 인해 인격적 자유와 프라이버시, 건강권 등의 피해를 입고 있는 작업장의 노동자들이다. 따라서 사업장 감시에 대한 효과적인 대응 역시 감시체제의 억압으로 인해 유·무형의 고통을 받아 온 노동자들을 중심으로 개인적, 조직적 수준에서 다양한 형태의 문제제기 활동이 조직화 될 필요가 있다.

노조는 전자감시 체제에 대한 문제제기를 조직화 하는 데 있어 중심 역할을 담당해야 한다. 작업장에 도입된 전자감시 기술의 용도와 목적 등에 대하여 명확한 범위가 규정되어야 하며, 기술 도입의 사전 단계부터 노조와의 긴밀한 평가에 기초한 사회적 합의가 도출될 수 있도록 단체협약 체계를 구축하기 위한 노력이 선행되어야 한다. 또한 사업장 감시가 노동자들의 인권, 건강권, 프라이버시 등에 미치는 영향에 대해 노사 공동 조사 등이 이루어질 수 있도록 적극적인 문제 제기가 필요하다.

감시기술이 갖는 이중성, 복합성에 비추어 볼 때 기술의 민주적 활용을 위해

서는 회사와의 단체협약 등을 추진하는 것이 필수적으로 요구되며, 이를 통해 기술의 도입과 활용에 대한 최소한의 민주적, 윤리적 기준을 마련하기 위한 노력이 전개될 필요가 있다. 노조의 경영 참여가 활발하고, 조직적 유대 수준이 높은 국가의 작업장에서 인간 중심의 기술 시스템들이 선진적으로 도입되고 있는 점들을 고려할 때 기술에 대한 노조의 관심 수준을 제고하는 것은 감시기술에 대한 효과적인 사회적 대응의 필수 조건이 될 것으로 판단된다.

전자감시에 대한 사회적 대응은 권력에 대한 민주적 통제의 문제와 불가분의 관련성을 맺고 있다. 사업장 감시의 문제 역시 이러한 문제의식 속에서 바라볼 필요가 있다. 다시 말해 작업장 수준에서 노동자들의 인권과 프라이버시를 보호하기 위한 적절한 수준의 법제도적 개입과 민주적 통제가 이루어지지 않을 경우 전자감시 시스템의 인권침해 가능성은 점점 더 높아질 것이 분명하다.

전자감시 시스템에 대한 민주적 개입을 위해서는 노동자 개인, 노조, 시민단체 등의 적극적인 관심과 개입을 위한 노력 또한 대단히 중요한 의미를 지닌다. 이들 시민사회 조직들은 전자감시로 인해 발생 가능한 사회적 문제들을 적극적으로 이슈화 하는 것은 물론, 인권침해의 피해 당사자들과 함께 정보기술의 인간적 활용을 위한 노력에 적극적으로 나서야 할 것이다.

### 4) 시민사회와 국제적 연대

감시기술에 대한 사회적 관심이 작업장의 차원을 넘어 시민사회와 국제적 연대의 문제로까지 확장되어야 하는 근원적인 이유는 이 기술이 기본적으로 전사회적 차원을 아우르는 '시스템'의 차원으로 확장되었기 때문이다. 과거의 감시기술은 개별 사업장이나 워크스테이션, 혹은 특정한 공간과 시간 영역에 제한적, 국지적으로 적용되었지만, 오늘날의 감시기술은 본질적으로 인간 활동의 전 영역과 차원을 아우르는 전방위 시스템의 개념으로 확장되어 있음을 보여준다.

감시 기술이 이른바 유비쿼터스 시스템으로 나아가는 것은 체계 확장의 필연적 과정으로 볼 수 있다. 인간의 작업이 이루어지고, 행위가 발생하는 사회적 장

은 고정된 작업장의 공간에 국한되지 않는다. 재화와 서비스의 생산과 이윤 추구를 향한 조직의 움직임은 더 시간과 공간의 한계를 넘어선지 오래이다. 감시 기술의 내용을 구성하는 모든 기술적 요소들은 실시간적 네트워크로 연결되어가고 있으며, 감시기술의 체계들은 점과 면을 넘어 공간과 시간의 모든 차원을 아우르는 거대한 기술적 연결망으로 존재하고 있다.

이러한 상황에서 감기기술의 확장은 우리의 일터 뿐 아니라 일상적 시민 생활의 모든 영역들을 포함하며, 그 범위는 본질적으로 세계적이다. 감시기술은 문화적 특성과 정치적 제한에도 불구하고 모든 사회에 적용 가능한 보편적 속성을 지니고 있기 때문에 이 문제에 대한 사회적 대응은 처음부터 국제적 성격을 지닐 수밖에 없다.

전자감시 기술로 인한 노동인권 침해 가능성의 문제는 이미 70년대부터 ILO 등을 중심으로 논의되기 시작하여 인권 침해에 대한 국제적 기준을 마련하는 데 상당한 성과를 거두고 있으며, 개별 국가 차원에서도 정보기술과 인권, 프라이버시 문제를 중심으로 그 남용 가능성을 규제하기 위한 노력이 상당한 부분 활성화되어 있음을 보여준다. 이렇게 볼 때 전자감시기술에 대한 인권적 대응의 문제는 한국사회에 국한된 내용이 아니며, 국제적 차원에서도 연대 가능성을 모색해야 하는 중요한 사안으로 규정될 수 있을 것이다.

국제적 연대와 결합한 시민사회의 활동은 감시기술의 오·남용으로 인한 인권 침해의 문제에 초점을 두고, 이를 방지하기 위한 사회적 공론화, 법제도 및 윤리적 기준 설정, 시민 행동 강령 설정, 윤리적 기준 마련 등에 주력할 필요가 있으며, 이러한 과정들이 효과적으로 조직되기 위해서는 노동 인권조직들과의 협력이 필수적이다. 전자감시 기술에 대한 대응이 기본적으로 국제적 차원의 인권 담론으로 전개될 수밖에 없는 이유는, 정보감시기술의 보편성 때문일 것이다. 전자감시기술은 이윤, 효율성, 통제, 권력 기제 등의 효과적인 작동을 위해 어디에서나 요구되는 보편적 성격의 기술이며, 이러한 기술에 대한 민주적 통제와 개입은 우리 사회에만 국한된 문제가 아니라 정보사회에 진입하고 있는 모든 국가, 조직, 직장 등에서 대처해야 할 문제이기 때문이다.

# < 참고문헌 >

* 외국 문헌


AMA (2001), "Workplace Monitoring & Surveillance - Summary of Key Fidings"

American Management Association (2001), AMA's 2001 Survey Workplace Monitoring and Surveillance: Summary of Key Findings.

American Management Association (2005), AMA's 2005 Electronic Monitoring & Surveillance Survey: Executive Summary.

Beirne, M. and H. Ramsay (eds.) (1992), *Information Technology and Workplace Democracy*, London: Routledge.

Beniger, James (1986). The Control Revolution: *The Technological and Economic Origins of the Information Society*, Cambridge: Harvard Univ. Press.

Bennett, Colin (1992), *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca: Cornell Univ. Press.

Bentham, Jeremy (1843), *Jeremy Bentham: Collected Works*, London.

Blackmore, Michael (2005), "Surveillance in the Workplace - an overview of issues of privacy, monitoring, and ethics".

Bowles, S. and H. Gintis (1987), *Democracy and Capitalism* (차성수・권기돈 역, 『민주주의와 자본주의』), 백산서당.

Callaghan, G. and P. Thompson (2001), "Edwards revisited: technological control and call centers", *Industry and Democracy*, Vol. 22 (1), pp. 13-37.

Cole, Stephen (2005), "Universal Human Rights and Employee Privacy: Questioning Employer Monitoring of Computer Usage", Weckert, John (ed.) (2005), *Electronic Monitoring in the Workplace: Controversies and*

*Solutions*, London: IDEA Group Publishing.

Cripps, Alison (2004), "Workplace Surveillance", Working paper of New South Wales Council for Civil Liberties.

Dichter and Burkhardt (1999), "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communication in the Internet Age"

Dorval, Danielle (2004), "Should Employers Have the Ability to Monitor their Employees Electronically?".

EU(1995), 「개인정보의 처리와 자유로운 유통에 관한 개인정보보호지침」 (Directive 95/46/EC).

EU(2002), 「회사에서의 전자통신 감시에 관한 특별조사위원회 보고서」, 2002.5.29

Flaherty, David (1989), *Protecting Privacy in Surveillance Societies*, Chapel Hill: Univ. of North Carolina Press.

Foucault, Michel (1977), *Discipline and Punish: The Birth of the Prison*, New York: Vintage.

GAO (2002), "Computer-Use Monitoring Practices and Policies of Selected Companies".

Geist, Micahel (2002), "Computer and E-mail Workplace Surveillance in Canada: the Shift frm Reasonable Expectation of Privacy to Reasonable Surveillance", Paper presented to Canadian Juidical Council.

Gurvich et al., "Privacy in the Age of the Internet" (presentation)

Habermas, Jürgen (1986), *The Theory of Communicative Action*, Cambridge: Polity Press.

Hartman, Laura and Gabriella Bucci (1998), "The Economic and Ethical Implications of New Technology on Privacy in the Workplace", *Business and Society Review*, Vol. 102/103, pp. 1-24.

Hendrickx, Frank (2001), Protection of Workers' Personal Data in the EU, http://europa.eu.int/comm/employment_social/labour_law/docs/dataprot

ection_hendrickx_combinedstudies_en.pdf

Hoffman, Michael et. al. (2003), "You've Got Mail... And the Boss Knows".

ILO (1993), *Conditions of Work Digest: Worker's Privacy*, Vol. 12.

ILO (1996), 「근로자의 개인정보보호에 관한 행동강령」, 1996. 10. (http://www.ilo.org/public/english/support/publ/pdf/protect.pdf)

Jankanish, Michele (1993), "Monitoring and Surveillance in the Workplace: Privacy Issues in an International Perspective", *Conditions of Work Digestion Workers' Privacy*, Vol. 12, No. 3.

Jay Stanley and Barry Steinhardt (2003), "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society"

Kizza, Joseph and Jackline Ssanyu (2005), "Workplace Surveillance", in Weckert, John (ed.) (2005), *Electronic Monitoring in the Workplace: Controversies and Solutions*, London: IDEA Group Publishing.

Knights, D. and H. Willmott (eds.) (1992), *Skill and Consent: Contemporary Studies in the Labour Process, London*: Routledge.

Kovatch, Paul (2000), "Privacy Rights in the Workplace: Constitutional and Statutory Considerations", *Journal of Individual Employment Rights*, Vol. 9, No. 1, pp. 3-12.

Lane III, Frederick (2003), *The Naked Employee: How Technology is Compromising Workplace Privacy*, New York: Amacom.

Lee, Eric (2000), "Online Rights for Online Workers in Member States of the European Union".

Lyon, D. and E. Zureik (eds.) (1996), *Computers, Surveillance and Privacy*, University of Minnesota Press.

Lyon, David (1994). *The Electronic Eye: The Rise of Surveillance Society*, Minneapolis: Univ. of Minnesota Press.

McKenzie, Robin (2003), "Employee privacy and biometrics" (presentation)

Mosco and J. Wasko (eds.) (1988), *The Political Economy of Information*, Madison:

Univ. of Wisconsin Press.

National Workrights Institute, "Privacy Under Siege: Electronic Monitoring int the Workplace",

New South Wales (2005), "Workplace Surveillance Bill 2005"

OECD (1980), 「프라이버시보호와 개인정보의 국제적 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data」, 1980

OECD (1998), Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet, Group of Experts on Information Security and Privacy, Committee for Information, Computer and Communication Policy.

Office of the Victorian Privacy Commissioner (2003), Submission to the Victorian Law Reform Commission on its Issues Paper into Workplace Privacy.

