직장내 모니터링 행위에 관한 법률문제와 제도 개선방안

주임연구원 강 준 모*

최근 회사의 영업비밀 내지 중요정보의 보호 등을 이유로 근로자에 대한 전자적 모니터링을 행하는 사례가 대기업을 중심으로 많아지고 있다. 그러나 이러한 전자적 모니터링은 현행법에 의하면 위법일 가능성이 높으나 이에 대한 명확한 법적인 판단이나 사례가 아직은 축적되지 않은 상태이며, 실제적으로 이를 규율하는 법률이나 제도가 우리나라에서는 전무하다고 할 수 있다. 이에 해외 여러 나라의 법제동향을 비교검토하고 우리나라의 입장에서 어떠한 방법으로 근로자에 대한 모니터링 행위를 합법적으로 인정하고, 이에 상응하는 근로자의 권리를 어떻게 부여할 것인가에 대해 살펴본다.

목 차

Ⅰ. 서 론
Ⅱ. 본 론
1. 직장 내 모니터링 행위 유형
2. 작업장 감시에 관한 통계
3. 각국의 관련 입법활동 및 관련 판례 등
Ⅲ. 우리 나라의 대응방안
1. 작업장과 관련한 프라이버시 관련 우리 나라 관련법 현황
2. 모니터링에 관한 법적 문제점
3. 관련법 제정의 방향

Ⅰ. 서 론

최근 회사기밀 유출방지 등을 명분으로 국내 기업들은 사내 직원에 대한 이메일 모니터링을 강화하는 등 직·간접으로 회사의 이익을 보호하기 위한 대책을 강구하고 있다. 이와 관련하여 최근 2002년 3월경 S사는 최근 회사의 주요 현안사항을 외부에 유출했다는 이유로 직원 3명을 해고한 바 있으며, 이에 해고된 직원들은 불법적으로 개인의 이메일을 검열했다는 이유로 이메일 내용을 지득한 관련자들을 고발하여 관련자들이 구속된 바 있다. 이외에도 지난 '98년에는 반도체 설계도면과 회로도 등 기밀자료를 복제하는 방식으로 64메가D램 핵심기

연락처: *정보사회연구실 (02) 570-4307, coolday@kisdi.re.kr

술을 대만 업체에 팔아넘긴 회사의 전·현직 연구원들이 구속되기도 하였으며 이외 경영실적·매출현황 등 경영기밀을 증권사에 유출한 혐의로 직원이 구속되어 자체 사내 통신보안 활동을 강화하는 기업도 늘어나고 있다. 이러한 모니터링 행위를 긍정적으로 평가하는 입장에서는 해당직원에 대한 모니터링과 보상행위를 연계함에 용이하고, 모니터링을 통한 고객서비스의 향상 및 노동자의 안전을 증대시킬 목적으로 전자적 감시·감독을 정당화 시킨다. 반면 모니터링 행위를 부정하는 입장에서는 피감시자가 모니터링 행위를 인지하지 못한 상황에서 획득된 자료가 자신의 직무평가의 자료로 사용될 수 있다는 잠재적 위험성을 들어 모니터링 행위를 비난하고 있다. 기술한 사례에서 보듯이 회사들은 사내의 중요한 정보나 영업비밀의 누출을 방지하기 위한 사내보안활동을 한층 강화하고 있으며 이외에도 ① 기업의 품위와 이미지 보호, ② 피용자의 생산성 유지, ③ e-메일 등을 통한 性的 및 다른 불법적인 행위방지 및 억제(명예훼손, cyber-stalking 포함), ④ 기타 지적재산권 침해(불법 소프트웨어 복제방지 등)를 미연한 방지하기 위해 모니터링을 할 유인이 발생한다. 문제는 이러한 제한적이고 정당한 목적 하에서 수행되는 모니터링 행위에 비례해서 근로자의 프라이버시 침해의 가능성도 그만큼 증대되고 있어 양자간 권리충돌을 합리적으로 조절하기 위한 제도적 장치가 마련되어 있어야 하나 외국의 사례와 비교해서 우리나라의 경우 이러한 제도적 장치가 거의 전무한 상황이며 이에 대한 기업과 근로자의 의식이 이제 싹터가고 있는 실정이다.

이러한 모니터링 행위가 가져오는 법적인 문제는 헌법상 기본권의 충돌이며, 이를 어떻게 해결하고 조절해야 하는가가 판단되어져야 한다. 사업주의 입장에서는 기술한 모니터링 행위의 유인에 따라 정당한 관점에서 재산권을 보호하거나, 예측가능하지 않은 손해배상 청구 등으로부터 자유로워지고 싶은 의지가 있는 반면 근로자의 입장에서는 사업주가 언급하는 정당하고 제한적으로 모니터링 행위가 이루어지더라도 결국 본인의 동의를 구하지 않은 이러한 행위는 명예훼손 내지 프라이버시권을 침해한다고 주장하게 된다. 결국 사업주의 재산권과 근로자의 프라이버시권이 충돌하는 기본권 충돌이 발생하는데 이를 합리적인 관점에서 해결하는 방안을 찾아야 할 것이다. 본론에서는 직장 내에서 행해지고 있는 모니터링 행위 유형과 외국에서 파악된 직장 내 모니터링의 통계 및 각국의 입법 내지 판례 사례를 본다. 이후 결론에서 우리나라에 있어 직장 내 모니터링에 관한 현 법률상의 문제점과 이러한 현상을 개선하기 위한 입법방향을 살펴보기로 한다.

Ⅱ. 본 론

1. 직장 내 모니터링 행위 유형

흔히 직장 내 모니터링 행위의 유형은 문서처리량, 회사資源(resource)의 사용, 컴퓨팅(Computing) 시간, 전화사용 횟수, 대화내용, 서비스태도, 도청행위(eavesdropping) 등을 들 수 있으며, 이와 같은 모니터링을 하기 위해 위치확인 카드, 호출기, CCTV 등이 이용되기도 한다.[1] 특히 정보사회가 도래하면서 근로환경이 점차 네트워크화·정보화되어 감에 따라 직무와 직·간접으로 관련된 근로자의 모든 행위는 관리자가 마음만 먹으면 언제든지 파악이 가능한 상황에 도달하게 되었다. 또한 매체에 따른 모니터링 행위의 유형을 나누자면 크게 컴퓨터 관련 사용감시와 전화·CCTV 등을 통한 감시로 나눌 수 있다.

