노 동 정 책 연 구
2005. 제5권 제4호 pp.135~192


연 구 논 문

# 사업장내 전자우편감시제도에 관한 연구

## (Study on E-mail Surveillance in the Workplace)

이 창 범*

인터넷, PC 등 정보통신기기의 보급 확대로 기업 정보화가 가속화됨에 따라 근로조건과 환경에도 많은 변화가 일고 있다. 정보통신기기의 활용으로 업무의 효율성과 편의성은 크게 증대하였으나 근무시간 중 근로자들이 사적인 전자우편 또는 메신저 활동에 보내는 시간이 점점 많아지게 되고, 때에 따라서는 기업내 비밀정보가 전자우편 등을 통해 외부로 유출되는 사고도 발생하고 있다. 이에 따라 많은 사용자들이 근로자들의 온라인 활동을 감시해야 할 필요성을 느끼고 있지만 근로자의 사생활 침해에 대한 논란 때문에 섣불리 나서지 못하고 있다. 그러는 사이 일부 사업장에서는 불법을 무릅쓰고 비밀리에 또는 공공연히 근로자의 온라인 활동을 무절제하게 감시하고 있는 실정이다. 따라서 작업장에서 근로자의 온라인 활동을 합법적으로 감시할 수 있는 합리적인 기준의 설정이 절실히 요구되고 있다. 본고는 먼저 국내외 입법과 판례 분석을 통해 근로자 감시의 이론적 근거의 제시와 함께 감시의 한계를 밝히고, 이를 바탕으로 전자우편 감시를 위한 기준을 제시하는 것을 그 목적으로 한다. 본고에 제시된 가이드라인은 RFID, 스마트카드, CCTV 등을 통한 근로자 감시에도 활용될 수 있을 것이다.

핵심용어 : 전자우편감시, 영업비밀보호, 근로자개인정보, 근로자프라이버시, 사용자의 감독권

투고일 : 2005년 8월 29일, 심사의뢰일 : 8월 30일, 심사완료일 : 10월 4일
* 개인정보분쟁조정위원회 사무국장, 한국소비자교육지원센터 이사, 법학박사
(happyday@kisa.or.kr)

# Ⅰ. 전자우편감시와 근로자 프라이버시

## 1. 전자우편감시의 의의

전자우편감시라 함은 통상 인터넷, 인스턴트 메신저, PC통신, 인트라넷 등을 통한 전자적인 메시지의 전송내용, 전송횟수, 전송시기, 작성시간, 송수신자 등을 모니터링하고 분석·보고·기록하는 일체의 행위를 말한다. 지난 2003년「노동자감시 근절을 위한 시민연대」가 전국 207개 사업장의 노동조합간부 또는 시스템담당직원을 대상으로 조사한 결과에 따르면, 89.9%에 이르는 사업장에서 노동자감시가 이루어지고 있는 것으로 나타났으며, 특히 41.5%의 사업장에서 인터넷 감시가 행해지고 있는 것으로 나타났다.[1)]

한편, 미국경영자협회(America Management Association)의 2000년 자료에 따르면, 미국 주요기업의 73.5%가 근로자의 전자우편을 감청하고 있으며, 특히 AMA 회원사 중에서는 88%가 통신감청에 관한 회사정책을 근로자에게 고지하고 있는 것으로 나타났다.[2)] 일본도 사정은 비슷하다. 니혼게이자이 신문이 2002년 150개 제조업체를 대상으로 조사하여 발표한 자료에 따르면, 42%가 사원들의 전자우편을 감시하고 있고, 38%가 전자메일의 감시를 검토중이거나 도입할 예정인 것으로 나타났다.[3)]

이와 같이 직장 내에서 행해지고 있는 사용자에 의한 근로자의 전자우편 이용감시는 기업의 영업비밀보호, 근로자의 비행방지, 통신설비의 오·남용 방지 및 사적이용의 통제, 노동생산성 향상 등을 위한 근로감시의 한 형태로 볼 수 있으나, 사용자가 반드시 그러한 목적만으로 이용하지 않고 근로자에 대한 해

1) 노동자감시 근절을 위한 연대모임,「2003 노동자감시 실태조사 결과 보고서」(www.nodong.org).
2) AMA, *2001 AMA Survey Workplace Monitoring & Surveillance*, New York (http://www.amanet.org/research/specials/elecmont.htm).
3) 부산타임즈, 2002.08.20. (www.inews.org/Snews/section.php?Domain=dsnb&SeqCode=35&Ho=8854).