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

Rule, James and Peter Brantley (1992), "Computerized Surveillance in the Workplace: Forms and Distributions," *Sociological Forum*, Vol. 7, No. 3, 405-423.

Schulman, Andrew (2001), "Computer and Internet Surveillance in the Workplace: Rough Notes", http://www.privacyfoundation.org/workplace.

Scott, Brandy (2001), "Employee E-Mail: a Protected Right to Privacy?" *Journal of Individual Employment Rights*, Vol. 9, No. 1, pp. 27-37.

Smythe, Narelle, Jason Shailer and Andre Stein (2004), "Watching the Workplace Surveillance Bill", *Privacy Law Bulletin*, Vol. 1, No. 3, pp. 3-4.

Stanley, Jay and Barry Steinhardt (2003), Bigger Monster, Weaker Chains: the Growth of an American Surveillance Society, Technology and Liberty

Program, American Civil Liberties Union.

Thompson, P. and C. Warhurst (eds.) (1998), *Workplaces of the Future*, Basingstroke: MacMillan.

Tribbey, Rebecca (1999), "Workplace Privacy: Audio and Video Surveillance," http://www.louisville.edu/cbpa/lmc.

Weckert, John (ed.) (2005), *Electronic Monitoring in the Workplace: Controversies and Solutions*, London: IDEA Group Publishing.

Wen, Joseph and Pamela Gershuny (2005), "Computer-based Monitoring in the American Workplace: Surveillance Technologies and Legal Challenges", *Human Systems Management*, Vol. 25. pp. 165-173.

Whitaker, R (1999), *The End of Privacy*, New York: New Press.

Zuboff, S (1988), *In the Age of the Smart Machine: the Future of Work and Power*, New York: Basic Books.

* 국내 문헌

강수돌 (2001), 「사업장 감시와 노동통제 - 그 배경과 효과」 (2001 Labormedia 발표문). □□ □□

계희열 (2002), 「헌법학(중)」, 박영사

고세일 (2005), 정보화시대 미국 근로자들의 사생활보호, 『국제노동브리프』 제3권 11호, p. 53-59.

권순원 (1998), 전자감시적 노동통제와 노동규율, "정보기술과 작업장감시" 워크숍 자료집, 1998. 11. 13.

권순원 (1998), 「전자 정보적 감시와 노동통제」 (민변 정책토론회 □□자료집).

김동노 (2003), 지식정보 사회의 감시체계와 개인의 프라이버시 보호, 계간 사상, 2003년 봄호.

김세곤 (2004), 「노동통제·감시와 노동자의 인권」, 조선대학교 박사논문.
김승환 (2001), "노동현장에서의 CCTV 설치와 노동자의 인권", 노동자 감시 문제와 대용 CCTV문제 해결을 위한 토론회, 발표문, 노동자감시 반대·대용 CCTV철거를 위한 전북공동대책위, 2001.9.12
김영권 (2004), 한국에서의 전자감시적 노동통제에 관한 사례 연구, (2004 산업사회학회 춘계학술대회 발표문).
김왕배·이경용 (2003), 「인터넷 사용과 직무감시」, 경제와 사회, 2003년 봄호.
김지형 (2000), 근로기준법 해설, 청림.
김철수 (2003), 헌법학신론, 박영사.
노동자감시근절을위한연대모임, (2003), 『보안관리시스템 관련 사업장 실태조사보고서』, (주)한길리서치연구소.
노동자감시근절을위한연대모임 (2004), 「노동자는 감시를 거부할 권리가 있다」.
노동자감시근절을위한연대모임 (2002), 첨단기술에 의한 노동감시, 어떻게 대응할 것인가, 토론회 자료집, 2002.11.1
민주노총 (2002), 2002 인권단협안 자료
민주노총 (2003), 노동자 감시 규제와 노동자 개인정보 보호에 관한 입법 제안, 2003.7.
민주노총·노동자감시근절연대모임 (2003), 노동 감시 실태조사 및 사례발표 기자회견 자료집, 2003. 7. 31.
박훈 (2001), 대용 손해배상 청구 사건에서의 핵심적인 쟁점과 이에 관련한 문제에 대하여, 노동자감시 반대·대용 CCTV철거를 위한 전북공동대책위, 노동자 감시 문제와 대용 CCTV문제 해결을 위한 토론회 자료집, 2001.9.12
성낙인, 통신에서의 기본권보호, 공법연구, 제30집 제2호
이광택·이병훈·임상훈·이종수 (2005), 전자 노동감시의 실태와 개선과제, 한국노동연구원.
이민영 (2003), 「직장내 전자우편의 감청에 대한 규율 방안」, 정보통신정책 15권 23호.

이병훈 · 김종성 (2004), 「전자감시와 노동자 반응: A은행 콜센터의 사례연구」, 『산업노동연구』 제 10권 2호.

이승준 (1994), 「정보사회에서의 감시 메카니즘에 관한 연구」, 성균관대 신문방송학과 석사논문.

이은우 (2002), 「노동감시 규제입법의 필요성과 내용」, "프라이버시위원회와 노동감시입법 - 외국의 경험과 우리의 모색" 국제워크샵 자료집, 2002. 11. 27.

이은우 (2002), 「노동감시에 대한 입법」, 유네스코한국위원회, 과학기술과 윤리 워크숍, 2002. 11. 16-17.

이은우 (2002), 「해외 입법사례와 반감시입법제안」, "첨단기술에 의한 노동자감시, 어떻게 대응할 것인가" 토론회 발표자료(노동자감시근절을위한연대모임), 2002. 11. 1.

이은우 (2003), 「위치정보 어떻게 보호할 것인가」, 진보네트워크센터, "정보인권과 위치정보의 보호 토론회" 자료집, 2003.6.24

임상훈 (2005), 「해외 노동현장 전자감시 사례와 관련 규제제도 및 정책」, 이광택 외, 『전자 노동감시의 실태와 개선과제』, 한국노동연구원.

작업장감시 조사연구팀 (1998). "정보기술과 사업장 감시" 워크숍 자료집.

장여경 (1998), 노동자를 감시하는 자본의 기술에 맞서기 위하여, 노동전선, 1998. 12.

장여경 (2002), 「노동 감시 기술의 사회적 형성」, 고려대 대학원 석사논문.

전국민주노동조합총연맹 (2003), "국가 · 자본의 정보화와 노동의 대응전략" 워크숍 자료집.

정진수 (1999), CCTV에 의한 감시와 사회통제, 형사정책연구 제10권 제3호(통권 제39호, 1999년 가을호)

조돈문 (1996), 「정보화와 노동과정의 변화: 자본의 전략적 선택과 딜레마」, 산업노동연구 제 2호, 1996.

최세진 · 권두섭 (2001), 노동자 감시 - 기술적 유형과 사례를 중심으로, 노동자 감시 반대 · 대용 CCTV철거를 위한 전북공동대책위, 노동자 감시 문제와 대용 CCTV문제 해결을 위한 토론회, 2001.9.12

최영호 (2003), 「이메일(E-Mail) 감시와 근로자의 인□□」, 노동법학□□, 서울대노동법연구회, 2003.7.19

하경효 (1994), 「근로관계에 있어서 근로자의 양심의 자유와 자기책□□」, 노동법에 있어서 권리와 책임□□ (김형배교수화갑기념논문집), 박영사, 1994

하경효 (2004) 「새로운 근로감시기술의 도입에 따른 법적 문□□」, 노동법학□□ 제18호, 한국노동법학회편, 2004.6

하경효, 전윤구 (2003), 「전자장비를 이용한 근로감시·관찰에 따른 법적 문□□」, 고려법학□□ 제41호, 고려대학교 법학연구원

함영언 (2000), 「정보기술의 도입과 노동통제의 변화에 관한 연□」, 연세대 사회학과 석사논문.

허영 (2003), 한국헌법론□□, 박영사.

## [부록1]

# 국제노동기구(ILO)의「 노동자의 개인정보 보호에 대한 행동 준칙(ILO Code of Practice: Protection of Workers' Personal Data」 (1996)

### 1. 서문

사용자는 구직자와 노동자에 대한 개인정보를 법을 지키기 위해, 직원의 고용과 훈련 및 인사 고과에서 참고삼기 위해, 개인의 안전·인적 담보·품질 관리·고객 서비스와 자산 보호를 위해서 수집한다. 다수의 국내법과 국제규범들이 개인정보의 처리에 관한 의무적인 절차를 규정하고 있다. 전산정보 검색기술, 사원 정보자동화시스템, 전자감시, 유전자 감별, 약물 실험 등은 개인정보보호장치가 개발되어야 할 필요성을 보여준다. 개인정보보호장치는 노동자의 존엄성, 프라이버시를 보호하고 노동자 자신이 누가 어떤 정보를 어떤 목적으로 그리고 어떤 조건하에서 사용할 것인지 결정할 수 있는 기본적인 권리를 보장해야 한다.

### 2. 목적

이 행동 강령의 목적은 노동자의 개인정보를 보호하기 위한 길라잡이를 제시하는 데 있다. 이 강령은 구속력은 없다. 이 강령은 제정법, 규칙·조례, 국제 근로기준이나 다른 일반기준을 대신하지 않는다. 이 강령은 법령, 규칙·조례, 단체협약, 근무규정, 정책과 실무적 규정을 발전시키는데 참고될 수 있다.

### 3. 정의

이 강령에서

3.1 개인정보라 함은 신원확인이 되었거나 신원확인이 가능한 노동자와 관계되는 모든 정보를 뜻한다.

3.2 처리라 함은 수집, 저장, 결합·배합, 교환 또는 개인정보의 다른 모든 사용을 포함한다.

3.3 감시라 함은 컴퓨터, 카메라, 영상장비, 음향설비, 전화기, 기타 통신장비와 같은 장비의 사용, 신원과 위치를 확인하는 다양한 방법, 혹은 기타 감시방법을 포함하면서 이에 국한되지 않는 것을 포함한다.

3.4 노동자라 함은 현재와 과거의 노동자 혹은 입사 지원자를 모두 포함한다.

## 4. 적용 범위

4.1 이 강령은

(a) 공공·민간부문 분야 모두에

(b) 노동자 개인정보의 수동·자동 처리에 모두 적용된다.

## 5. 일반적인 원칙

5.1 개인정보는 반드시 적법하고 공정하게, 그리고 오직 노동자의 고용과 직접 관련한 이유로만 처리되어야 한다.

5.2 개인정보는 원칙적으로 반드시 수집할 당시의 원래 목적과 동일한 목적으로만 사용되어야 한다.

5.3 만일 개인정보가 처음 수집될 당시의 목적과 다른 목적으로 처리되는 경우, 고용주는 반드시 원래의 목적과 모순된 목적으로 사용되지 않을 것임을 보장해야 하며, 상황 변화로 인해 발생할 수 있는 오해를 방지하는 데 필요한 대책을 반드시 수립해야 한다.

5.4 자동 정보 시스템의 보안이나 적절한 운영을 보장하기 위해 기술적이거나 관리적인 차원의 대책을 수립할 때 수집된 개인정보는 노동자의 행동을 통제

하는 데에 사용될 수 없다.

5.5 어떤 노동자에 대한 결정이 그 노동자에 대한 자동 처리된 개인정보에만 의존해서 이루어지면 안 된다.

5.6 전자 감시로 수집된 개인정보가 직무 수행 평가의 유일한 요소가 되어서는 안 된다.

5.7 고용주는 자신의 정보 처리 업무에 대해 정기적으로 평가해야한다.

(a) 수집된 개인정보의 종류와 양을 가능한 한 줄이기 위해

(b) 노동자의 프라이버시를 보호하는 방법을 개선하기 위해

5.8 노동자와 그 대표는 모든 정보수집 과정, 그 과정을 제어하는 규칙, 그리고 자신의 권리에 대해 통지 받아야 한다.