문제는 특히 정보기술적 측면에서 사용되는 기계들의 특성상 일대일의 '통신'의 개념에 포함되는 것이 많아서 기업의 입장에서는 이러한 기계들을 이용한 근로자의 각종행위를 모니터링하는 데는 실정법적 한계를 가지게 된다. 이러한 통신의 개념에 해당되는 모니터링 대상유형은 'e메일(e-mail)', '인스턴트 메시징(instant-messaging)', '전화(Telephone)', 등인데 이러한 유형의 모니터링은 "통신비밀보호"의 적용을 받아 사업자가 처벌될 가능성이 높다. 이외 이러한 컴퓨터 관련 정보통신기기 외에 CCTV 등 출입보안시스템[2]에 의한 모니터링도 들 수 있는데, 특히 CCTV에 의한 감시유형은 통신비밀에 해당하는 것이 아니라 법적으로는 초상권의 보호라는 개념으로 보호될 수 있을 것이다.[3] 다만 작업장 내에서 인터넷 "로깅(logging)"에 대해서는 이를 통신의 개념으로 볼 수 있다하더라도 사업자는 근로자가 특정 웹페이지(web page)에 접속했다는 기록만을 보여주는 데이터를 볼 뿐이므로 내용을 지

1) 고영삼, 작업장 감시와 개인정보 프라이버시 보호대책, 2001.8.참조. 특히 인터넷 사용과 관련된 모니터링으로 인터넷 사용현황 실시간 모니터링/사내직원의 인터넷 이용 통계 리포팅/증권, 신문, 도박, 섹스 사이트 등에 대한 접근 감시/유출되는 메일 실시간 모니터링/직원들이 송/수신하는 모든 전자우편에 대한 사본유지/자동적으로 네트워크 사용자 정보수집/다양한 옵션으로 특정 전자우편만 실시간 모니터링/관리자 프로그램을 통한 원격 동작 감시/인터넷 접속 제한기능/다양한 차단 메시지를 통한 그룹별 차등정책 적용/시간별 차단·감시 정책적용 및 시간별 사용기록 YES/NO 정책적용/그룹별로 카테고리·차단시간대 지정을 통하여 얼마든지 근로자를 통제할 수 있다.

2) 홍채인식, 지문인식, 정맥인식 등 생체적 특성을 이용한 출입보안시스템을 들 수 있다.

3) 주 3)의 출입보안시스템을 위해 근로자의 홍채 등의 모양을 회사가 요구할 때 단순히 근로계약에 기초해서 이를 근로자가 제공해야만 하는 가는 법적으로 문제가 될 수 있다.

득해야하는 통신비밀의 보호와는 다른 법리구성이 필요하다고 보아진다.

또한 정의의 개념으로 주의할 것은 '직장'의 한계와 범위이다. 과거 산업사회 시절의 제조업 중심의 작업장의 개념은 물리적·지리적으로 획정되던 개념이지만 현재 정보화 시대의 산업환경은 정보통신기기를 중심으로 한 '원격근무'의 형태가 보편화되어가는 과정으로 볼 수 있으므로 직장의 개념을 물리적·지리적으로 개념을 제한할 것이 아니라 근로자가 정보통신기기를 통하여 근무와 관련된 접속을 하는 등 근로와 연속된 선상에서의 공간은 모두 직장으로 인정하는 보다 광의의 개념으로서 직장정의가 필요하다 할 것이다. 다만 이와 관련한 법률이 신설된다는 가정을 전제로 감시요건의 위반으로 인한 처벌조항이 생긴다면 보다 작업장의 정의가 보다 정교하고 세분화되어져야 함은 말할 필요도 없다.

2. 작업장 감시에 관한 통계

가. 미국 e메일 감시 조사통계

1977년 이후 미국 주요 기업을 대상으로 작업장 감시를 조사해온 AMA(American Management Association)는 2001년 조사에서, 미국 주요기업의 77.7%가 업무 수행 중 종업원

〈표 1〉 미국 경영자협회의 조사결과[4)]

종 류	1997	1998	1999	2000	2001
전화통화 기록/리뷰	10.4	11.2	10.6	11.5	11.9
음성메일 메시지의 축적/리뷰	5.3	5.3	5.8	6.8	7.8
컴퓨터 파일의 축적/리뷰	13.7	19.6	21.4	30.8	36.1
에메일 메시지의 축적/리뷰	14.9	20.2	27.0	38.1	46.5
모니터링 인터넷 결합				54.1	62.8
CCTV로 종업원 작업 감시	15.7	15.5	16.1	14.6	15.2
커뮤니케이션과 업무수행에 대한 적극적 모니터링의 총계	35.3	42.7	45.1		
- 인터넷 모니터링을 포함한 계				73.5	77.7
- 인터넷 모니터링을 제외한 계				66.2	70.8
전화사용(시간/횟수)	34.4	40.2	38.6	44.0	43.3
컴퓨터 사용(로그온 시간/keystroke 횟수 등)	16.1	15.9	15.2	19.4	18.9
보안목적으로 비디오 감시	33.7	32.7	32.8	35.3	37.7
전자모니터링(감시)의 모든 총계	63.4	67.1	67.3		
- 인터넷 모니터링 포함한 계				78.4	82.2
- 인터넷 모니터링 제외한 계				73.4	77.1

4) 출처: AMA, http://www.amanet.org

의 전화사용, 이메일, 인터넷 서핑, 그리고 컴퓨터 파일 등 일반 커뮤니케이션과 행동을 기록하고 점검하는 것으로 밝힌바 있다.