고의 근거확보, 불만불평세력의 색출, 근로자의 동태감시, 노동조합활동 감시 등 근로자의 권리를 침해하고 위협하는 목적으로 사용될 수도 있다는 데 문제가 있다.

이 경우 근로자에 대한 사용자의 지시·감독권과 근로자의 프라이버시권이 상호 충돌하는 결과를 가져오게 되어 노사간 분쟁이 발생하게 된다. 사용자의 입장에서도 현행 통신비밀보호법상 정당성을 구비하지 못한 전자우편 감시를 통해 수집된 자료는 해고의 증거로 사용하기 어렵다. 따라서 사용자의 지시·감독권과 근로자의 프라이버시권이 서로 존중되는 가운데 전자우편 감시가 적법하고 평화적으로 행해질 수 있도록 명확한 기준의 제시가 필요하다.

## 2. 전자우편감시의 목적

### 가. 산업정보의 유출 방지

최근 기업간 기술경쟁의 격화, 인재 스카우트로 인한 이직·전직의 일반화, 아웃소싱, 고용불안과 이로 인한 평생직장 개념의 변화 등으로 노사간 신뢰관계가 무너지고 회사에 대한 임직원의 충성심도 점차 떨어지고 있다. 따라서 재취업과 신분상승 그리고 일확천금을 노린 임직원들에 의한 기업정보 유출이 빈번해지고 있다.

정보유출은 종이복사, 팩스, 도청이나 도촬, 디스켓 복제, CD·USB 복제 등에 의해서도 이루어지지만, 전자우편을 이용할 경우 훨씬 더 간편하고 신속한 정보유출이 가능하다. 특히 최근에는 전자우편에 의해 전송할 수 있는 정보의 양이 갈수록 확대되고 있고, 그림·사진·동영상·음성 등 모든 형태의 정보 전송이 가능하도록 전자우편의 성능이 개량되고 있어 대량의 설계정보도 순식간에 유출이 가능하다.

이러한 정보유출은 대개 임직원에 의해 의도적으로 이루어지지만, 경우에 따라서는 회사동료·친구·가족들과 주고받는 전자우편상에서 무의식중에 실수나 부주의에 의해서도 이루어질 수 있다. 사소한 것이라도 기업정보의 유출은 회사의 존망을 좌우할 수 있기 때문에 기업정보의 유출 방지를 목적으로 행하는 전자우편 감시는 기업의 자위행위로서 불가피한 조치라고 보아야 할 것이다.

### 나. 통신설비의 사적이용 통제

컴퓨터, 인터넷 등 정보통신기술의 발달과 보급 확대로 업무의 효율성이 크게 향상되고 노동생산성이 높아지게 되었다. 신속한 업무처리를 위해 대다수 회사들이 근로자들에게 컴퓨터와 전자우편계정을 무료로 배급하고 있다. 이와 같은 컴퓨터와 전자우편계정은 비록 근로자가 개인적으로 사용하고 있다고 하더라도 그 소유는 전적으로 회사소유이다. 그러므로 근로자는 원칙적으로 회사의 업무가 아닌 사적인 업무를 위해 회사의 재산을 이용해서는 안 된다.

그러나 회사 재산의 사적 이용보다 더 심각한 것은 근로자들이 사적인 전자우편을 송·수신하기 위해 낭비하는 시간이다. 최근 인재파견회사인 보보스(www.boboslink.com)가 대기업과 중소기업에 재직중인 우리나라 직장인 603명을 대상으로 조사한 결과에 따르면, 남녀 모두 하루 2시간 이상을 업무와 관련 없는 일에 낭비하고 있으며, 특히 다수 응답자(남자 27.7%, 여자 32.2%)가 사적인 인터넷 활동에 시간을 허비하고 있는 것으로 나타났다.[4)]

이러한 현실에서 사용자가 근로자의 전자우편, 메신저, 채팅 등의 활동을 어느 정도 감시하고 규제하는 것은 불가피하다. 사용자가 집단적인 노동력을 효율적으로 서로 연계하면서 합리적으로 통제하여 저항력을 감소시키고 노동생산성을 높이기 위한 수단으로 사용하는 것이 바로 노동관찰과 감시이다.