5.9 개인정보를 처리하는 사람은 정보 수집과 이 강령의 원칙을 적용하는데 있어 자신의 역할을 이해하기 위해 정기적으로 훈련받아야 한다.

5.10 개인정보의 처리는 고용이나 취업에서 불법적인 차별 효과를 주어서는 안 된다.

5.11 고용주, 노동자와 그 대표는 개인정보를 보호해야 하고 이 강령에 따라 노동자의 프라이버시에 대한 정책을 개발하도록 협력해야 한다.

5.12 고용주, 노동자 대표, 고용 알선 기관, 노동자 등 개인정보에 접근할 수 있는 모든 사람은 자신의 의무 이행과 이 강령의 원칙에 어긋나지 않는 비밀유지 의무를 지켜야만 한다.

5.13 노동자는 프라이버시권을 포기할 수 없다.

## 6. 개인정보의 수집

6.1 원칙적으로 모든 정보는 반드시 노동자 개인에게서 획득되어야 한다.

6.2 만약 개인정보를 제3자로부터 획득해야할 필요가 있을 경우, 노동자는 반드시 사전에 이를 통보 받아야 하고 이에 대한 명백한 동의 의사를 전달할 수 있어야 한다. 고용주는 반드시 처리 목적, 고용주가 사용하려는 출처와 수단 뿐 아니라 수집 정보의 유형, 그리고 만약에 동의 거부가 있다면 그 결과를 명시해야

한다.

6.3 만약 어떤 노동자가, 고용주나 다른 어떤 사람 혹은 조직에게 자신의 정보를 수집하거나 노출시킬 권한을 위임하는 계약서에 대한 서명을 요구받을 때에는, 계약서가 평이한 용어로 작성되어야 하고 구체적이어야 하며, 단체나 기관이 명시되어야 하고, 문제의 신상정보가 드러나 있어야 하며, 개인정보가 무엇을 목적으로 수집되는지와 계약서의 유효 기간이 명시되어 있어야 한다.

6.4 고용주가 노동자의 개인정보 사용에 대한 동의를 얻었을 경우, 고용주는 정보를 수집하거나 조사하는 사람과 기관이 언제나 조사 목적을 염두에 두고 그 재현에서 실수나 오해가 없도록 보장해야 한다.

6.5 (1) 고용주는 노동자의 다음 정보를 수집할 수 없다.

(a) 성생활

(b) 정치적인, 종교적인 또는 그 외의 믿음・신앙

(c) 전과

(2) 예외적으로 고용 결정에 직접 관련이 있고 적법한 경우에 고용주는 (1)의 경우에 해당되는 개인정보를 수집할 수 있다.

6.6 고용주는 법이나 단체협약에 의하여 강제되거나 허락된 경우가 아니면 특정 노동 단체에서의 지위나 노동자 조합활동에 관한 정보를 수집할 수 없다.

6.7 개인 의료정보는 적법하고 의료상의 기밀과 작업 현장의 건강과 안전에 대한 일반 원칙에 따라, 그리고 아래와 같이 필요한 경우가 아니면 수집될 수 없다.

(a) 노동자가 특정 직업에 맞는지 결정하기 위해

(b) 작업 현장의 건강과 안전을 위한 요구 조건을 만족시키기 위해

(c) 사회보장혜택을 위한 자격을 심사하고 그 혜택 수락여부를 결정하기 위해

6.8 만약 노동자가 이 강령의 5.1, 5.10, 6.5, 6.6 그리고 6.7에 어긋나는 요구를 받았을 때 노동자가 부정확하거나 불완전한 답을 한 경우, 노동자는 고용 관계가 종료되거나 다른 규율상의 처분을 받지 않아야 한다.

6.9 개인정보 요청에 대한 노동자의 잘못된 이해로 제공된 개인 정보 혹은

관계없거나 범위를 넘어서는 개인정보는 처리될 수 없다.

6.10 거짓말 탐지기, 사실 증명 장비와 기타 유사한 검사 절차는 사용될 수 없다.

6.11 인성 테스트 또는 유사한 검사 절차는 이 강령 규정에 따라야 하며, 노동자는 검사를 거부할 수 있음을 명시해야 한다.

6.12 유전자 검사는 금지되거나 법적으로 명확히 인정된 경우에만 한정되어야 한다.

6.13 약물 검사는 국가의 제정법과 관습법 또는 국제법 표준에 따라 이루어져야 한다. ILO는 사업장에서의 알콜과 약물 관련 사안의 처리에 대한 행동 강령과 "사업장에서의 약물과 알콜 검사에 대한 규범"을 가지고 있다.

6.14 (1) 노동자를 감시할 때에는 사전에 감시의 목적과 예정 시간, 사용되는 방법과 기술, 수집되는 정보를 알려야만 한다. 또한 고용주는 노동자의 프라이버시 침해를 최소화해야만 한다.

(2) 비밀스런 감시는 다음의 경우에만 허용된다.

(a) 국가의 법에 따를 때

(b) 합리적 근거에 기반하여 범죄행위 또는 그에 준하는 심각한 행위가 의심될 때

(3) 단, 지속적인 감시는 건강과 안전 또는 재산의 보호를 위해 필요할 때에만 허락된다.

## 7. 개인정보의 보안

7.1 고용주는 정보의 유실, 정보에 대한 권한 없는 접근과 그 사용, 수정, 유포를 막기 위하여 상황에 따른 적절한 보안 수단을 사용하고 개인정보를 보호할 의무가 있다.

## 8. 개인정보의 보관

8.1 이 강령의 개인정보 수집에 관한 원칙에 따른 방법으로 수집된 개인정보에 대해서만 보관을 허용해야 한다.

8.2 비밀이 보장되어야 하는 개인 의료 정보는 의료 기밀 규정에 따라야 하는 담당자에 의해 보관되어야 하며 다른 모든 개인정보와 분리하여 다루어져야 한다.

8.3 고용주는 전반적인 정보와 정기적으로 검토되는 개별 노동자의 개인 정보 항목과 그 처리에 대한 정보를 제공해야 한다.

8.4 고용주는 저장된 개인정보가 정확하고 최신의 것이며 완전하다는 것을 정기적으로 확증해야 한다.

8.5 개인정보를 수집할 당시의 특정한 필요성이 계속적으로 존재하는 동안에만 그 정보를 보관할 수 있다. 단, 다음의 경우는 예외로 한다.

(a) 노동자가 특정 기간 동안 구직자 명단에 올라 있기를 원할 때

(b) 국가의 법으로 개인정보의 보관이 요구될 때

(c) 현재 존재하거나 과거에 존재했던 고용 관계와 관련한 법적 증명 절차를 위하여 고용주 또는 노동자가 개인정보를 요구할 때

8.6 개인정보를 다음과 같은 방법으로 보관하고 작성되어져야 한다.

(a) 노동자가 이해할 수 있어야 한다.

(b) 노동자의 특성을 거론하며 그 노동자에 대한 차별을 유발해서는 안 된다.

## 9. 개인정보의 이용

9.1 개인정보는 그 수집, 교환, 보관에 대한 이 강령 안의 원칙에 따라 이용되어야 한다.

## 10. 개인정보의 전달

10.1 개인정보는 다음의 경우를 제외하고 노동자의 명시적 동의 없이 제3자

에게 전달될 수 없다.

(a) 생명과 건강에 대한 중대하고 절박한 위협을 막기 위해 필요할 때

(b) 법률로 요구되었거나 승인되었을 때

(c) 고용 관계의 관리를 위해 필요할 때

(d) 형법집행을 위해 요구될 때

10.2 노동자의 개인정보는 노동자의 인지와 명시적 동의 없이 상업적·영리적 목적을 위해 전달될 수 없다.

10.3 제3자에 대한 정보 전달 규칙은 동일 조직 내의 고용주들 간에 혹은 정부 각 기관간의 개인정보 전달에도 적용된다.

10.4 고용주는 노동자의 개인정보를 전달받은 자에게 그 개인정보는 제공한 목적에 한해서만 사용되어야 함을 고지해야 하며, 이의 이행에 대한 확인을 요청해야 한다. 단, 법적 의무에 따른 정식 전달은 예외로 한다.

10.5 개인정보의 내부적 전달은 노동자가 명백히 인지한 사람들에 한해야 한다.

10.6 개인정보의 내부이용은 그 개인정보가 특정 작업의 수행에 필요한 경우에 한하여 승인 받은 특정 이용자에게만 허용된다.

10.7 노동자의 개인정보를 포함한 자료들의 취합은 이 강령의 규정에 엄밀히 따르지 않는 한 금지된다.

10.8 의료 검사의 경우, 고용주는 특정한 고용의 결정에 관련한 판정만을 제공받을 수 있다.

10.9 그 판정은 어떠한 의료 정보도 포함할 수 없다. 판정은 제안된 작업에 적합한지를 나타내거나, 일정 종류의 직업, 일시적 혹은 영구적으로 의학적으로 금해야 하는 근무환경을 적시하는 내용을 포함할 수는 있다.

10.10 노동자의 대표에게 개인정보를 전달하는 것은 국가의 법률이나 관습법에 따른 단체협약에 따라 이루어져야 한다. 또한, 노동자 대표의 특정한 업무 수행에 필요한 개인정보에 국한되어야 한다.

10.11 고용주는 개인정보의 내부 흐름을 파악할 수 있고 그 처리과정이 이 강령에 따르도록 보장을 할 수 있는 절차를 채택해야 한다.

## 11. 개인의 권리

11.1 노동자는 확보된 자신의 개인정보와 그 개인정보의 처리과정을 정기적으로 고지받을 권리를 가진다.

11.2 개인정보가 자동화된 시스템으로 처리되었거나 노동자별로 특정한 수작업 파일에 보관되었거나 기타 어떤 형태로 노동자의 개인 정보가 보관되었든지 간에 노동자는 자신의 모든 개인정보에 접근할 수 있어야 한다.

11.3 노동자가 자신의 개인정보의 처리과정에 대하여 알 권리는 그 노동자의 개인정보를 포함하는 모든 형태의 기록을 검토하고 사본을 소지할 수 있는 권리를 포함한다.

11.4 노동자는 근무시간 중 자신의 개인정보에 대해 접근할 수 있는 권리를 가진다. 만약 근무시간에 이루어지지 못할 때에는 노동자와 고용주의 편의를 고려하여 실시되어야 한다.

11.5 노동자는 접근권의 행사를 보조할 노동자 대표나 보조자를 지명할 권리가 있다.

11.6 노동자는 자신이 선택한 의료전문가를 통해 자신의 의료 정보에 접근할 권리를 가진다.

11.7 고용주는 노동자가 자신의 기록에 접근하거나 복사하는 것에 대해 비용을 부담 지울 수 없다.

11.8 고용주는 안전 점검할 때 점검에 현저한 위해가 예상되는 경우에 한하여 점검이 끝날 때까지 노동자가 자신의 개인정보에 접근하는 것을 거부할 수 있다. 그러나 노동자가 자신의 모든 개인정보에 접근하기 전에는 인사에 관한 어떠한 결정도 이루어져서는 안 된다.

11.9 노동자는 잘못되고 불완전한 개인정보 및 이 강령의 규정에 따르지 않는 개인정보에 대해 삭제 혹은 수정을 요구할 권리를 갖는다.

11.10 개인정보를 삭제 혹은 수정할 경우, 고용주는 앞서 부정확하고 불완전한 개인정보를 제공받았던 모든 사람에게 삭제 혹은 수정된 내용을 알려야만 한다. 단, 삭제 혹은 수정의 통지가 필요하지 않다는 노동자의 동의가 있을 때에

는 알리지 않아도 된다.

11.11 고용주가 개인정보의 수정을 거절할 때, 노동자는 그 개인정보에 동의하지 않는다는 진술 혹은 그 근거 기록을 개인정보에 첨부할 권리를 가진다. 이후에 개인정보가 사용될 때에는 언제나 이 개인정보가 논란이 있음을 알리는 정보와 함께 해당 노동자의 진술이 포함되어야 한다.