이외 Privacy Foundation이라는 곳에서 2001년 7월 미국 및 전 세계 온라인 노동자 중 모니터링을 받는 작업자를 조사 연구한바 가 있다. 〈표 2〉에서 보듯이 미국의 경우 온라인 노동자 전체의 35%(1천4백만명), 전 세계의 경우 27%(2천7백만명)가 현재 온라인 감시 하에 있는 것으로 나타나고 있다.

〈표 2〉 지속적으로 온라인 감시하에 있는 노동자 수[5)]

구 분	전체노동자 수	온라인 노동자	모니터링 받는 작업자 (온라인 노동자의 비율)
미 국	1억4천	4천만	1천4백만(35%)
전세계	3억	1억	2천7백만(27%)

한편 Privacy Foundation에서는 작업장에서의 모니터링을 이메일 모니터링과 인터넷 모니터링으로 구분하여 조사하였는바 〈표 3〉과 같다.

〈표 3〉 인터넷 모니터링과 이메일 모니터링 수

구 분	온라인 작업자수	이메일 모니터링	인터넷 모니터링
미 국	4천만	625만(15%)	775만(19%)
전세계	1억	1천2백만(12%)	1천5백만(15%)

나. 우리나라의 전자적 모니터링 실태조사

우리나라의 경우 아직 체계적으로 자세하게 조사된 바는 없지만, 최근 모 포털사이트가 직장인을 대상으로 조사한 바에 따르면, 직장인 10명중 4명은 자신이 다니는 직장에서 상사나 회사로부터 인터넷 사용을 감시당하고 있다는 결과가 나왔다. 이 설문조사에서는 직장인 3만 7천660명을 대상으로 인터넷 설문조사를 실시하였는데, 응답자의 40.3%가 직장에서 인스턴트 메신저나 e-메일 사용이 자유롭지 못하다고 답했으며, 최근 인터넷상에서 실시간 의사소

5) 출처: Privacy Foundation, 2001; Nielsen//NetRatings; U.S. Bureau of Labor Statistics; International Labour Organization

통의 수단으로 급부상하고 있는 메신저의 사용을 자제하라는 회사 측의 경고를 받거나 아예 봉쇄당하고 있다는 직장인이 20.0%에 달한 것으로 나타났다. 또한 8.7%가 회사 인터넷으로는 특정 사이트에 접속할 수 없다고 답했고, 로그파일(log file)분석을 통해 자신이 방문했던 인터넷사이트 내역이 체크되고 있다는 대답이 7.6%, e-메일이 상사에게 보고되거나 감청당하고 있다는 응답자도 4.1%에 달했다. 반면 인터넷 사용에 아무 제약이 없다는 응답은 46.5%로 나타나[6] 약 절반 정도의 직장인이 사실상 전자적 모니터링을 당하고 있다는 사실을 알 수 있다.

이외에 1999년 한국노총과 민주노총에 가입한 전 사업장의 노동조합들을 모집단으로 각 산별연맹을 가입 조합수에 따라 분류한 후 가중치를 두어 연맹별로 150개를 무작위로 표집, 총 300개의 표본을 대상으로 조사한 바에 따르면,[7] 조사대상 108개 사업체 가운데 63%인 68개 사업장이 컴퓨터 네트워킹 시스템을 구축한 것으로 나타났고, 이러한 시스템을 통해 작업지시와 통제가 이루어지는 곳이 무려 81%에 달한다는 것을 밝히고 있다. 또한 이러한 시스템을 이용해 노동자의 작업상황 내지 결과를 수집, 저장, 기록하고 있는 곳도 50여곳에 달해 이미 정보기술을 적용한 생산인프라를 구축한 대부분의(82.3%) 사업체들에서 노동력 관리의 주요한 장치로 정보기술을 활용하고 있음을 알 수 있다.[8]

〈표 4〉 네트워킹 컴퓨터의 도입유무와 이용실태

	네트워크로 연결된 컴퓨터	컴퓨터를 이용한 작업지시	작업상황 및 결과의 기록・저장
Yes	63.0(68)	50.9(55)	51.9(56)
No	15.7	18.5	8.3
Missing	21.3	30.6	39.9
※ ( )안의 숫자는 해당되는 사례 숫자임			

이러한 컴퓨터 관련 모니터링 행위 이외에도 최근 CCTV를 통한 모니터링 행위가 증대되고 있다. 컴퓨터를 통한 감시의 방식이 주로 디지털화된 텍스트들의 분류 및 재배치에 의하

6) 본 설문조사에서 '어느 정도 수준의 감시가 프라이버시 침해인가'라는 설문조사에서는 응답자의 68.2%가 회사의 인터넷 사용 내역이나 e-메일 감시, 특정 사이트 접근 차단이 프라이버시 침해라고 답했다. "직장인 40% 인터넷사용 감시당한다", 중앙일보 2002. 8. 25자 기사 참고.

7) 권순원, 전자・정보적 감시와 노동통제, 민주사회를 위한 변호사모임 토론회 발표자료. 1999. 4. 7면 참고. 조사방법은 우편조사와 면접조사를 병행하였으나 대부분이 우편으로 조사된 관계로 회수율이 저조하여 총 108개의 설문지만 수거된 것으로 적고 있다.

8) 권순원, 앞의 보고서 7~8면 참고.

여 이루어지는 반면 CCTV를 이용한 방식은 동작이나 작업수행에 대한 무매개적이고, 직접적인 감시라는 점, '지배자 없는 지배', '감시자 없는 감시'의 효과가 시스템의 효과로서 극대화된다는 점, 나아가 감시의 효과가 중단없이 지속될 수 있는 점 등에서 통제의 자동장치라 할 수 있다.[9] 위의 사례조사와 병행하여 CCTV에 대한 설문조사도 1999년에 진행되었는데, 조사대상 사업체 가운데 CCTV를 도입한 사업체가 37.1%에 달하고 있으며, 최근 5년 이내 CCTV가 도입된 경우가 5년 이상된 사업체가 CCTV를 도입하는 비율에 약 3배에 달하고 있다는 점에서 CCTV에 의한 모니터링 행위가 급속하게 확산될 것으로 예측된다.