### 다. 근로자의 각종 비행 예방

전자우편은 오늘날 정보전달 및 의사표현 수단으로서 핵심적인 위치를 차지하고 있다. 이것은 근로자들의 직장생활에 있어서도 마찬가지이다. 그러나 일부 근로자들은 회사에서 배급한 전자우편계정을 이용하여 헛소문을 퍼뜨리거나 회사·동료·상사 등의 명예와 신용을 훼손하는 데 사용하기도 한다. 전자우편을 통해 이성 동료를 성희롱하거나 스토킹하기도 하며, 사진을 공개하겠다고 협박하기도 한다. 그 결과 직장 분위기가 어수선하고 동료들간 불필요한 오해를 낳기도 하며, 그것이 생산성 저하로 이어지기도 한다.

미국에서는 직장 내에서 근로자간에 행해지는 성희롱, 성차별 또는 인종차별

4) 매일경제신문 2004.5.19 1쪽; 경향신문 2004.5.20 22쪽.

적 언행, 명예훼손 등에 대해서 이른바 '적대적 작업환경'(a hostile work environment) 법리에 따라 사용자가 법적인 책임을 지는 경우가 많다. 이 때문에 한국과 일본의 사용자들이 기업정보유출 방지를 이유로 주로 근로자의 전자우편 감시를 행하는 것과는 달리, 미국의 사용자들은 전자우편 감시의 이유를 기업의 법적 책임회피 및 노동생산성 향상에서 찾는다.

우리나라에서도 노동법상 사용자는 근로자에게 임금지급의무 외에 근로자의 생명·신체·건강을 안전하게 보호할 안전배려의무를 부담하는 것으로 이해되고 있다. 근로자가 제공하는 노동력은 근로자의 인격권과 분리할 수 없는 관계를 이루고 있기 때문에 사용자는 자신의 지배하에 들어온 근로자의 생명·신체·건강에 대하여 적절한 조치를 강구할 의무를 진다. 이러한 안전배려의무는 근로자가 사용자의 경영체 또는 사업장 내에 현실적으로 편입됨으로써 발생되는 반사적 법률효과라고 볼 수 있다.[5]

이 경우 사용자의 안전배려의무는 근로자의 생명·신체·건강을 침해해서는 안 된다고 하는 소극적 의무뿐만 아니라 예견되는 위험으로부터 근로자를 안전하게 보호하기 위해 적절한 조치를 강구해야 하는 적극적인 의무도 포함된다. 그 밖에 근로자의 인격이 침해되지 않도록 배려해야 하는 것도 안전배려의무의 내용을 구성한다.[6] 따라서 우리나라에서도 근로자간에 행해지는 성차별, 성희롱, 스토킹, 명예훼손, 사생활침해 등이 근로자에 대한 사용자의 안전배려의무 위반을 구성할 가능성이 없지 아니하다.

이 밖에 근로자가 사용자의 전자우편시스템을 이용하여 해킹·바이러스 프로그램을 유포하거나 스팸메일을 전송하여 제3자에게 피해를 입힌 경우 또는 저작권법에 의해 보호받는 타인의 저작물(소프트웨어, 콘텐츠 등)을 무단으로 전송한 경우 사용자는 근로자의 행위에 대하여 책임을 져야 할 경우가 생길 수 있다.

---

5) 김형배, 『노동법』, 2002, 242쪽.

6) 이희성, 「직장내에서의 전자메일 및 CCTV의 감시와 근로자의 프라이버시보호」, 개인정보분쟁조정위원회 워크숍 자료(2002.10.17), 14쪽; Zöllner/Loritz, *Arbeitsrecht*, 5. Aufl., 1998, S.204f; Dütz, *Arbeitsrecht*, 1990, Rdn. 180 ; Söllner, *Grundriβ des Arbeitsrechts*, 10. Aufl., 1990, S.269.

## 3. 사용자의 감독권과 근로자 프라이버시권의 충돌

### 가. 직장에서의 근로자 프라이버시권

근로계약의 체결에 의하여 근로자는 사용자에게 노무급부의무를 부담하고 사용자의 지시·감독권에 복종하게 되지만, 그렇다고 해서 직장 내에서 인간으로서 기본적으로 누려야 할 프라이버시권까지 포기한 것은 아니다. 근로자가 출근과 동시에 자신의 모든 프라이버시를 포기했다고 생각하는 것은 일반의 상식에 반하기 때문이다. 근로자는 인간관계의 상당부분을 직장 내에서 발전시키므로 일정 수준 사생활 보호에 대한 합법적인 기대를 가진다고 보아야 한다.[7] 따라서 프라이버시 보호에 대한 근로자의 합리적인 기대는 직장 내에서도 존중되고 보호되어야 한다.