11.12 사법 기록에 들어가는 개인정보의 경우 삭제나 수정이 불가능할 때에 노동자는 자신의 관점을 서술한 진술을 첨부함으로써 그 내용을 보충할 권리를 가진다. 이 진술은 포함하지 않아도 된다는 노동자의 동의가 없는 한 모든 개인정보의 전달시 포함되어야 한다.

11.13 이 강령의 규정에 따라 마련된 모든 법률, 규칙 조례, 단체협약, 업무규정 혹은 정책에 있어서, 고용주가 절차를 제대로 이행하지 않을 때 노동자가 배상받을 수 있는 방법을 적시해야 한다. 노동자가 제출하는 어떠한 진정도 받아들이고 답변하는 절차를 마련해야 한다. 진정 절차는 노동자가 이용하기 쉽고 간단해야 한다.

## 12. 집단적 권리

12.1 노동자의 개인정보 처리에 관한 모든 협상은 자신에 대한 어떠한 개인정보가 어떠한 조건 하에서 어떤 목적으로 사용되어야 하는지 알고 결정할 수 있는 개별 노동자의 권리를 보장하는 것을 목적으로 하는 이 행동 강령의 원칙에 따라야 한다.

12.2 노동자의 대표는 다음의 사항을 통지받고 조언할 수 있다.

(a) 노동자의 개인정보를 처리하는 자동 시스템의 채택 및 변경에 관하여

(b) 사업장 안의 전자 노동자 감시 시스템의 채택에 앞서

(c) 노동자의 개인정보에 대한 설문조사 및 검사를 해석하고 관리하는 방법과 내용, 목적에 대하여

## 13. 고용 알선 기관

13.1 만약 고용주가 노동자를 채용하기 위해서 고용 알선 기관을 이용한다면, 고용주는 고용 알선 기관에게 이 강령의 규정에 따라 개인정보를 처리할 것을 요구해야 한다.

## [부록2]

## EU의회「 회사에서의 전자통신 감시에 관한 특별조사위원회 보고서」 (2002년 5월)[45)]

노동자들은 매일 아침 회사에 들어서면서부터 자신의 개인정보를 보호받을 권리를 포기하지 않는다. 회사에서 타인들과 인간관계를 넓혀나감에 따라, 프라이버시 보호에 대한 적절한 수준의 기대를 하게 된다. 하지만 노동자의 권리는 고용주의 합법적인 권리와 요구, 특히 회사를 어느 정도 효율적으로 운영할 권리와 무엇보다 노동자의 행동에 의한 피해를 입는 것으로부터 보호받을 권리 사이에 균형을 이뤄야 한다. 이러한 고용주의 권리와 이익은 노동자의 프라이버시를 제한하는 적절한 제도를 정당화하는 합법적 근거가 된다. 고용주가 노동자의 범죄행위의 피해자가 되는 경우가 그런 예에 해당한다. 이렇게 다양한 권리와 요구들의 균형을 이루기 위해선 여러 가지 원칙들이 필요하다. 감시행위가 고용주의 요구를 만족시키기에 편리하다는 단순한 사실만으로 고용주의 행위가 정당화되지는 않는다는 것을 명심해야한다. 감시는 이 보고서에 제시된 여러 원칙들의 검토를 거쳐 수행되어야 한다.

다음의 질문으로 그러한 평가가 요약될 수 있겠다.

a) 감시행위가 노동자에게 투명한가?

b) 전자통신감시가 필요한가? 전통적인 감시방법으로는 똑같은 결과를 얻을 수 없는가?

c) 개인정보의 처리가 노동자에게 공정하게 여겨지는가?

d) 결합되는 이해관계 간에 균형이 유지되는가?

본 보고서는 이러한 원칙들의 실질적인 적용에 초점을 맞추어 회사의 특성과

45) 노동자감시근절연대모임(http://www.gamsi.net)에서 작성한 자료임.

규모, 정보보호와 관련된 법을 고려하는 등 좀 더 세심하게 노동자와 고용주 모두 최소한으로 받아들일 수 있는 이메일과 인터넷 사용에 대한 회사방침에 가이드라인을 제시한다.

사적인 용도로 인터넷을 사용하는 것에 대해, 허용해 놓고 감시하는 것보다는 아예 그런 용도로 사용하지 못하게끔 하는 것이 고용주의 요구를 더욱 만족시킨다. 이런 맥락에서 기술적 해법이 굉장히 유용하다. 인터넷을 사적인 용도로 사용하는 것에 대한 포괄적인 금지는 근거가 없어 보이고, 인터넷이 노동자의 일상생활에서 얼마나 도움이 되는지를 고려하지 않은 처사가 된다.

고용주는 노동자에게, i) 감시장비의 위치, 용도, 목적에 대해 고지해야 하고, 비공개 감시가 지속될 만한 중요한 근거가 없는 한, ii) 적발된 인터넷과 이메일의 오용에 대해 고지해야 한다. 노동자에게 시스템이 감시되고 있고, 허용되지 않은 네트워크의 사용을 금지한다는 경고 메시지를 띄움으로써 즉시 고지하는 것이 가능하다.

고용주가 노동자에게 두 개의 계정을 주는 것도 고려해볼 수 있다.

a) 하나는 오로지 업무용으로서, 이 보고서에서 제시하는 허용된 범위에서 감시가 가능하다.

b) 다른 하나는 오직 사적 용도로만 쓰이는 계정(또는 웹메일 사용의 허가)으로서, 안전규제만을 받으며, 예외적인 경우에만 남용을 점검할 수 있다.

*** 회사에서의 감시 사회에 대한 도전**

최근 들어 직장에서 이메일 사용이 점증함에 따라 노동자 감시문제가 주목을 받고 있다. 감시 문제를 고려함에 있어 직장에서 노동자의 프라이버시가 어느 정도 보장되어야 하지만 고용주의 정당한 이해관계를 침해할 수 있는 노동자의 행동으로부터 자신을 방어할 권리, 예를 들어 노동자의 행동에 대해 고용주가 책임을 져야할 경우와 회사를 효율적으로 운영하려는 고용주의 권리 간에 균형을 이루어야 한다.

새로운 기술은 고용주에게 유용한 자원의 발전에 기여하는 반면, 전자감시 장비는 노동자의 권리와 자유를 침해하는 수단으로 사용될 위험이 내재되어 있다.

명심해야 할 것은 새로운 정보기술의 도래함에 따라 노동자들이 온라인에서든 오프라인에서든 간에 작업하는 동안 자신의 권리가 침해되어서는 안 된다는 사실이다. 더욱이 작업환경이 점점 발달하여 업무시간과 사생활을 명확히 구분하기가 쉽지 않다는 사실이다. 특히 '홈오피스'가 발전함에 따라 대다수의 노동자들은 고용주가 제공한 컴퓨터 작업환경이 갖추어진 집에서 일을 한다. 노동자의 존엄성은 다른 어떤 조건보다 우선한다. 이 문제를 고려하는 데 있어 감시행위가 노동자와 고용주간의 관계와 업무 그 자체에 끼칠 수 있는 부정적인 영향을 인지하는 것이 중요하다.

## 2. 국제 법적 기구

### 2.1 '인권과 기본적 자유 보호를 위한 유럽협약'의 제8항, 제10항

제8항

1) 누구나 자신의 개인과 가족생활, 집, 통신을 존중받을 권리가 있다.

2) 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.

제10항

1) 누구나 표현의 자유를 누린다. 이 권리는 국경에 상관없이 공공기관의 방해를 받지 않고 생각과 이념을 자유롭게 교환할 수 있음을 의미한다. 이 조항은 국가가 텔레비전이나 영화를 통해 방송할 수 있는 권리를 요구하는 것을 금지하지 않는다.

유럽인권재판소는 제8항에 명시된 '사생활'의 보호는 노동자의 집안 내에서의

생활로만 제한하지 않고 업무활동도 포함하는 개념임을 명확히 했다. '니미츠 對 독일' 사건에서 재판소는 다음과 같이 진술했다. "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 對 영국' 사건에서 재판소는 업무중 노동자의 전화를 가로채는 행위는 '협약'의 제8항을 위반한 것으로 판명했다. 해포드에게는 두 대의 전화가 있었는데, 그 중 하나는 개인용이었다. 그 전화의 사용에 대한 어떤 지침이나 제한도 없었다. 해포드도 자신의 전화사용을 가로챈 행위는 협약의 제8항을 위반한 것이라고 진술했다. 그러나 정부는 개인전화의 사용에 있어서 프라이버시 보호가 기대될 만한 근거가 없기 때문에 회사에서 그녀가 사용한 전화는 제8항에 해당되지 않는다고 제기했다. 정부의 변호인단은 고용주는 원칙적으로 노동자에게 사전고지 없이도 고용주가 제공한 전화의 통화내역을 감시할 수 있다고 주장했다. 그러나 재판소는 "집에서뿐만 아니라 업무활동에서 사용한 통화내역도 제8항이 의미하는 바의 '사생활'과 '통신'의 범위에 포함된다. 내선전화의 사용자인 해포드에게 시스템이 가로채일 수 있다는 경고를 했다는 증거가 없다. 따라서, 본 재판소는 그녀가 전화통화시 프라이버시 보호에 대한 기대를 했을 것이라 생각한다."

'통신'은 종이로 주고받는 편지뿐만 아니라 회사에서 사용하는 모든 전자통신 수단을 의미한다. 노동자가 고용주로부터 통신이 감청될 위험이 있다고 사전에 경고를 받았다면, 프라이버시에 대한 기대를 하지도 않을 것이고 감청을 해도 협약 8항에 저촉되지 않는다는 의미로 받아들이는 사람도 있다.

그러나 위원회는 노동자에 대한 사전경고가 정보보호 권리의 침해를 정당화할 수 없다고 생각한다.

제8항에 관련된 판결들로부터 유추할 수 있는 세 가지 원칙

a) 노동자는 회사에서의 프라이버시 통신장비나 사무기구가 고용주가 제공

했다는 사실로 인해 침해되어서는 안 되는 것에 대한 정당한 기대치가 있다.

b) 통신비밀에 대한 일반적 원칙은 작업장에서의 모든 통신을 포함한다. 이메일과 첨부파일도 포함한다.

c) 사생활에 대한 존중은 타인과의 관계를 발전시킬 권리를 포함한다. 그러한 관계 맺기가 상당부분 회사에서 이루어진다는 사실은 감시제도에 대한 고용주의 합법적 요구에 제한을 가한다.

2.2 개인정보의 자동처리에 있어 개인의 보호에 관한 협약

- 고용관계에서 사용되는 개인정보 보호에 관한 유럽의회 보고서(89)
- 의료정보 보호에 관한 보고서(97)
- 사회보험을 목적으로 쓰이는 개인정보 보호에 관한 보고서(86)
- 통신서비스 영역에서 개인정보 보호에 관한 유럽의회의 권고안(95)

2.3 EU의 인권헌장

제7항 개인과 가정생활의 존중

제8항 개인정보의 보호

2.4 ILO 개인정보 보호에 관한 행동강령(96) - [부록 1] 참조

3. 회사에서의 전자통신 감시(지침 95/46/EC)

회사에서의 감시기제는 여러 가지가 있는데 본 보고서에서는 비슷한 원칙이 적용되는 이메일과 인터넷 사용의 감시에 대해서만 다룬다.

3.1 이메일과 인터넷 감시에 적용되는 일반적 원칙

다음의 정보보호에 관한 원칙들은 반드시 준수되어야 하고, 감시활동의 합법

성을 획득하는데 필요하다.

① 필요성

- 고용주는 감시행위를 시작하기 전에 어떤 형태의 감시활동이건 특별한 목적을 위해 절대적으로 필요한지 점검해야 한다.