〈표 5〉 CCTV의 도입유무와 이용실태

CCTV 설치현황		CCTV 도입시기	
있다	371.(40)	5년 이내	18.6(20)
없다	58.3	5년 이상	7.4
Missing	4.6	Missing	74.0
※ ( )안의 숫자는 해당되는 사례 숫자임. (%/108 Case)			

〈표 6〉 CCTV 설치장소별 분류

CCTV 설치장소	
작업공간과 작업공간 밖 모두에 설치	27.5(11)
작업공간에만 설치	37.5(15)
작업공간 밖(휴게소, 화장실 등)에만 설치	35.0(14)
※ ( )안의 숫자는 해당되는 사례 숫자임. (%/40Case)	

〈표 7〉 CCTV 녹화내용 보관여부

CCTV 녹화내용 보관여부	
보관하고 있다	42.5(17)
보관하고 있지 않다	0.8(3)
모르겠다	40.0(16)
Missing	1.0(4)
※ ( )안의 숫자는 해당되는 사례 숫자임. (%/40Case)	

9) 권순원, 앞의 보고서, 9면 참조.

3. 각국의 관련 입법활동 및 관련 판례 등

가. 영 국

영국의 경우 2000년 8월에 통과된 '조사권한규제법(Regulation of Investigatory Powers Act 2000)'에 의하면 고용주가 그러한 통신의 송신자와 수신자 양쪽의 동의를 구하지 않고 전화와 e메일을 감청하는 경우 위법이라고 규정하고 있다. 그러나 동법의 4절 (2)의 Telecommunications (Lawful Business Practice) (Interception of Communication) Regulation 2000 의하면 ① 사업과 관련된 사실존재를 입증하거나(establishing the existence of facts relevant to the business), ② 관련 규제 혹은 자율규제 관행과 절차에 따르는 것을 확인하거나(ascertain compliance with relevant regulatory or self-regulatory practices and procedures), ③ 피용자에 의해 제시된 표준을 확인하기 위해서(ascertain the standards achieved by employees), ④ 범죄를 예방하거나 탐지하기 위해서(prevent or detect crime), ⑤ 전기통신시스템의 허가받지 않은 사용을 조사하거나 탐지하기 위해서(investigate or detect unauthorised use of the telecommunications system), ⑥ 시스템의 보안과 효과적인 운용을 확보(ensure the system}s security and effective operation)하기 위해서 고용주가 피용자의 동의를 구하지 않고 모니터링을 하거나 통신을 녹음할 수 있음을 밝히고 있다.

이외에도 작업장내 프라이버시 보호와 관련한 법률로 데이터보호법(The Data Protection Act 1998)이 있으며, 영국정보보호위원회(The Office of the Data Protection Commissioner)에서는 고용주와 종업원의 관계에서 개인정보이용에 관한 실무규정 초안(Code of Practice on workplace privacy)을 만들어 협의 중에 있다. 이 실무규정의 주요 내용으로 ① 고용주는 개인정부 수집에 있어서 정당한 사유와 분명한 목적 하에서만 수집하고 사전에 종업원에서 알리고 동의를 구해야 하고, ② 종업원은 고용주가 자신의 데이터를 보유하고 있는 것의 데이터 내용, 용도, 의도를 정기적으로 통보 받아야 하며(복사본), ③ 특별히 민감한 데이터는 해당법의 특별한 통제를 받는다(정치적 성향, 종교, 성생활, 민감한 건강 데이터 등). 또한 ④ 종업원의 범죄기록, 유전자 검사는 특별한 제한을 두며, ⑤ 작업장 감시는 정당한 사유를 가지고 사전에 통보하며 감시장치는 눈에 보이는 곳에 설치할 것 등에 대해서 규정하고 있다.

나. 미 국

미국의 경우 이에 관한 판례와 관련 법률의 제정활동이 가장 많은 나라이다. 미국의 연방 및 주헌법이 보장하고 있는 프라이버시권은 정부행위(state action)에 의한 침해를 전제로

하기 때문에 사적인 분야(private sector)에 대해서는 원칙적으로 적용되지 않는다. 이와 관련하여 연방 및 주법률 중 e메일 검색과 관련된 연방법으로는 1986년에 제정된 Electronic Communication Privacy Act가 있다. 이 법률은 전자통신의 도청을 금지하는 법으로 해석상 e메일에 적용되기는 하자 직장에서 고용주가 하는 e메일 검색행위에 적용될 수 있는 지는 논란이 되고 있다.[10] 이외 connecticut주의 EMAUP(Electronic Mail Acceptable Use Policy) 등 주차원이 활동이 일부 있으며, 의회에 상정된 법률안으로서Notice of Electronic Monitoring Act(NEMA), The Electronic Communications Privacy Act of 2000, 1993년 부결된 the Privacy for consumers and Workers Act(PCWA) 등이 작업장 프라이버시보호와 관련해서 언급되고 있다.

미국에서 Common Law의 관점에서는 고용주의 피용자에 대한 e메일 감시행위로 인한 불법행위책임을 묻기 위해서는 일정한 요건을 충족하여야 한다. 이를 위해서는 ① 피용자가 회사의 컴퓨터를 이용해서 송수신하는 e메일의 내용에 관한 프라이버시가 보호될 것이라는 합리적인 기대(reasonable expectation)가 있어야 하며, ② 가해자(고용주)의 행위가 고의에 의한 정신적 가해행위(intentional infliction of emotional distress)여야 하고, ③ 고용주의 행위가 극단적으로 비난받아야 할 행위(extreme and outrageous conduct)라야 불법행위책임을 고용주에게 물을 수 있다.