최근 정보통신기술의 발달로 근로자들의 작업환경이 크게 바뀐 것이 사실이고 그만큼 사용자들이 신경을 쓰고 책임져야 할 일들이 많아진 것도 사실이다. 통신근무(telework, u-work)의 확산도 그 중 하나이다. 그러나 근로자는 온라인으로 일을 하든지 오프라인으로 일을 하든지 같은 권리를 누릴 권리가 있다. 특히 최근의 업무조건은 전문적인 직업일수록 근무시간과 개인적인 생활의 분명한 구분이 점차 어렵게 되어가고 있다.

따라서 근로자가 회사소유의 통신설비를 이용하여 사적인 전자우편을 송·수신한다고 하여도 그것을 이유로 사용자가 당연히 근로자의 전자우편을 감시해도 좋다는 것을 의미하는 것은 아니다. 왜냐하면 사용자가 근로자에게 당해 통신시설의 사용을 허가하고 또는 묵인하는 한에 있어서 근로자는 그곳을 통해서 교류하는 사적인 통신에 대해서 프라이버시의 기대를 가지고 있기 때문이다. 전화도청과 마찬가지로 사용자가 근로자의 사적인 전자우편의 내용을 무단으로 모니터링하는 것은 프라이버시의 침해에 해당한다고 하여야 한다.

업무상의 이유라고 하더라도 사용자가 모든 전자우편의 내용을 무단으로 모니터링하는 것은 근로자의 프라이버시 침해를 야기할 수 있다. 사용자는 미리

---

7) EU Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace*, 2002.5.29, p.4.

근로자의 동의를 받거나 사전에 그러한 취지를 근로자에게 통지할 필요가 있다. 또한 근로자의 사전 동의를 받았다고 해서 모든 전자우편 감시가 정당화되는 것도 아니다. 사용자와 근로자의 관계에서는 동의의 자발성이 담보되기 어렵기 때문이다. 따라서 객관적으로 감시의 필요성이 있어야 하고 감시의 방법·절차 및 정도가 적정하여야 한다.

하지만, 근로자의 프라이버시권도 사용자의 합법적인 권리, 즉 시설관리권(Ownership Rights)과 지시·감독권(Right of Direction and Control)[8]－영업비밀의 유출로부터 자신의 재산을 보호할 권리, 자신의 사업을 효율적으로 운영할 권리, 근로자의 비행이 야기할 수 있는 책임과 위해로부터 자신을 보호할 권리 등－에 의하여 제약을 받는다. 근로자의 프라이버시권은 사용자의 권리와 균형을 이룰 때에만 보호받을 수 있다.

### 나. 근로자 감독권의 내용과 한계

사용자와 근로자의 관계는 당사자간에 체결되는 근로계약에 의해서 구체화된다. 근로계약이 체결되면 근로자는 사용자에 대하여 크게 근로제공의무와 그 밖의 부수적 의무를 지게 된다. 근로를 제공해야 할 주된 의무 외에 근로자가 부담해야 할 부수적인 의무로는 업무전념(업무충실)의무, 비밀유지의무, 겸업금지의무, 고지의무, 뇌물을 받지 않을 의무 등이 있다.

사용자는 일정한 범위 내에서 지시·감독권을 가지고 근로자에 대하여 노무급부의무의 실현을 일방적으로 지시할 수 있다. 근로계약은 노무의 급부를 목적으로 하는 계속적 계약이고 당사자 쌍방이 근로의 내용을 일일이 계약에 구체화할 수도 없기 때문에 근로자가 근로계약에 의해 제공해야 할 근로의무는 추상적이고 개괄적일 수밖에 없다. 따라서 근로의무의 내용을 구체화하기 위하여 사용자의 지시·감독권은 근로관계에 있어서 필수적이다.[9]

근로계약에서는 근로자의 일반적인 노무급부의 종류만이 결정되기 때문에 근로자가 취업상태에서 이행하여야 할 작업의 내용·장소·시간 등은 근로계약

8) 사용자의 시설관리권과 지시·감독권은 영미법계에서도 널리 인정되고 있다. Charles Morgan, “Employer Monitoring of Employee Electronic Mail and Internet Use”, *McGill Law Journal,* Vol.44, 1999, pp.889~890.

9) 김형배, 앞의 책, 126쪽; 이병태, 『최신 노동법』, 2003, 778쪽.