- 예외적인 경우 : 고용주의 입장에서 노동자의 특정한 행동에 대한 증거나 확신을 얻을 필요가 있을 경우. 고용주가 노동자의 행위에 대한 책임을 대신 저야 할 경우 등과 같이 고용주의 이해관계를 침해하는 노동자의 범죄행위나 통신시스템의 안전을 유지하기 위해 바이러스를 찾거나 시스템을 점검하려 할 때. 또한 노동자가 질병이나 휴일로 회사에 없는 경우 통신을 계속 가동하기 위해서나, 자동응답이나 자동전달 방법 외에는 통신이 유지될 수 없는 경우에도 노동자의 이메일을 열어볼 수 있다.

② 합목적성

- 고용주는 적절하고 합법적인 목적하에 정보를 수집해야 한다. 그런 목적에 부합하지 않는다면 당장 금지되어야 한다. 이런 맥락에서 '일관성'이란 원칙은, 예를 들면 통신시스템의 안전을 위해 정보를 수집했다면 이 정보는 다른 목적 노동자의 감시 으로 쓰여서는 안 된다는 의미이다.

③ 투명성

- 고용주는 감시행위에 대해 항상 공개해야 한다. 이 원칙은 지침의 13항에 명시된 예외의 경우를 제외하고는 비공개 감시가 허용되지 않음을 의미한다. 특정한 범죄행위가 명백하거나 고용주가 작업장에서의 위법행위를 적발하는 것이 법적으로 허용되있는 경우에 해당한다.

- 정보주체에게 고지할 의무

고용주는 노동자에게 이메일과 인터넷 사용의 감시에 관해 명확한 진술과 용이한 접근을 제공해야 한다. 노동자는 예외적 규칙이 적용되는 경우는 무엇인지

그리고 감시가 허용되는 범위는 어디까지인가에 대한 모든 정보를 제공받아야 한다. 제공되는 정보는 다음과 같다.

1) 회사가 소유한 통신장비가 노동자의 개인용도로 사용될 수 있는 범위에 대한 자세한 설명(예를 들면 사용시간의 제한 등)

2) 감시의 근거와 목적에 대한 정보. 고용주가 회사의 장비를 사적인 용도로 사용하는 것을 허락했을 때, 통신 내용은 매우 제한적인 조건 하에서 감시될 수 있다. 이를테면 바이러스 체크와 같은 시스템의 점검을 위해서

3) 감시를 누가, 무엇을, 어떻게, 언제 하는지에 대한 정보

4) 노동자에게 고용주들의 요구에 대해 대응할 기회와 내부방침의 위반을 알려주는 것이 언제, 어떻게 이루어지는지에 대한 자세한 시행절차

- 보통의 경우 감시가 지속될 만한 정당한 근거가 없다면 전자감시의 오용에 대해 노동자에게 즉시 고지하도록 해야 한다. 허가받지 않은 네트워크 접속을 감시하고 있다는 경고메시지를 띄움으로써 노동자에게 즉각적인 고지가 가능하다. 투명성의 원칙의 또다른 예로서 고용주가 노동관련 정책을 입안하기 전 노동자 대표에게 알리거나 자문을 구하는 방식이 있다.

- 자동전산처리를 하기 전 감독기관을 명시할 의무

노동자가 정보보호 규정(정보의 범주, 목적, 고용주가 노동자의 개인정보를 처리하게 되는 수용자는 누구인지)을 항상 점검할 수 있게 한다.

- 개인정보에 대한 접근 권리

노동자는 고용주가 수집한 자신에 관계된 개인정보에 접근할 권리를 갖는다. 또한 정보가 부정확하고 불완전하다면 지침을 위반하지 않는 선에서 노동자는 정보의 수정, 삭제, 접근금지에 대한 요구를 할 수 있다. 노동자가 적절한 기간동안 과도한 비용이나 지연 없이 손쉽게 정보에 접근할 수 있도록 하는 것은 노동자들로 하여금 작업장에서의 행동감시가 여전히 노동자에게 공정하고 합법적임을 확신시키는데 좋은 수단이 된다. 그러나 소위 평가자료에의 접근과 같은 예외적인

경우에는 문제가 될 수 있다.

④ 합법성

- 정보의 처리는 지침 7항에 의해 합법적인 목적 하에 수행되어야 한다. 경쟁사에 영업비밀이 유출되는 것과 같은 영업상의 비밀보호는 합법적 요구에 해당한다. 민감한 정보를 다루는 것은 문제가 되는데, 8항(b)은 다음과 같이 언급하고 있다. "적절한 안전장치가 있는 국내법에 의해 규정되는 한에서 고용관계법에서의 권리와 법적의무를 다해야 할 목적하에서는 민감한 정보의 처리가 가능하다."

- 감시행위와 관련된 민감한 정보의 처리는 어려운 문제인데, 고용관계에서만 문제가 되는 것은 아니다. 실제로 법에 의해 적절한 보호장치가 마련되지 않는다면 노동자의 민감한 정보를 다룰 목적으로 행해지는 감시는 지침에 비춰볼 때 적법하지 않고 용납되지도 않을 것이다. 그러나 많은 경우 합법적일 뿐 아니라 시스템의 안전을 위해 바람직하기까지도 한 감시행위를 민감한 정보처리가 불가피하게 수반된다는 사실만으로 금지하거나 어렵게 하는 것 또한 용납되지 않을 것으로 보인다.

⑤ 적절성

감시과정에서 얻은 개인정보는 특정한 목적을 이루는데 있어 적절해야 하고 과도하지 않아야 한다.

기업의 정책은 기업이 직면한 위험의 크기와 형태에 따라 적절히 맞춰져야 한다. 따라서 시스템의 안전을 위한 목적 이외에는 모든 직원들의 통신사용을 비밀리에 감시하는 행위는 금지된다. 가능하다면 이메일 감시는 고용주가 걱정하지 않아도 된다면 그 내용보다는 시간이나 이동정보로 한정해야 한다. 이메일의 내용에 대한 접근이 절대적으로 필요하다면 받는 사람 뿐 아니라 보내는 사람의 프라이버시에 대한 고려도 해야한다. 고용주는 보내는 사람에게 고지를 하는 충분한 노력을 해야한다.

⑥ 정보의 보존과 정확성

고용주에 의해 합법적으로 저장된 정보는 정확해야하고 필요이상으로 오랫동안 보존되어서는 안된다. 고용주는 영업적 요구에 기반하여 중앙서버에의 보존기간을 명시해야 한다. 보통 3달을 넘기지 않아야 한다.

⑦ 안전성

고용주는 보존하고 있는 개인정보가 외부로부터 안전함을 보장할 적절할 기술적인 대책을 시행해야 한다. 위원회는 시스템안전의 유지가 중요하다는 점에서 이메일의 자동검사는 적절한 안전장치가 마련된다면 노동자의 프라이버시 침해가 아니라고 생각한다. 시스템 운영자나 감시과정에서 노동자 개인정보에 접근하려는 모든 사람은 비밀 유지 의무를 지닌다.

4. 이메일 감시

4.1 통신비밀 원칙

위원회는 이메일이건 전통적 방식의 편지건 똑같이 보호의 대상이 되어야 한다고 생각한다. 유럽인권재판소는 민주사회에서 '통신비밀에 관한 원칙'의 적용에 대한 가이드라인을 제시했다. 업무영역에서의 전자통신도 앞서 언급했던 협약 8항의 '사생활'과 '통신'의 개념에 포함된다.

협약이 보호하고 있는 다른 권리와 자유(고용주의 합법적 요구)와 충돌할 때, 위의 원칙이 얼마나 훼손되거나 제한될 것인가 하는 문제가 있다. 어떤 경우든 감시에 사용된 전자장비의 소유권과 위치는 법에 규정된 통신비밀을 배제하거나 불가능하게 하지 않는다. 위원회는 보고서에 제시된 해결책이 다양한 이해관계를 잘 조정하는데 유용할 것이라 확신한다.

4.2 지침(95/46/EC)에 따른 합법성

- 개인정보가 담긴 이메일은 지침에 의해 보호된다. 그래서 고용주는 이 정

보를 처리할 정당한 근거가 있어야 한다. 노동자는 자유로운 상황에서 동의할 수 있어야 하고 충분히 정보가 제공되어야 하며, 일반적으로 합법적 수단으로써 노동자의 동의에만 근거해서 개인정보를 처리해서도 안 된다.

제7항(f)에도 있듯이 정보가 공개되는 제3자나 통제자의 정당한 이해관계가 걸려있을 때는 이메일 감시가 합법화된다. 그러나 그렇다고 해서 통신비밀권리에 해당하는 노동자의 기본적 권리와 자유를 침해해선 안 된다.

- 동의란 노동자가 정말로 자유롭게 선택할 수 있어야 하고, 어떤 손해 없이도 그 동의를 파기할 수 있어야 한다.

- 노동자에게 순전히 개인적인 용도로 메일계정이 부여되거나 웹메일에 접근할 수 있도록 허용되었을 경우, 고용주가 이 계정을 열람하는 것은 (바이러스 체크와는 별도로) 아주 제한적인 조건에서만 정당화될 수 있다.

4.3 기업이 노동자에게 제공해야하는 최소한의 정보

1) 노동자에게 순수한 개인용 메일계정을 가질 권리가 부여되는지, 작업장에서 웹메일 계정의 사용이 허락되는지, 고용주가 개인용도로 쓸 웹메일 계정의 사용을 권유했는지 여부

2) 노동자가 예기치 않게 부재중일 때 메일의 내용에 접근하기 위한 설비, 접근을 하려는 목적

3) 메시지의 백업화일이 있을 때, 그것의 보존기간

4) 이메일이 서버에서 틀림없이 지워졌다는 증거

5) 안전문제

6) 정책형성과정에서 노동자 대표의 참여

4.4 웹메일

위원회는 노동자가 웹메일이나 개인용 계정을 사용하도록 하는 것은 문제를 해결하는데 실질적인 도움이 된다고 생각한다. 고용주의 입장에서 쓴 보고서에서는 개인용과 업무용을 명확히 구분하여, 고용주가 노동자의 프라이버시를 침해할 위험을 감소시킬 것이라 한다. 더 나아가 고용주에게는 초과 비용이 들지 않을 것

이라 한다.

고용주가 이런 정책을 채택한다면 노동자의 행동이 의심스러운 경우에 있어서 웹메일 계정을 사용하는 시간을 알려줌으로써 노동자가 개인용 PC를 얼마나 많이 사용하는지 감시하는 것이 가능하다. 이런 방법을 사용하면 노동자의 민감한 정보가 공개될 위험 없이 고용주의 요구가 보장될 수 있다.

1) 웹메일이나 허용된 개인계정의 사용은 4장에서 언급한 다른 메일계정에 적용되는 원칙을 똑같이 적용 받는다.

2) 웹메일 사용을 허락했을때 회사는 특히 바이러스의 확산과 같이 네트워크의 안전이 위협당할 수 있다는 사실을 명심해야한다.

3) 때로는 웹메일의 서버가 개인정보보호에 관한 조항이 없는 다른 나라에 위치할 수도 있다는 점을 노동자는 명심해야 한다.

## 5. 인터넷 접근의 감시

### 5.1 업무시 인터넷의 개인적 사용

제일 먼저 강조되어야 할 것은 노동자에게 개인용도로 인터넷의 이용을 허락할 것인지와 그 허용범위는 어디까지인가에 대한 결정을 회사가 전적으로 하게 된다는 것이다. 위원회는 노동자의 인터넷 사용의 총괄적 금지는 노동자가 일상생활 속에서 인터넷으로부터 얼마나 많은 도움을 받는지가 전혀 고려되지 않기에 비현실적이라고 생각한다.