이러한 미국의 입법적 태도와 동시에 전자적 모니터링에 관한 판례는 다수 있어 왔다. 전자적 모니터링에 관한 직접 판례는 아니지만 피용자의 개인소유의 사물함에 관한 회사의 검색행위에 대한 피용자의 프라이버시를 인정한 K-Mart Corp. Store No. 7441 v. Trotti 사례가 있으나, 전자적 모니터링의 법적논리구조와는 다른 양상을 보이는 사례이다. 캘리포니아주에서 어떤 피용자가 타 직원에게 업무에 관계없는 性的인(sexual) e메일을 보내는 등 근무태만을 이유로 해고당하자 고용주를 상대로 헌법상의 프라이버시 권리침해를 이유로 소송을 제기한 사례가 있었다.[11] 본 사건에서 캘리포니아 지방 및 고등법원은 '헌법이 보장하는 개인의 프라이버시권은 각 개인이 보호받을 수 있는 프라이버시가 객관적으로 타당하게 기대되는(objectively reasonable expectation of privacy) 경우에만 존재한다'고 판시하여 원고의 訴를 기각하였다. 이외에도 Smyth v. Pillsbury Co 판결(1996), McLaren v. Microsoft Corp 판결(1999), Simmons v. Southwestern Bell Telephone Co 판결(1979), Bohach v.

10) 그러나 본 법률에서 ①기계제공자에 대한 예외, ②일반적 기업행위에 대한 예외, ③피도청자의 동의에 대한 예외 등을 규정하고 있어 직장내 프라이버시 보호를 위한 문제해결에는 도움을 주지 못한다.

11) Bourke v. Nissan Motor Corp.

City of Reno 판결(1996) 등이 있으나 대부분 피용자의 프라이버시에 대한 합리적 기대가 있다고 보기 힘들다고 판단하여 고용주의 손을 들어준 바 있다.

다. 일 본

일본의 경우 '노동자의개인정보보호에관한행동지침'에서 사업장에서 전자적 방식의 모니터링에 관한 기준을 제시하고 있다. 동지침 제2장 개인정보의 처리에 관한 원칙 중 제6조 특정한 수집방법에서 이를 규율하고 있는데 동조 4항은 사용자가 직장에서 노동자에 관한 비디오카메라, 컴퓨터 등에 의한 모니터링을 행하는 경우에, 노동자에 대해 실시사유, 실시시간대, 수집된 정보내용 등을 사전에 통지하여야 한다고 규정하고 있다. 다만 법령에 정한 경우 내지 범죄 기타 중요한 부정행위가 있을 것이라는 충분하고 상당한 이유가 있을 때는 사전통지를 하지 않아도 된다. 또한 동조 5항에서는 직장에 있어서 작업장에 대해 상시 모니터링을 행하는 것은 노동자의 건강 및 안정의 확보와 업무상 재산보전에 필요한 경우에 한하여 인용된다고 규정하고 있으며, 6항에서는 사용자는 원칙적으로 개인정보의 컴퓨터 등에 의한 자동처리 또는 비디오 등에 의한 모니터링의 결과에 기인하여 노동자에 대한 평가 또는 雇用上의 결정을 행하여서는 안된다고 규정하고 있다.

이외에도 일본의 경우에는 작업장 프라이버시 보호에 관한 법률제정의 움직임은 아직 없으나 과거 작업장과 관련하여 사용자가 무단히 도청한 사례에 대해서 프라이버시 침해로서 불법행위에 해당한다고 판시한 사례[12]가 다수 있다.

라. 프랑스/이탈리아

프랑스의 경우 국민헌장 9조는 사업장에서의 개인의 프라이버시를 보호하도록 규정하고 있으며 1991년 통신비밀법에 의하면, 고용주는 신의성실에 기한 도청 내지 사법부의 영장에 의하지 않고는 여하한 경우라도 작업장에서 피용자의 개인적인 통신에 접근할 수 없음을 규정하고 있다.[13] 또한 프랑스 노동법 L. 121-8조에 의하면 고용주는 피용자에게 고지하지 않고

12) 岡山電氣軌道事件(岡山地判 平3.12.17 勞判606號 50頁)은 노조활동의 정보수집을 위하여 종업원휴게실에 도청기를 설치하였던 것으로 직장내의 사적 영역이라고 할 수 있는 장소에서 이루어지는 종업원의 대화를 엿듣는 것은 프라이버시침해로서의 불법행위에 해당한다고 판시하고 있다. 또한 目黑高校事件(東京地判 昭47.3.31.勞民集 23卷 2號 155頁)은 학교장이 4개월간에 걸쳐서 고등학교의 종교론수업 전체를 무단으로 녹음하였던 사례이며, 光澤自動車學校事件(德島地決 昭61.11.17 勞判488號 46頁)은 운전지도원의 교육훈련을 위하여 교습차에 녹음기를 설치하여 운전지도원과 교습생간의 대화를 녹취했던 사례이다. 특히 본 판례에서는 사용자의 녹취행위가 직무와 관련된 경우라 하더라도 당해 근로자의 동의 없이 녹음한 경우에는 위법이라고 판시하고 있어 작업장 프라이버시에 관한 일본의 법감정을 간접적으로 보여주고 있다.

서는 피용자와 관련된 개인적 정보를 수집할 수 없음을 규정하고 있는데 이는 고용주에 의해 설치된 감시장치의 존재를 반드시 피용자에게 고지하여야 한다는 것을 의미한다. 이외 작업장 프라이버시 보호와 관련한 Neocel 사례[Cass. Soc. 20/11/91(RDS 1992(2), 77)/에서 국민헌장은 피용자에 대한 은밀한 감시를 제한한다고 언급하고 있으며, 최근 Nikon France 사건에서 프랑스 대법원은 피용자는 존중되어야 하는 그만의 프라이버시권을 가지고 있으며 이것은 곧 고용주는 피용자에 의해 송수신된 개인적 메시지의 내용에 접근할 수 없다고 판시한 바 있다.

이탈리아의 경우 피용자의 e메일 메시지에 고용주가 접근하기 위해서는 사법부의 명령이 요구된다. 물론 이탈리아 헌법 제15조는 여하한 형태의 통신과 우편은 비밀의 자유를 가진다고 보장하고 있으며 이탈리아 정보보호위원회는 e메일 감시에 관해 고용주의 장치를 이용하는 제한적 접근이 허용되는 뉴스그룹과 메일링 리스트를 통해 순환되는 전자적 메시지는 사적 우편으로 고려되어져야 하고 고용주에 의해 접근되어서는 안된다는 의견을 제시하고 있다.