의 범위 내에서 근로기준법·단체협약·취업규칙·경영관행 등에 기초해서 사용자에 의하여 다시 구체적으로 확정된다. 이러한 사용자의 지시·감독권의 법적 근거에 대해서는 견해가 일치하지 않고 있으나 지배적인 견해는 채권적 급부의 내용을 일방이 결정할 수 있도록 규정하고 있는 법률의 조항(독일 민법 제315조)을 원용하고 있다.[10]

근로자는 사용자의 지시·감독권에 복종할 의무와 업무에 전념할 의무(업무충실의무)[11]를 부담한다. 근로자가 이를 위반할 경우에는 징계의 사유가 된다. 더욱이 사용자의 업무지시에 대하여 정당한 이유 없이 불복하여 직장규율 및 경영질서를 문란하게 하고 근로계약관계의 신뢰를 상실하게 한 것이라고 인정되는 경우에는 해고의 정당한 사유가 될 수 있다.[12]

따라서 사용자가 지시·감독권 실행의 한 방법으로서 기업비밀 보호, 생산성 향상, 법과 규칙의 준수, 고객서비스 향상 등을 목적으로 하여 일반적으로 허용되는 방법과 절차로 전자우편을 감시하고 있다면 근로자는 이를 감수해야 할 것이다. 일반적으로 허용될 수 있는 감시인지의 여부는 다음 사항을 고려해서 판단해야 한다. 첫째, 감시활동이 근로자에게 투명한가? 둘째, 감시가 꼭 필요한가? 즉 사용자는 전통적인 방법으로는 감시와 같은 결과(효과)를 얻을 수 없는가? 셋째, 제안된 감시활동의 내용이 근로자에게 공정한가? 마지막으로 감시활동이 관련된 여러 사항들과 균형적인가?[13]

예를 들어 사용자가 단순히 근로자들의 동태를 파악하려는 목적으로 은밀하게 전자우편을 감시하는 행위는 지시·감독권의 이름으로도 허용되지 않는다고 보아야 한다. 전자우편 감시가 사용자의 이익을 추구하는 데 편리하다고 하는 단순한 사실만으로 근로자의 사생활 침해가 정당화될 수는 없다. 또한 부당한 목적으로 모니터링하는 것은 허용되지 않으며, 특단의 사정이 없는 한 특정의 근로자만을 상대로 한 차별적인 모니터링도 허용되지 않는다. 모니터링을 통해서 획득한 정보를 근로자의 동의없이 그 목적 이외에 이용하거나 제3자에게 개시하는 것도 감독권의 남용이다. 업무상의 전자우편이 아닌, 근로자의 사적인

10) 이희성, 앞의 논문, 13쪽.
11) Charles Morgan, 앞의 논문, 889쪽.
12) 김형배, 앞의 책, 126쪽; 이희성, 앞의 논문, 13쪽.
13) EU Data Protection Working Party, 앞의 보고서, 4쪽.

우편을 모니터링할 때에는 더욱더 주의해야 한다.

## Ⅱ. 전자우편감시 규제에 관한 해외의 법정책 동향

### 1. 국제기구

#### 가. ILO(국제노동기구)

ILO는 근로자의 개인정보보호에 관한 구체적인 가이드라인을 제시함으로써 직장에서 근로자의 인간존엄성과 프라이버시를 보호하기 위해 1996년「근로자의 개인정보보호를 위한 실행규약(Code of Practice on the Protection of Workers' Personal Data)」을 채택하였다.[14] 동 규약에 따르면 사용자가 근로자의 전자우편을 모니터링하고자 하는 경우에는 첫째, 미리 그 사유와 기간, 모니터링 방법과 기술, 수집할 정보 등을 당해 근로자에게 알려야 하고, 근로자의 프라이버시 침해를 최소화하여야 한다(제6조제14항제1호). 둘째, 비밀 모니터링은 국내법규에 근거가 있는 경우 또는 범죄행위나 심각한 비행을 의심할 만한 합리적인 근거가 있는 경우에만 할 수 있다(제6조제14항제2호). 셋째, 연속적인 모니터링은 보건안전이나 재산보호를 위해 필요한 경우로 한정된다(제6조제14항제3호). 넷째, 근로자대표가 선임되어 있는 경우에는 전자적 모니터링 방법을 도입하기 전에 근로자대표에게 미리 그 사실을 통지하고 협의하여야 한다(제12조제2항제2호). 마지막으로 전자적 모니터링 방법으로 수집된 개인정보가 근로자의 근무성적을 평가하는 유일한 요소가 되어서는 아니 된다(제5조제6항).