### 5.2 인터넷 감시에 관한 원칙들

인터넷의 개인적 사용을 감시하려는 것보다는 기술적으로 아예 금지하는 것이 더 낫다. 다시 말해, 요용을 감시하는데 자원을 낭비하는 것보다는 기술적으로 오용을 막는 것이 고용주의 입장에선 더 낫다는 것이다. 가능한 범위 내에서 자동 접근경고를 한다거나 몇 개의 사이트를 차단하는 등 행동에 대한 감시를 하기보다는 기술적으로 접근을 제한하는 방식에 의존해야한다.

인터넷의 의심스러운 사용을 적발하는 즉시 고지하는 것은 문제를 최소화하

는데 중요하다. 비록 이것이 필요한 방법이라 할지라도 감시는 고용주가 처한 위험에 대한 적절한 대응책이 되어야 한다.

대부분의 경우 인터넷의 오용은 방문한 사이트의 내용을 검사할 필요도 없이 적발할 수 있다. 예를 들어, 사용시간을 체크하고 가장 자주 방문하는 사이트를 체크하는 것은 고용주가 자신의 장비가 오용되고 있는지 여부를 확인하기에 충분하다.

노동자의 인터넷 사용을 점검할 때 고용주는 검색엔진이나 링크, 배너광고, 오타 등으로 인해 의도치 않게 사이트를 방문할 수도 있다는 사실을 고려하여, 쉽게 결론을 내려서는 안된다. 어떤 경우든 노동자에게 고용주가 주장하는 오용에 대해 사실을 알려야 하고, 이에 대해 이의를 제기할 수 있는 기회를 주어야 한다.

5.3 회사의 인터넷 정책에 대한 추천항목

1) 3.1의 투명성의 원칙

2) 고용주는 노동자가 복사하거나 검색할 수 없는 자료에 대해 충분히 고지하고 인터넷의 개인적 사용이 허용되는 조건에 대해 명확히 제시해야 한다.

3) 노동자는 인터넷의 오용을 감시하고 특정한 사이트를 차단하는 시스템에 대해 고지받아야 한다. 감시가 개인이나 회사의 영역과 관련이 있는지, 고용주가 특정한 환경에서 방문한 사이트를 보고, 기록하는지 등 감시의 범위가 정해져야 한다.

4) 위반사실의 조사와 정책수행과정에서의 노동자 대표 참여

## [부록3]

# 호주 뉴사우스웨일즈 주의 「작업장비디오감시법 (Workplace Video Surveillance Act)」(1998년 제정)

1. 도입

최근 몇 년간 뉴사우스웨일즈에서는 도로, 공중교통시설, 금융 기관, 소매 상점, 그리고 직장에서의 비디오 감시 카메라 설치가 급증해 왔다. 감시가 증가하는 만큼 많은 사람들이 정기적이거나 지속적인 비디오 감시를 받고 있다.

비디오 감시는 상대적으로 저렴한 가격으로 특정 지점을 지속적으로 감시할 수 있으며, 그 가격도 점점 더 저렴해지는 추세이다. 최신 감시 장비는 열악한 조명 아래서도 순간을 녹화할 수도 있는 비범한 능력을 가지고 있다. 카메라 렌즈는 핀홀 정도 작은 구멍의 크기로 축소되어 왔으며 이제 어느 장소에서나 어떤 물건으로도 녹화되는 것을 찾아내지 못하도록 할 수도 있다. 비디오 감시의 이점은 노동자의 안전을 모니터하고 생산 관련 문제를 방지할 수 있다는 데 있다. 또한 고객서비스를 향상시키는 데 도움이 될 수 있으며 노동자 교육 수단으로 사용될 수도 있고 어떤 경우에는 회사나 노동자의 법적 문제에서 책임 여부를 분명히 밝힐 수도 있다.

동시에, 비디오 감시는 노동자 개인의 프라이버시와 이동의 자유, 그리고 단결권에 대한 현저한 위협이다. 비디오 감시는 의심하고 불신하는 풍토를 유발하면서 직장의 사기를 떨어뜨릴 수 있다. 노동자는 지속적으로 감시당하기 때문에 노동자의 직장 스트레스가 증가되고 생산성이 저하된다. 노동자의 행동은 노동자가 모르는 새 영원히 추적되고 저장된다. 이제는 넓은 영역에서의 이동도 손쉽게 감지된다.

직장에서 비디오 감시를 사용할 때는 회사의 사업상 이익과 노동자의 프라이버시 간에 균형을 꾀하는 것이 중요하다. 이 강령은 이런 균형을 달성하기 위한 지침으로 만들어졌다.

이 강령은 법적인 규제와 더불어 작동하도록 고안되었다.

비디오 감시는 직장내 개인의 프라이버시에 대한 중대한 위협이다. 회사가 비디오 감시 장비를 설치할 때는 높은 수준의 규제를 받아야 한다. 이런 결정 과정은 이하의 내용을 고려해야 한다.

2. 금지된 사용

직장에서 다음의 경우 비디오 감시를 사용할 수 없다.

(1) 개별 노동자의 작업 수행을 모니터링하기 위한 목적을 위한 비디오 감시

(2) 노동 관계법원에서 허용하지 않는 공개적인 비디오 감시

(3) 화장실과 샤워룸, 탈의실에서의 비디오 감시

(4) 노동 관계법원이 허용하지 않는 락카룸과 직원 휴게실에서의 비디오 감시

3. 협의

회사는 비디오 감시 기기를 설치할 때 노동자와 노동자 대표와 협의해야 한다. 이러한 협의의 영향을 받는 노동자들은 회사로부터 감시 정책, 절차와 그 목적에 대한 문서를 제공받아야 한다.

4. 고지

초기에 노동자 협의가 끝나면 비디오 감시의 영역은 명확하게 표시되어야 한다. 이 표시들은 노동자들과 감시 행위의 공중에게 고지하려는 목적과 더불어 불법적이고 부적절한 감시 행위를 제지하기 위한 목적을 충족시킨다. 표시는 아래의 내용을 고지해야 한다.

(1) 감시를 하는 영역
(2) 감시의 명확한 목적
(3) 감시를 하는 시간
(4) 조직 내 감시의 책임자

5. 정당한 감시

카메라를 설치하고 12개월 안에, 회사는 비디오 감시가 본래의 목적을 달성하는데 효과적이라는 것을 증명해야 한다. 카메라는 오직 그 초기 목적을 달성하는데 효과적이고 그 감시가 계속 실재적으로 정당함을 보여줄 수 있는 경우에만 유지해야 한다.

6. 카메라 가동 시간

비디오 감시는 카메라가 원칙 1(역주: 뉴사우스웨일즈의 데이터 보호 원칙)에서 언급된 특정한 목적에 비추어 정당하게 사용되는 시간 동안에만 가동될 수 있다.

7. 감시 카메라의 위치

카메라는 명확하고 분명한 보안 위험이 있는 장소에만 설치될 수 있다. 카메라는 작업 기능의 직접적인 수행에 관여되어 있지 않은 노동자를 감시하는 장소에 설치되어서는 안 된다.

8. 감시의 수행

감시 카메라는 윤리적으로 가동되어야만 한다. 카메라는 개인을 확대하거나 이유없이 개인의 활동을 염탐하는데 사용되어서는 안 된다. 카메라는 그 목적에

적합하지 않은 기능을 위해 사용되어서는 안 된다. 회사는 카메라 조작자가 적절하지 않은 방법으로 감시를 행하는 것을 발견하였을 경우 적절한 징계 행위를 취해야만 한다.

9. 테이프에 대한 접근

테이프에 대한 접근은 감시를 본래 목적 내에서 제한적으로 기록을 사용하는 개인에게 한정되어야만 한다. 이것은 보안 담당자나 상급 관리직에 있는 사람이 될 수 있겠다. 테이프에 대한 접근이 있었던 경우는 모두 기록되어야만 한다. 개인들은 직장에서 자신들의 행위를 기록한 테이프에 접근할 자격이 주어져야만 하며, 그런 테이프는 일반적인 보존 기간 이상으로 보존되어야만 한다.

10. 보존

특별한 탐문의 목적이 없는 한 테이프는 최대 7일 동안 보존된 후에 삭제되거나 파괴된다.

11. 테이프에 대한 제3자 접근의 제한

법에서 보장하는 접근 이외에 직장에 대한 제3자는 테이프 기록에 접근할 수 없다.

12. 노동자가 자신의 기록에 접근할 수 있는 권리

감시 카메라에 잡힌 화면으로 인해 노동자가 경고나 (법적 처분 등) 어떤 징계에 처하게 될 경우, 사고 당시의 비디오테이프에 대한 노동자나 노동자 대표의 접근을 경고, 징계나 법적 처분이 내려진 후 14일 내에 허용해야 한다.

13. 예외

회사가 이 강령으로부터 특별한 예외를 적용하려면, 직장의 어떠한 특별한 상황이 직장에 일반적으로 적용되는 원칙으로부터 예외가 될 수 있는지 합리적인 설명을 제공할 수 있어야만 한다. 이러한 예외의 적용은 프라이버시 위원회에 의해 승인 또는 거부될 수 있다.

14. 협력 사항

회사는 비디오 감시를 수행하는 담당자를 임명한다. 자문적 판정을 하는 프라이버시 위원회에 대해 강령의 시행과 관련해 이의를 제기할 수 있다.

## [부록4]

# 민주노총의「 단체협약 모범안」 중 노동자감시 관련조항(2002)

제10장 노동자 인권·개인 정보 보호와 감시규제

제2절 노동자 개인 정보 보호

제114조【개인 정보의 보호】회사는 업무상 취득한 조합원의 성명, 나이, 생년월일, 근속년수, 금융거래, 전 직장, 가족현황, 병역, 정당가입 여부, 결혼내역, 성적지향 등 일체의 개인 정보를 보호해야 한다.

제115조【개인 정보의 수집】①회사는 노동자의 개인 정보의 수집에 있어서 고용과 직접적으로 관련된 것만을 대상으로 해야 하며 그 목적과 내용, 수집방법, 담당부서와 담당자에 대해 조합과 사전 합의해야 한다.

②회사는 개인정보를 수집할 경우 조합원 본인으로부터 직접 취득해야 하며 개인정보를 제3자로부터 획득해야 할 필요가 있을 경우라 하더라도 해당 조합원의 명시적인 동의없이 취득해서는 아니된다.

③회사는 사상, 신념, 종교 등 조합원의 권리, 이익, 사생활을 침해할 우려가 있는 개인 정보를 수집하여서는 아니된다.

④회사는 조합원들의 조합활동이나 사내외 단체 활동 및 업무외 사적인 활동에 대한 정보를 수집해서는 안된다.

제116조【개인 정보 제공 거부권 】조합원은 고용과 직접적으로 관련되지 않은 사생활을 침해할 수 있는 개인 정보에 대해 거부할 권리가 있으며, 회사는 이를 이유로 불이익 처우를 해서는 아니된다.

제117조【개인 정보의 관리】① 회사는 조합원의 개인 정보를 관리함에 있어 다음 각호에 대해 조합과 사전 합의하여야 하며 조합원들에게 고지하여야 한다.

1.보관기간과 방법

2.처리 및 폐기 방법

3.담당부서와 담당자

② 회사는 조합원의 개인 정보를 해당 조합원의 동의없이 담당부서와 담당자를 제외한 회사내외의 제3자에게 제공해서는 아니된다.

③ 회사는 조합 또는 해당 조합원이 개인 정보의 열람 및 사본복사를 요구할 경우 이에 응해야 하며 비용을 부담한다.

④ 회사는 개인 정보 관리를 위해 별도의 규정을 마련하고 그 내용에 대해 조합과 사전협의하여야 한다.

제118조【개인 정보의 수정과 폐기】① 회사는 조합 또는 조합원이 다음 각호의 경우에 대해 개인 정보의 수정, 폐기를 요구할 경우 이에 응해야 하며 그 결과를 통보해주어야 한다.