마. 노동관련 국제단체의 기준

국제노동기구(ILO)에서의 노동자의 프라이버시 문제에 대한 논의는 주로 개인정보 보호라는 차원에서 진행되어 관련된 몇몇 결의안이 제출된 바 있다. 1988년 제75차 ILO 총회에서 ILO 사무총장은 인권보고서에서 노동자들에 대한 감시행위의 기준설정이 문제화 될 것임을 우려한 바 있으며, 노동자의 프라이버시와 관련 국제적으로 공인된 원칙은 1996년 ILO에서 발표한 고용주의 프라이버시 침해로부터 노동자를 보호하기 위한 권리보호 규약이 유일하다고 할 수 있다. 세부적인 내용으로 ① 고용주는 노동자에 관한 정보를 반드시 작업과 관련된 범주에서 본인으로부터 직접 취득해야 함, ② 고용주는 노동자의 성생활이나 정치, 종교적 신념에 관한 정보를 취득하려 해서는 안됨, ③ 노동자는 프라이버시에 관한 권리를 포기하지 말아야 함, ④ 노동자에 대한 마약 복용 여부 검사는 반드시 법률 규정에 따라야 하며 자의적 검사는 허용되지 않음, ⑤ 고용주가 특정 노동자를 감시할 경우 본인에게 그 사유와 방법, 시간 등을 통보해야 하며, 비밀 감시는 형사범죄 용의자에게만 해당됨, ⑥ 의료상 비밀 사항에 해당되는 개인 정보는 다른 인사 정보와 분리돼 안전하게 보관돼야 함 등이 그것이다.

이외 국제노동조합(International Confederation of Free Trade Unions)의 경우 1987년 제73차 국제노동회의에 제출된 결의문에서 피용자들에 대한 모니터링은 피용자들의 프라이버

13) 신의성실에 대한 프랑스 정보보호위원회의 해석은 e메일의 내용을 읽지 못한다는 것이지, 첨부된 문서의 형태와 동시에 그 메시지의 크기 등을 모니터링하는 것은 허용된다고 한다.

시·존엄·독립을 위협하는 것이므로 금지되어야 한다고 강조한 바 있으며, FIET(the International Federation of Commercial, Clerical, Professional and Technical Employees)가 주최한 1985년 인사정보 수집 및 처리시스템에 관한 국제노동조합회의는 인사정보의 수집 및 처리시스템에 관한 국제노동조합의 지침을 채택한 바 있다. 이의 주요한 내용으로는 ① 개별 피용자들의 작업수행이나 작업장에서의 행동을 모니터링하고 기록하는 행위와 자동적으로 수집된 자료를 고용에 대한 결정의 근거로서 사용하는 것을 금함, ② 자료수집의 방법을 피용자에게 고지하고 동의를 받아야 함, ③ 전화모니터링시스템을 불허함, ④ 개인신분증, 뱃지의 사용은 엄밀하게 정의되고 동의된 보안상의 필요에 국한됨 등이다.

Ⅲ. 우리 나라의 대응방안

1. 작업장과 관련한 프라이버시 관련 우리 나라 관련법 현황

먼저 프라이버시와 관련한 가장 상위법으로서는 헌법을 들 수 있다. 동법 제17조에서 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다고 규정하고 있으며 이를 사생활 보호권이라 해석하고 있는데, 넓게 보아 초상권과 명예권도 여기에 포함되므로 CCTV에 의한 무단감시행위도 헌법 제17조의 위반행위가 될 수 있다. 또한 동법 제18조에서는 모든 국민은 통신의 비밀을 침해받지 아니한다고 규정하고 있어 본 조항은 의사소통에 관한 프라이버시 보호조항이라 말할 수 있다. 여기서 말하는 "통신"은 면대면 커뮤니케이션에서부터 전신, 우편, 전화, 컴퓨터 통신, 一對多 통신 등 모든 형태의 커뮤니케이션을 포함하는 의사소통 일반이라고 이해해야 할 것이며 본 조항에 따라 통신에 해당하는 모든 유형의 근로자 행위에 대한 사용자의 감시행위는 불법이라고 해석할 수 있다.

다음으로 중요한 법률로서는 통신비밀보호법이 있다. 동법 적용대상은 형법 등 10개 법률 130여종의 범죄에 관한 것으로 감청범위는 유선전화(통화내용의 지득·채록, 송수신방해, 실시간 착발신 번호추적 등), 이동전화(실시간 착발신 번호추적, 음성사서함 비밀번호), 무선호출(실시간 착발신 번호추적, 음성사서함 비밀번호), PC 통신(발신 e메일 내용의 지득·채록, 수신 e메일 내용은 일부 사업자만 가능) 등이 포함된다. 따라서 사업장(작업장) 내에서의 이메일 감시행위는 동법 제2조 7호에 의한 감청행위로 간주되어 동법 제16조에 따라 7년 이하의 징역에 처해질 수 있다.

이외에도 프라이버시 보호와는 직접관련이 없지만 기업의 영업이익 등 중요정보를 보호하기 위한 사후 보완적 의미로서의 법률로 부정경쟁방지및영업비밀보호에관한법률(제10조 내

지 제14조, 제18조 제1항・제2항(처벌관련))이 있으며,[14] 전자거래기본법(제13조, 영업비밀 보호),[15] 정보통신망이용촉진및정보보호등에관한법률(제51조, 중요정보의 국외유출제한 등)[16] 등이 있다. 이러한 법률의 의미는 작업장내 프라이버시 보호와는 별개의 문제로서 실제적으로 중요 정보의 유출자체를 처벌하기 위한 것으로 이해해야 할 것이다.