#### 나. OECD(경제협력개발기구)

OECD는 개인정보의 '적절한' 보호와 자유로운 이전을 보장하기 위해 1980년「프라이버시보호 및 개인정보의 국제유통에 관한 가이드라인(Guidelines on

14) 동 규약에 관한 상세한 설명은 이창범,「전자우편감시를 위한 법적 구비요건」,『산업보안연구논총』, 국가정보원, 2004.11, 103~182쪽 참조.

the Protection of Privacy and Transborder Flows of Personal Data)」을 채택하였다. 동 가이드라인은 공·사부문에 관계없이 모든 영역에서 이루어지고 있는 개인정보의 수집과 처리에 적용되기 때문에 직장에서 행해지는 전자우편 감시에도 적용된다. 그러나 OECD 가이드라인은 모든 형태, 모든 방식, 모든 영역의 개인정보처리에 전반적으로 적용되는 일반원칙 성격의 규범이기 때문에 전자적 모니터링이나 전자우편 감시에만 특화된 별도의 규정은 두고 있지 않다.[15]

사용자는 근로자의 전자우편을 감시하고자 하는 경우 OECD 가이드라인에 따라 미리 근로자의 동의를 받거나 알려야 하고(수집제한원칙), 감시의 목적을 명확히 제시하여야 하며 그 목적 달성에 필요한 범위 내에서 감시를 행해야 한다(목적명확화원칙). 또한 감시를 통해 수집된 개인정보를 수집시 제시한 목적 이외의 용도에 이용해서는 안 된다(이용제한원칙). 또한 사용자는 감시해야 할 정보의 내용 및 성격, 감시의 장소·시간·방법, 감시에 대해서 책임을 지는 담당자의 성명과 연락처, 기타 감시와 관련한 회사의 일반적인 절차와 방침을 공개해야 한다(공개원칙).

### 다. EU(유럽연합)

EU는 어느 국제기구보다 개인정보보호에 대해서 관심이 높고 입법 및 조사·연구 활동도 활발하다. 1995년 개인정보보호에 관한 일반규범으로서의 성격을 가지고 있는 「개인정보의 보호 및 자유로운 이전에 관한 지침」[16]을 채택한 외에, 1997년에는 전자통신분야에서의 개인정보 처리와 프라이버시 보호를 목적으로 한 별도의 지침[17]을 채택하였다. 특히 EU는 일찍부터 직장에서의 근로자들의 개인정보보호에 큰 관심을 가지고 1989년 세계 최초로 고용목적으로

15) 동 가이드라인에 관한 상세한 설명은 이창범, 앞의 논문, 103~182쪽 참조.

16) Directive 95/46/EC on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data.

17) Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. 이 지침은 2002년 7월 새로운 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)으로 대체되었다.

수집·이용되고 있는 개인정보를 보호하기 위한 권고[18]를 채택하기도 하였다.

이어 2001년 9월에는 정보보호 및 사생활보호에 관한 독립적인 자문기구로서 EU 개인정보보호지침 제29조의 규정에 의해 설치된 EU정보보호특별조사위원회가 「고용상황에서의 개인정보처리에 관한 의견서」[19]를 통해 근로자의 개인정보 보호를 위한 구체적인 원칙을 제시하였으며, 2002년 5월에는 「직장내 전자통신의 감시와 감독에 관한 조사보고서」[20]를 통해 직장내 전자통신 감시로부터 개인정보보호를 위한 실무 원칙을 제시하고 있다.

EU정보보호특별조사위원회는 2002년 보고서에서 전자우편도 기존의 종이편지와 똑같은 보호를 받아야 한다는 입장을 취하고 있다. 즉 전자우편도 유럽인권협약[21] 제8조제1항에서 규정하고 있는 '사생활'과 '통신'의 개념에 포함되며, 사용된 전자통신수단의 소유자가 누구이고 그 장소가 어디냐에 따라 통신비밀보호의 원칙이 배제되어서는 안 된다고 한다. 특히 전자우편 감시에서는 근로자 본인만이 아니라 그와 통신한 상대방, 특히 조직외부의 사람들의 사생활도 존중되어야 한다고 주장한다.

그러나 사용자의 정당한 이익을 보호하기 위해 근로자의 통신비밀은 어느 정도 침해를 감수하여야 한다. 문제는 어떤 목적, 어떤 방법, 어느 정도의 감시가 근로자의 기본적 권리를 침해하지 않는 적법한 감시인가 하는 점이다. 사용자에 의한 전자우편 감시가 정당화되기 위해서는 최소한 필요성, 최종성, 투명성, 접근성, 합법성, 균형성, 정확성, 보안성 등 직장내 전자통신 감시를 위한 8가지 일반원칙을 준수해야 한다.[22] 여기에 위원회가 특별히 강조하고 있는 몇 가지 중요한 쟁점을 정리해 보면 다음과 같다.