1. 조합과 합의없이 수집, 관리되고 있는 개인 정보

2. 사실과 다른 개인 정보

3. 고용과 직접적으로 관련되지 않은 사생활을 침해할 수 있는 개인 정보

② 회사는 보관기간이 종료되었을 때는 폐기해야 하며, 해당 조합원에게 통보해주어야 한다. 단, 다음 각호의 경우는 그렇지 아니한다.

1. 조합 또는 해당 조합원이 개인 정보의 유지를 요구한 경우

2. 조합과 해당 조합원이 개인 정보 유지에 명시적으로 동의하는 경우

3. 법률에 의해 개인 정보의 유지가 요구되는 기간

### 제3절 노동자 감시규제

제119조【감시장비】 회사는 조합 또는 조합원을 감시할 목적으로 컴퓨터, 전화, 비디오 카메라, 지문, 홍체, 정맥 등 생체인식기기 및 기타 정보통신·음향·영상기술을 이용하여 조합원의 이동, 작업과정을 기록·저장할 설비 및 소프트웨

어(이하 감시장비)를 설치하여서는 아니된다. 단, 노동안전, 도난 등 위험·사고방지를 위해 장비를 설치할 경우에는 다음 각호에 대해 조합과 사전합의하여야 하며 사용중에는 조합원에게 인지할 수 있는 조치를 취해야 한다.

1. 설치목적과 사용기간
2. 설치방법, 설치장소와 기록내용
3. 감시장비의 종류와 기술내용
4. 담당부서와 담당자

제120조【사생활 보호】회사는 화장실, 탈의실, 세면실, 휴게실, 기숙사 등 사생활을 침해할 수 있는 장소에 감시장비를 설치해 조합원의 사생활을 침해해서는 아니된다.

제121조【감시장비의 철거】회사는 조합과 사전합의없이 설치한 감시장비, 설치목적과 사용기간이 만료된 감시장비는 즉시 철거해야 하고 그 결과를 조합에 통보해야 한다.

제122조【기록물 관리】①회사는 감시장비에 의한 기록물(이하 '기록물')에 대해서는 다음 각호에 대해 사전에 조합과 합의해야 한다.

1. 보관기간
2. 처리 및 접근방법
3. 담당부서와 담당자

②회사는 기록물 관리를 위해 별도의 규정을 마련하고 그 내용에 대해 조합과 사전 협의하여야 한다.

③회사는 기록물을 담당부서와 담당자 외에는 어느 누구에게도 제공해서는 아니된다.

④회사는 감시장비에 의해 기록된 내용을 조합 또는 해당조합원이 열람을 요구할 경우 이에 따라야 한다.

제123조【기록물 수정과 폐기】① 회사는 조합 또는 조합원이 다음 각호의 경우에 대해 개인 정보의 수정, 폐기를 요구할 경우 이에 응해야 하며 그 결과를 통보해주어야 한다.

1. 조합과 합의없이 수집된 기록물

2. 사생활을 침해할 수 있는 기록물

3. 조작되었거나 사실과 다른 기록물

②회사는 기록물이 그 목적과 보관기간을 마쳤을 경우에는 복구할 수 없게 폐기하고 이를 조합에 통보하여야 한다. 단, 다음 각호의 경우는 제외한다.

1. 조합 또는 해당 조합원이 자료의 보관·유지를 요구할 경우

2. 조합 또는 해당 조합원의 명시적 동의가 있을 경우

3. 현재 법적 소송의 증거물로 요구되고 있는 경우

제124조【평가제한】회사는 감시장비에 의한 기록물의 내용을 인사고과에 반영해서는 아니된다.

## [부록5] 면접조사지

# 전자장비를 이용한 사업장 근로감독, 감시시스템이 노동자 인권에 미치는 영향 연구

본 조사는 국가인권위원회의 의뢰를 받아 한국노동사회연구소에서 실시하는 "전자장비를 이용한 사업장 근로감독, 감시시스템에 대한 연구"의 일환으로 진행되는 것입니다. 아래의 항목에 대하여 응답해 주시고, 관련된 참고자료가 있다면 제공해 주시기 바랍니다. 조사 결과는 연구의 목적으로만 이용할 것을 약속드립니다.

2005년 11월

(사) 한국노동사회연구소

주소 : 서울시 서대문구 충정로2가 69-18 석당빌딩 2층
담당 : 김현우 연구위원 (02-393-1459, nuovo90@hanmail.net)

<조사요령>

- 조사자는 아래의 체크리스트 항목에 따라 질의하고 응답지를 작성하세요.
- 사업장별로 노동자측과 관리자측 응답지 2세트를 작성하십시오.
- 응답자가 직접 기입을 원하거나 가능한 경우는 그렇게 하시고, 추가 면접을 통하여 응답지를 보충하여 작성해도 좋습니다.

조사자 : _____ 조사일시 : _____

사업장(주소) : _____

# [체크리스트]

**0. 응답자** (노동자 대표/ 사용자 대표)

1) 이름 :
2) 직위 :
3) 연락처 :
4) 참고사항 :

**1. 사업장 개요**

1) 창립 연도 :
2) 소재지 :
3) 종업원수 (정규직/비정규직, 성별) :

4) 주된 작업내용:
5) 업종 (제조업, 서비스업, 금융업, 보건의료 등) :
6) 작업과정에서 컴퓨터(pc) 사용 유무 :
7) 노사관계 :
   ① 노조 조직 유무(가입률, 상급단체) :
   ② 최근 노사관계(쟁의 경험) :
8) 감시시스템과 연관된 사업장 특성 (부품/정보/기술유출, 노조탄압, 경쟁압력 등) :

## 2. 전자장비 이용한 근로 감독,감시 시스템 운영 상황

1) 감시 시스템 종류 (대상 사업장에 존재하는 것 모두 기록)

(1) 인터넷 이용 체킹 시행 여부
① 기술적 방식 : 메신저, 메일, pc이용 원격감시(SMP Client류)
② 업무용 PC, 중앙네트워크 연결 유무
③ 이용 데이터 저장 여부 및 방식 (이용하는 원격 소프트웨어 종류)
④ 체킹 및 모니터링 사실 고지, 비고지

(2) 하드디스크 내용 모니터링 시행 여부
① 기술적 방식
② 모니터링 주기

(3) 전화 송수신 기록 시행 여부
① 기술적 방식
② 감시사실 고지, 비고지

(4) CCTV 설치 여부
① 설치장소와 숫자 (작업장/직원 생활공간/노조 업무 관련공간)
② 조망 범위(비율) 대상, 및 설치 위치, CCTV. 성능(기종, 모델)
③ 설치 사실 고지, 비고지

(5) 전자신분증 사용 여부
① 기술적 방식 : 바코드 카드, RFID 카드(칩), 생체인식 등
② 이용 데이터 저장 여부 및 방식
③ 카드의 경우 수록 정보 내용
④ 생체인식 경우 생체정보 제공 동의 여부

(6) ERP(전사적 자원관리) 사용 여부

① 기술적 방식

② 이용 데이터 저장 여부 및 방식

2) 도입 과정

① 도입 시기 (단계적, 도입 확대 과정 포함)

② 도입 이유 (논리 또는 계기)

<예시>

* 작업조직 통제 강화 -> 직무생산성 제고 위하여
* 기업/조직 정보유출 차단 및 기업재산 보호 위하여 (도난 방지 등)
* 작업장내 사고/산재 발생 예방을 위하여
* ICT(정보통신기술) 관련 설비의 사적 이용 방지를 위하여
* 해적판 S/W와 바이러스 및 시스템 기능 저하를 억제/차단키 위하여
* 근로자의 개별/집단적 저항행위 및 불법행위 규제를 위하여
* 업무실적 모니터링-보상/고객서비스/규칙준수/안전 연계를 위하여 등

③ 도입시 노-사간 고지 및 협의 여부

④ 도입으로 인한 갈등 발생 여부 및 내용

3) 운영 형태

(1) 관리, 감시시스템 적용 범위

① 전 사원 감시 / 일부 사원 감시

② 노조 관련 직원 등 특정 직원 대상 여부 (이유)

(2) 시스템 관리 주체 및 방식

① 관리 부서 (이유)

② 모니터링 또는 기록 방식 (자동/수동, 센서 등)

(3) 기록 보관 유무

① 보관 경우 보관 기간 및 방식 (백업 시스템 자동 기록 등)

② 보관 데이터의 활용 여부 (인사, 처우 등에 반영 여부)

(4) 시스템 운영에 관한 협의, 규정 존재 여부 및 내용

(5) 감시시스템 설치 및 운영 소요비용

**3. 시스템 설치의 영향**

1) 사업주(관리자)의 의견 및 제출 가능한 자료

2) 노동자의 의견 및 제출 가능한 자료

<예시>

* 긍정적 측면 : 생산성 향상, 보안성 향상, 관리비용 절감, 산업재해 감소, 인사평가 합리화 등

* 부정적 측면 : 인권침해, 노동통제 강화, 분위기 침체, 스트레스 강화, 노조활동 저해 등

3) 관리,감시 시스템으로 인한 노사간 갈등, 분쟁 발생 사례와 해결 여부

4) 관리,감시 시스템으로 인한 건강권 침해 사례

① 정신적 스트레스, 수치심 등 영향 여부

② 심각한 제보 사례 (산재인정 요청 등) 유무

(5) 관리, 감시 시스템에 대한 의견

① 사용자 고유권한으로 근로자가 뭐라 할 바 아니다?

② 경쟁력 확보와 관리 합리화 위해 도입과 사용이 불가피하다?

③ 현재의 시스템 도입말고 비슷한 효과를 거두기위한 대체수단은 없었다?

④ 관리,감시 시스템 운영 관련 협약이나 관련 제도가 존재할 필요가 있다?

**4. 기타**

① 향후 관리, 감시 시스템 개선방향에 대한 의견 (주관식)

② 연구진에게 하고 싶은 말

## [부록6] 설문지

| 응답자 ID | | | | |
|---|---|---|---|---|

# 전자기술사용과 인권에 관한 의견조사

안녕하십니까?

한국노동사회연구소에서는 국가인권위원회와 더불어 정보화시대의 직장사회에서 정보기술의 사용이 인권에 미치는 영향에 대한 의견조사를 실시하고 있습니다. 본 조사는 날로 증가하고 있는 전자기술의 사용이 근로현장에서 인권에 미치는 영향에 대한 기초 실태를 파악하기 위한 목적으로 시행되고 있습니다.

귀하의 의견은 연구를 위한 소중한 자료로 이용될 것이며, 통계법 제13조 개인의 비밀보호 조항에 의거 본 연구 이외의 목적으로는 절대 사용되지 않을 것이며, 응답 내용은 모두 통계적 수치로 처리될 것입니다.

시간을 내어 응답해 주시면 대단히 감사하겠습니다.

2005년 10월

한국노동사회연구소 · 국가인권위원회

* 조사와 관련된 문의나 확인은 한국노동사회연구소 김현우 연구위원(전화: 02-393-1457, e-mail: nuovo90@hanmail.net)로 해주십시오.