2. 모니터링에 관한 법적 문제점

작업장에서의 프라이버시 보호의 문제는 기본적으로 개인의 프라이버시권(헌법 제17조 내지 제18조)과 국민(기업)의 재산권 보장(동법 제23조)과의 충돌문제(기본권 충돌의 문제)이다. 기본권 충돌의 경우 上位기본권 우선원칙, 同位기본권 상충시에는 인격권 내지 자유권이 우선(법익형량의 방법)되며, 형평성의 원칙, 규범영역의 분석, 수인한도 이론을 통해 해결한다. 프라이버시권과 재산권보호 양쪽 모두를 만족시키는 합리적인 방안은 상호수인한도 내에서 기본권의 침해를 받아들이는 방법을 택해야 할 것인데, 고용자는 피고용자에게 사전에 감시/감독의 방법, 범위, 수집된 정보의 사용범위 등에 대해 명확하게 고지하며 피고용자는 이러한 범위 내에서 감시/감독행위를 수인하는 형태가 되어야 한다.

감시유형별로 살펴보면 전화, e메일 모니터링의 경우 사용자에 의한 근로자의 전화나 전자메일의 모니터링의 경우 사용자가 업무상의 전화나 메일에 한하지 않고 근로자의 사적인 것에 대한 모니터링까지도 허용되는가 여부가 문제될 수 있다. 사용자는 근로자가 회사소유의 통신설비를 이용하여 사적인 통화 또는 메일의 송수신을 한다는 것을 이유로 당연히 그것을 모니터링 하여도 된다고 해석해서는 안된다고 해석될 가능성이 크다. 왜냐하면 사용자가 근로자에 의한 당해 통신시설의 사용을 허가하고 또는 묵인하는 한에서 근로자는 그것을 통해서 교류하는 사적인 통신에 있어서 프라이버시의 이익을 가고 있기 때문이다.[17] 사용자가 만일 모니터링를 통해서 얻은 개인정보를 근로자의 동의 없이 그 목적 이외에 이용하고, 또는

14) 본 법률의 영업비밀 누설에 관한 처벌조항은 사후손해에 대한 복구를 규정한 법률이며, 사업자의 모니터링과 직접 관련된 법률은 아니다. 영업비밀을 누설한 자에 대해서는 최고 7년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 규정하고 있다.

15) 전자거래이용자의 영업비밀에 관한 전자거래사업자의 영업비밀준수의무를 부과하고 있다. 그러나 이의 위반에 대한 처벌사항은 없다.

16) 정보통신부장관은 국내의 산업・경제 및 과학기술 등에 관한 중요정보가 정보통신망을 통하여 국외로 유출되는 것을 방지하기 위하여 정보통신서비스제공자 또는 이용자에 대하여 필요한 조치를 강구하게 할 수 있다.

17) 강희원, 첨단 정보과학기술시대에 있어서 노동관찰 및 감시의 노동법적 문제, 디지털경제시대를 위한 노동법 및 사회보장법적 과제, 디지털경제법제⑦, 한국법제연구원, 2001. 7. 21면 참조.

제3자에게 開示하면 모니터링 행위문제와는 별도로 사용자는 프라이버시 침해의 법적 책임을 질 수도 있다.

CCTV에 의한 모니터링의 경우 사용자가 근로자의 직무수행과 관계없이 이른바 몰래카메라에 의하여 근로자를 관찰하거나 감시하는 경우는 어떠한 경우에도 위법하다고 해석될 수 있다. 이러한 경우에는 그러한 모니터링이 근로자의 프라이버시(특히 초상권) 또는 인격권의 침해에 해당될 수 도 있다. 다만 보안 및 그 사용을 필요로 하는 구체적이고 합리적인 이유가 있는 한도 내에서의 공개적인 CCTV의 이용은 위법하지 않다고 해석되어야 할 것이다.

컴퓨터 네트워크에 기반한 모니터링의 경우, 작업과정에서 이것을 당하는 근로자는 전혀 감지할 수도 없으며, 컴퓨터가 대상에 관계없이 무차별적으로 계속적 자동적으로 근로자의 직무수행상태를 보다 상세히 관찰하고 기록하여 엄청난 정보가 체계적으로 집적된다. 이러한 컴퓨터 네트워크에 의한 모니터링은 그 자체로서 규제되어야 할 것이나 이에 대해서 우리나라에서는 이 문제에 대한 법적 논의가 전혀 이루어지지 않고 있다. 근로자에게 과도한 스트레스를 주는 감시방법 내지 수단의 도입에 있어서는 그 사정을 사전에 당해 근로자에게 설명한 다음에 근로자와의 충분한 협의를 거쳐서 합리적인 범위 내에서만 인정되어야 할 것이다. 충분한 협의 없이 이루어지는 컴퓨터 네트워크 시스템에 의한 감시는 일응 사용자의 노무지휘권의 행사의 일환으로 해석되기 보다는 근로자의 인격권의 침해행위에 해당한다고 해석해야 할 것이다.[18]

3. 관련법 제정의 방향

작업장에서의 전자적 감시·감독에 관한 이해조율 방법은 크게 새로운 법률을 제정하거나 기존의 법률을 개정하는 방법 그리고 단체협약 등 사용자와 노동자의 계약방식을 통한 통제방법 등 크게 두 가지로 구분하여 볼 수 있다. 첫 번째 방식은 작업장에 한정하는 프라이버시 보호에 관한 법률을 만드는 것인데, 작업장이라는 특수한 환경만을 고려하여 세분화된 법률을 만들 수 있다는 장점이 있을 수 있으나 현재 프라이버시 일반에 대한 관련법이 전무한 상황에서 사업장이라는 특수한 환경만을 고려하여 일반화되지 못한 법률을 제정한다는 비판을 받을 수 있다. 첫 번째 방법에서도 기존의 법률을 개정하는 방법, 즉 헌법의 하위법률로서 노동 관련법, 특히 근로기준법에 사업장에서의 프라이버시에 관한 추상적인 조항을 신설하는 방안도 고려할 수 있다. 이 방법은 다만 그 규정 내용이 새로운 법률의 제정보다는 구체적이지 않은 방법이 되어 프라이버시 침해에 관한 구체적인 기준과 판단은 노동관련 기관 및 법

18) 강희원, 앞의 논문 23면 참조.

원을 통하여 구하여야 할 것이다.