전자우편은 수신자와 발신자 모두의 개인정보를 포함하고 있고, 사용자는 일반적으로 별다른 어려움 없이 수신자와 발신자 중 한쪽의 동의를 얻을 수 있다

---

18) Council of Europe's Recommendation (89) 2 on the Protection of Personal Data Used for Employment Purposes.

19) Opinion 8/2001 on the processing of personal data in the employment context (13 September 2001). 상세한 설명은 이창범, 앞의 논문, 103~182쪽 참조.

20) Working document on the surveillance of electronic communications in the workplace (29 May 2002).

21) European Convention for the Protection of Human Rights and Fundamental Freedoms.

22) 2002년 EU직장내 전자통신감시 보고서에 관한 상세한 설명은 이창범, 앞의 논문, 103~182쪽.

는 점을 감안하면, 동의를 바탕으로 한 전자우편감시는 합법화되기 어렵다. 사전 고지나 경고만으로 전자우편을 감시하는 것은 더더욱 안 된다. 순전히 개인적 목적을 위해 제공되거나 이용되고 있는 전자우편계정을 사용자가 감시하는 것은 바이러스 점검과 같은 아주 제한된 경우를 제외하고는 거의 정당화되기 어렵다.

따라서 위원회는 무분별한 전자우편 감시에 의한 사생활 침해의 위험을 줄이고 감시의 효과를 극대화하기 위해 근로자에게 업무용 전자우편계정과 개인용 전자우편계정을 분리해서 제공하도록 사용자들에게 권고하고 있다. 업무와 관련한 전자우편에 대해서는 근로자의 사생활 침해의 위험이 없기 때문에 사용자의 열람과 감시가 비교적 폭넓게 인정되나, 개인적 목적의 전자우편에 대해서는 고지나 동의만으로는 열람이나 감시가 제한되어야 한다고 한다.

이러한 정책은 근로자가 사적인 전자우편을 보내기 위해 낭비하는 시간을 통제하고 근로자의 각종 불법행위(성희롱, 인종차별, 바이러스유포 등)로 인해 사용자가 져야 할 책임을 회피하는 데는 많은 도움이 될 수 있다. 예컨대, 근로자의 행동이 상당히 의심스러운 경우 사용자는 사적인 전자우편을 열어볼 필요도 없이 전자우편계정에서 보낸 시간을 점검하는 것만으로도 근로자가 사적인 목적으로 낭비한 시간을 추정해 낼 수 있다. 또한 근로자의 갑작스러운 결근이나 휴가, 출장시에도 업무용 전자우편은 언제든지 열어볼 수 있어 편리하다.

그러나 개인적인 전자우편을 통한 업무상 비밀정보의 누설과 같은 행위에 대해서는 여전히 규제가 필요하기 때문에 사적 목적의 전자우편이라도 일정한 요건하에서 감시는 불가피하다. 이 밖에도 전자우편 감시와 관련해서는 근로자가 회사에서 배급한 전자우편계정 이외의 전자우편계정을 사용할 수 있는지 여부, 전자우편 내용에 접근하기 위한 조건 및 목적의 구체화(결근, 출장, 기타 근로자와의 합의사항 등), 메시지 백업용 카피의 저장기간, 서버에서 메시지의 영구삭제에 관한 고지, 보안에 관한 정보, 전자우편 감시방침의 제·개정시 직원대표와의 협의 등에 관한 정책이 고려되어야 한다.

## 2. 주요 선진국

### 가. 미 국

미국은 판례를 통해 프라이버시권에 관한 법리를 가장 먼저 개척한 나라이지만, 정보통신기술의 고도화로 파생된 근로자나 소비자의 사생활보호 문제에 대해서는 유럽 국가는 물론 같은 영미법계 국가인 캐나다나 호주보다도 관심도가 떨어진다. 근로자의 전자우편 감시와 관련한 사건에서 법원은 일관해서 사용자 측에 우호적인 판결을 내리고 있다. 연방 및 주정부의 공무원들은 연방 수정헌법 제4조에 의하여 명시적으로 프라이버시권을 보호받고 있지만, 전자우편 감시와 관련해서는 연방 헌법도 역시 공무원 편이 아니다.