## I. 전자기술의 종류와 사용 실태에 관한 질문입니다.

1. 다음은 직장에서 이용되는 전자기술의 종류를 나열한 것입니다. 귀하의 직장에서 사용되고 있는 모든 전자기술의 사용 여부와 도입 시기에 관해 답해주십시오.

| | 사용 여부 | | | 도입 시기 |
|---|---|---|---|---|
| | ①사용함 | ②사용하지 않음 | ③모르겠음 | 전자기술이 도입된 시기 |
| 1-1. 인터넷 이용 모니터링 (웹사이트 접속, 메신저, 메일사용 체킹) | | | | _____년 전 |
| 1-2. 컴퓨터 하드디스크 내용 모니터링 | | | | _____년 전 |
| 1-3. 전화 송수신 내역 기록 | | | | _____년 전 |
| 1-4. CCTV (작업장, 생활공간 등 촬영) | | | | _____년 전 |
| 1-5. RFID(무선인식장치) | | | | _____년 전 |
| 1-6. 전자신분증(출입카드) | | | | _____년 전 |
| 1-7. 지문 및 생체인식 | | | | _____년 전 |
| 1-8. ERP(전사적 자원관리) | | | | _____년 전 |
| 1-9. 기타 ( ) | | | | _____년 전 |

2. 다음은 귀하의 직장에서 사용되고 있는 전자기술과 관련한 사항입니다. 각 항목에 답해 주세요.

| | ① 매우 잘 안다 | ②잘 아는 편 | ③잘 모른다 | ④ 거의 모른다 |
|---|---|---|---|---|
| 2-1. 귀하의 직장에서 사용되고 있는 전자기술의 구체적인 목적을 알고 계십니까? | | | | |
| 2-2. 귀하는 직장에서 사용되고 있는 전자기술로 어떤 정보가 수집되고 있는지 알고 계십니까? | | | | |
| 2-3. 귀하는 직장에서 사용되고 있는 전자기술로 수집된 정보가 회사 내에서 어떻게 활용되고 있는지 알고 계십니까? | | | | |

3. 귀하는 직장에서 사용되고 있는 전자기술이 노동자를 관찰, 감독, 감시할 목적으로 사용되고 있다고 보십니까? (  )

① 매우 그런 편이다  ② 어느 정도 그렇다

③ 별로 그렇지 않다  ④ 전혀 그렇지 않다  ⑤ 모르겠다

4. 귀하는 직장에서 전자감시기술로 인해 얼마나 자주 관찰, 감독, 감시당하고 있다고 생각하십니까? (  )

① 항상  ② 종종 ③ 이따금씩

④ 관찰당하고 있지 않다  ⑤ 모르겠다

5. 다음과 같은 각각의 전자기술이 노동자를 관찰, 감독하는데 사용될 경우 귀하에게 불안감을 주는 정도에 대해 답해주십시오.

| | 관찰, 감독, 감시에 따른 불안 정도 | | | | |
|---|---|---|---|---|---|
| | ① 매우큼 | ② 큰 편 | ③ 약간있음 | ④ 거의없음 | ⑤사용하고 있지 않음 |
| 5-1. 인터넷 이용 모니터링 (웹사이트 접속, 메신저, 메일사용 체킹) | | | | | |
| 5-2. 컴퓨터 하드디스크 내용 모니터링 | | | | | |
| 5-3. 전화 송수신 내역 기록 | | | | | |
| 5-4. CCTV (작업장, 생활공간 등 촬영) | | | | | |
| 5-5. RFID(무선인식장치) | | | | | |
| 5-6. 전자신분증(출입카드) | | | | | |
| 5-7. 지문 및 생체인식 | | | | | |
| 5-8. ERP(전사적 자원관리) | | | | | |

5-9. 기타(  )

## Ⅱ. 다음은 전자기술의 직장 설치 과정에 관한 질문입니다

**6. 귀하의 직장에 전자시스템이 설치된 주된 이유는 무엇이라고 생각하십니까? (  )**

① 생산성 향상을 위해

② 업무의 효율성을 위해

③ 노동자를 관찰, 감시하기 위해

④ 잘 모르겠다

⑤ 전자기술이 설치되지 않았다

**7. 직장에서 전자기술을 설치할 때 노동자 개인에게 고지나 안내가 있었습니까? (  )**

① 아무 말 없이 도입했다

② 설치 후 노동자에게 설치했다는 사실만 알려 주었다.

③ 노동자에게 설치여부와 함께 설치장소 및 활용 방안에 대해 알려 주었다.

④ 잘 모르겠다

**8. 직장에서 전자기술을 설치할 때 회사가 노동자의 대표인 노동조합이나 이에 상응하는 기구에 고지나 안내가 있었습니까? (  )**

① 아무 말 없이 도입했다

② 설치후 노조(노동자대표기구)에게 설치했다는 사실만 알려 주었다

③ 노조에 설치여부와 함께 설치장소 및 활용 방안에 대해 알려 주었다

④ 잘 모르겠다

**9. 전자기술을 설치할때 노동자나 노동자대표와 협의나 합의가 있었습니까? (  )**

① 있었다  ② 없었다  ③ 잘 모르겠다

10. 귀하는 직장의 전자기술 시스템 도입과 운영에 대해 노동자가 얼마나 참여해야 한다고 보십니까? (　　)

① 경영진의 고유권한이기 때문에 노동자가 관여할 필요가 없다
② 경영진이 감시시스템의 도입이나 설치시 최소한 설명은 해주어야 한다
③ 감시시스템이 운영되면 노동자의 직장생활에 영향을 미치기 때문에 적극적으로 참여해야 한다
④ 잘 모르겠다

## III. 다음은 직장에서 전자기술 사용에 따른 효과에 대한 질문입니다

11. 다음은 전자시스템을 사용함으로써 나올 수 있는 결과입니다. 각각의 결과에 대해 귀하는 어떻게 생각하십니까?

| | ① 매우 그렇다 | ② 약간 그렇다 | ③ 별로 그렇지 않다 | ④ 전혀 그렇지 않다 |
|---|---|---|---|---|
| 11-1. 생산성이 향상된다 | | | | |
| 11-2. 인사상의 불이익이 발생한다 | | | | |
| 11-3. 회사의 보안성이 향상된다 | | | | |
| 11-4. 노동통제가 강화된다 | | | | |
| 11-5. 업무효율성이 향상된다 | | | | |
| 11-6. 개인의 사생활이 침해된다 | | | | |
| 11-7. 회사의 관리비용이 절감된다 | | | | |
| 11-8. 안전향상, 산업재해 예방에 도움이 된다 | | | | |
| 11-9. 노사간 불신이 증대된다 | | | | |
| 11-10. 인사평가가 합리화된다 | | | | |
| 11-11. 건강악화를 가져온다 (스트레스, 불안증, 압박감 등) | | | | |
| 11-12. 노동조합 활동이 저해된다 | | | | |

**Ⅳ. 다음은 전자시스템을 이용하여, 노동자를 관찰, 감시하는 것에 대한 규제의 필요성과 대책에 관련된 문항입니다.**

12. 귀하께서는 인권침해를 방지하기 위해 헌법 17조에 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다”라고 명시한 것을 알고 계십니까? (  )

① 알고 있다 ② 모르고 있다

13. 귀하께서는 전자기술을 활용한 회사의 노동자 관찰/감시에 대해 규제가 있어야 한다고 보십니까? (  )

① 매우 필요하다 ② 약간 필요하다

③ 별로 필요하지 않다 ④ 전혀 필요하지 않다

14. 귀하는 회사가 전자기술을 통하여 노동자를 관찰 또는 감시하는 것을 규제하기 위한 제도적 장치가 필요하다고 보십니까? (  )

①그렇다 ②아니다

15. 귀하는 회사가 전자기술을 통하여 노동자를 관찰 또는 감시하는 것을 규제하는 제도나 규정이 다음의 각 수준에서 얼마나 필요하다고 보십니까?

| | ① 매우 필요하다 | ② 어느 정도 필요하다 | ③ 별로 필요하지 않다 | ④ 전혀 필요하지 않다 |
|---|---|---|---|---|
| 15-1. 정부 차원의 법안 | | | | |
| 15-2. 회사 내의 업무규정 | | | | |
| 15-3. 단체협약 등 노사간 합의문 | | | | |

16. 다음은 전자기술을 사용하여 노동자를 관찰, 감시하는 것과 관련하여 규정이 마련될 경우 포함될 수 있는 사항입니다. 귀하는 각각의 항목에 얼마나 동의하십니까?

| | ① 매우 그렇다 | ② 약간 그렇다 | ③ 별로 그렇지 않다 | ④ 거의 그렇지 않다 |
|---|---|---|---|---|
| 16-1. 회사는 전자감시기술을 이용해 노동자를 감시하고 있다는 사실을 알려주어야 한다 | | | | |
| 16-2. 회사는 특정 전자기술을 도입해야 하는 이 유에 대해 노동자에게 설명해 주어야 한다 | | | | |
| 16-3. 새로운 전자감시시스템의 도입이나 설치에 대해 노동자의 동의를 구해야 한다 | | | | |
| 16-4. 노동자는 도입 또는 설치된 전자시스템의 기술적 방법을 선택할 수 있어야 한다 | | | | |
| 16-5. 회사는 전자감시의 종류, 감시방법, 감시시기와 기간에 대해 설명해야 한다 | | | | |
| 16-6. 노동자는 전자감시 기록의 결과에 접근 가능해야 한다 | | | | |
| 16-7. 일과 관련되지 않은 장소에서의 전자감시가 있어서는 안 된다 | | | | |
| 16-8. 업무와 관련되지 않은 노동자의 정보에 대한 수집은 제한해야 한다 | | | | |
| 16-9. 부적절한 감시 자료나 자료의 해석에 대해 이의를 제기할수 있는 절차나 규정이 필요하다 | | | | |
| 16-10. 노동자의 동의를 받지 않고 개인정보를 유출하는 것을 방지해야 한다 | | | | |

17. 귀하가 일하고있는 직장의 경영진과 노동자의 상호신뢰는 어떠합니까? (  )

① 매우 신뢰하고 있다　② 신뢰하고 있는 편이다

③ 별로 신뢰하지 않는다　④ 거의 신뢰하지 않는다

## Ⅳ. 다음은 통계적 처리를 위한 문항입니다.

**18. 귀하의 성별은? (　　)**　① 남성　② 여성

**19. 귀하의 연령은?　만 (　　) 세**

**20. 귀하의 최종학력을 표기하여 주십시오. (최종학력이므로 중퇴는 이전 졸업단계에 표기하시면 됩니다) (　　)**

① 초등학교 졸업　② 중학교 졸업
③ 고등학교 졸업　④ 2년제 대학 졸업
⑤ 4년제 대학 졸업　⑥ 대학원(석사)졸업
⑦ 대학원(박사)졸업

**21. 귀하는 현재 어떤 고용형태로 일하고 계십니까? (　　)**

① 자가 경영　② 임금근로자 중 상용직 근로자(정규직근로자)

③ 임금근로자 중 임시, 일용, 시간제 등 비정규근로자
④ 무급 가족 종사자　⑤ 기타(　　)

**22. 귀하가 일을 해서 버는 월평균 소득은 얼마나 되십니까? (　　)**

① 50만원 미만　② 50~100만원 미만
③ 100~150만원 미만　④ 150~200만원 미만
⑤ 200~300만원 미만　⑥ 300~400만원 미만
⑦ 400~500만원 미만　⑧ 500만원 이상

**23. 귀하의 현재 직장 근속 년수는? (　　) 년**

24. 귀하는 현재 노동조합에 가입해 있습니까? (  )

① 가입했다  ② 가입하지 않았다  ③ 노동조합이 없다

24-1. 노동조합에 가입하신 경우 노조 간부이십니까? (  )

① 노조간부이다  ② 평조합원이다

25. 귀하가 현재 다니고 있는 직장의 종업원 총수는 얼마나 됩니까? (  )

① 1인-49인  ② 50-99인  ③ 100-299인
④ 300-499인  ⑤ 500-999인  ⑥1000인 이상

26. 귀하는 다음 중 어떤 직업에 종사하고 계십니까? (  )

① 의회의원, 고위임직원 및 관리자  ② 전문가
③ 기술공 및 준전문가  ④ 사무 종사  ⑤ 서비스 종사
⑥ 판매 종사  ⑦ 농업, 임업 및 어업  ⑧ 장치, 기계조작/조립
⑨ 단순 노무  ⑩ 기타 (  )

27. 귀하가 하는 일은 어느 업종에 해당합니까? (  )

① 제조업  ② 서비스업  ③ 금융업  ④ 공공부문
⑤ 기타 (  )

**- 성실히 답변해 주셔서 감사합니다 -**