두 번째 방식은 작업장 내 프라이버시 보호를 법률이라는 규범에서 찾기보다 계약법적으로 해결하는 방법이다. 즉, 근로자가 취업계약을 체결할 시 회사와 근로자간 계약을 통해서 그 간섭한계를 설정하고 이를 상호간에 준수하는 방법이다. 물론 이 방법은 협상력의 차이에서 오는 불공정한 계약체결로 인한 근로자의 무한한 위험감수를 요구할 수도 있는 방법이므로 근로자 입장에서는 보다 확고한 보장방법으로 법률이라는 제도화를 요구하겠지만 법률의 제·개정 이전의 과도기적 방법으로는 권장할 만하다 하겠다. 구체적으로는 고용계약 체결보다는 노동조합과 회사간의 단체협약에 프라이버시 보호라는 조항을 신설하여 이를 규정하면 기존의 근로자뿐만 아니라 새롭게 채용되는 근로자에게도 적용될 수 있을 것이다. 다만 이 방법은 해당회사의 노동조합의 협상력의 정도에 따라 결정될 수 있어 균등한 보호의 정도가 전영역의 사업장에 적용되지 않는다는 단점이 존재한다.

결론적으로 사업주가 정당하게 근로자의 행동을 전자적으로 모니터링하기 위해서 기본적으로 사업주가 모니터링의 범위와 수단 그리고 관련정보의 사용범위 등에 대해 사전에 근로자에게 고지하여야 한다는 점이 가장 중요하다 하겠다. 현재 사업장에서 취하여 지고 있는 전자적 모니터링은 그 수단(media)의 다양성과 타법과의 관계로 인해 현행 법체계로는 근로자의 효과적인 프라이버시 보호를 기대할 수 없는 상황이다. 따라서 강력한 규범력을 바탕으로 하는 관련 법률의 입법추진을 통해 사업주와 근로자간의 이해를 조정할 필요가 있다. 특히 프라이버시 침해로 피해를 입은 근로자는 민법상 손해배상(750조)만을 청구할 수밖에 없다. 또한 통신비밀보호법에서는 전화, PC통신을 보호대상으로 할 뿐이어서 CCTV나 기타 지문, 홍채인식행위 등에 대해서 규율하지 못하므로 이런 모니터링 수단을 포괄하는 법률이 필요한 시점이라 하겠다. 만일 법률을 제정하게 된다면 고려해야 할 사항으로는 ① '사업장'과 '전자적 감독'의 범위,[19] ② 전자적 감독매체 도입에 대한 동의여부와 고지,[20] ③ 정보의 근로자 열람권 보장 및 정보이용범위의 제한,[21] ④ 수집된 기록의 관리 등에 관한 사항,[22] ⑤ 근로자

19) 사업장의 개념이 과거 일정한 물리적 공간에 한정되던 것이 정보화 진전에 따라 정보통신기기를 이용하는 여하한 곳도 사업장이 될 수 있다는 가정 하에서 전향적으로 판단해야 할 것이다. 이외 전자적 감독에 사용되는 매체의 종류와 기술적 발전가능성을 감안하여 매체의 기술중립적인 조항이 필요할 것이라 판단된다.

20) 일부 국가(스웨덴, 노르웨이)의 경우 회사에 전자적 감독매체를 도입하는 경우 허가를 받게 하고 있으며, 허가시스템이 아니라 하더라도 노사협의체에서 이를 도입함에 있어 동의를 전제요건으로 하는 경우도 있다.

21) 정보주체로서 개인(근로자)에 대한 해당정보의 열람권을 회사만이 독점하지 말고 해당 근로자에게도 열람권을 부여할 것인가를 결정해야 한다. 이에 대해 미국에서 제안된 일부 주법과 연방

의 동의없이 모니터링이 가능한 예외사항 규정,[23] ⑥ 본 법률에 위반하는 행위에 대한 처벌과 손해배상권의 명시[24] 등이 될 것이다. 이를 위해서 위에서 언급한 프라이버시 보호방안에 대한 여러 논의 외에도 현재 여러 사업장 내에서의 감시행위에 관한 실태조사가 병행되어 기초자료가 축적되고 이를 바탕으로 위의 보호방안 중 가장 최적의 방안, 즉 재산권 보호와 프라이버시권 보호라는 두 가지 축의 절묘한 조화를 형성할 수 있는 방법으로 제도개선이 이루어져야 할 것이다.

참 고 문 헌

[1] 강희원, 첨단 정보과학기술시대에 있어서 노동관찰 및 감시의 노동법적 문제, 디지털경제시대를 위한 노동법 및 사회보장법적 과제, 디지털경제법제⑦, 한국법제연구원, 2001. 7.
[2] 고영삼, 작업장 감시와 개인정보 프라이버시 보호대책, 2001. 8.
[3] 권순원, 전자·정보적 감시와 노동통제, 민주사회를 위한 변호사모임 토론회 발표자료. 1999. 4.

법에서는 근로자가 정보에 대한 열람권을 가지지 못함을 규정하고 있음은 주목할 만 하다. 이외 수집된 정보를 목적범위 내에서만 이용하고 이외의 사항에 대해 회사측이 자의적으로 사용하지 못하게 금지하는 등 모니터링의 부수물인 정보의 이용에 관한 명확한 사용범위의 한계를 설정해야 할 것이다.

22) 수집된 정보의 보관기관 및 방법, 처리 및 폐기근거 및 방법, 책임부서와 담당자, 해당정보의 수정에 관한 사항을 명시해야 한다.

23) 위법행위에 연관된 근로자의 모니터링에 있어 위법의 한계와 범위에 대해 명확한 기준설정이 필요하다.

24) 수집된 정보를 목적범위외 사용하거나 동의된 매체외 다른 수단으로 정보를 수집하는 행위, 수집된 정보의 유출 등에 대해서 형벌을 부과하는 규정을 제정해야 할 것이며, 이와는 별도로 위법행위로 피해를 입은 근로자에 대한 위자료 형식의 손해배상청구가 용이하도록 규정을 제정해야 할 것이다.