EU정보보호특별조사위원회는 근로자의 동의나 사용자의 고지만으로는 전자우편의 감시가 정당화되지 않는다고 보지만, 미국의 법원들은 사용자가 근로자의 전자우편을 감시하겠다는 입장을 발표한 이상 근로자의 명시적인 동의가 없더라도 전자우편상에서 근로자의 프라이버시권은 보장되지 않는다는 입장이다. 즉 사용자가 전자우편에 대한 감시정책을 채택하고 있고 근로자가 그 같은 사실을 알고 있는 한 전자우편상에서 자신의 프라이버시가 보호받으리라는 근로자의 기대는 합리적으로 인정되지 않는다는 것이다.

또한, 판례는 사용자에 의한 전자우편 감시가 정당화될 수 있는 요건이나 기준을 명확히 제시하고 있지 않다. 사용자의 컴퓨터 시스템을 이용한 전자우편에 대해서는 프라이버시 보호에 대한 근로자의 기대 가능성이 없다는 전제에서부터 출발하기 때문에 사용자의 감시행위의 적정성 여부를 판단할 기준이나 요건의 개발에 대해서 소홀한 것은 당연하다고 할 수 있다. 그만큼 사용자에 의한 전자우편 감시의 남용이 우려되고 있다. 캘리포니아에서는 주의회가 두 차례에 걸쳐 사용자가 미리 전자모니터링에 관한 정책을 작성해서 근로자들에게 배포하지 아니하는 한 근로자의 개인 전자우편이나 다른 컴퓨터 기록을 감시하지 못하게 하는 법안[23]을 통과시켰으나 주지사의 거부권 행사로 아직까지 입법에는 이르지 못하고 있다. 이에 비해 EU는 사용자의 전자우편 감시가 정당화되기

23) Electronic Monitoring in the Workplace Act : SB 1016(1999), SB 1822(2000).

위해서는 감시의 고지나 근로자의 동의만으로는 부족하고 필요성, 최종성, 비례성, 투명성 등의 원칙이 충족되어야 함을 분명히 하고 있다.

1) 판례 및 코먼로(common law)

가) O'Connor v. Ortega사건(1987년)

직장내 근로자의 프라이버시권 보호와 관련한 가장 기념비적인 판례는 O'Connor v. Ortega사건[24]이라고 할 수 있다. 이 사건에서 연방 대법원은 근로자도 자신의 책상, 캐비닛 등과 같은 특정 영역에 대하여는 프라이버시 보호에 대한 합리적인 기대를 가질 수 있으며, 법적으로 보호받아야 할 프라이버시 이익이 있음을 인정하였다.

그러나 근로자의 프라이버시 보호에 대한 기대는 현실의 업무관행이나 절차에 따라 감소될 수 있으며, 직장 현실과도 균형을 이루어야 한다고 한다. 따라서 근로자가 프라이버시 보호에 대해 합리적인 기대를 가질 수 있는지 여부는 그가 일하고 있는 직장의 업무관행에 따라 다를 수 있으며, 근무환경에 따라 케이스 바이 케이스(a case-by-case)로 처리되어야 한다.

위 사건의 개요를 보면, 피고 나파(Napa) 주립병원은 자기 병원의 교육책임자인 원고 Magno Ortega에게 조사가 진행되는 동안 자리를 비워줄 것을 요구한 후 관계자를 시켜 원고의 사무실을 수색하고 책상과 캐비닛에서 몇 가지 사물(私物)을 압수해 갔다. 이에 대해 법원은 원고가 다른 직원들과 자신의 책상과 캐비넷을 공유하지 않았던 사실을 지적하면서 원고에게 프라이버시 보호에 대한 합리적인 기대가 있음을 확인하고 원고의 손을 들어주었다.

그러나 이 사건에서 법원이 보다 더 중요하게 생각했던 것은 병원측이 근로자들에게 사무실의 책상이나 캐비닛에 사적인 물건을 보관하지 못하게 하는 어떠한 규정이나 방침도 사전에 가지고 있지 않았다는 사실이다. 병원이 그와 같은 규정이나 방침을 제정하지 않았다고 해서 근로자의 없었던 프라이버시권이 새롭게 만들어지는 것은 아니라는 주장을 덧붙이고는 있지만, 명시적인 방침의 부재가 사용자를 패소에 이르게 한 결정적 사실이었던 것만은 분명하다. 이 판례에 따르면 근로자는 직장에서도 프라이버시 보호에 대한 합리적인 기대를 가

24) *O'Connor v. Ortega*, 480 U.S. 709, 107 S.Ct. 1492, 94 N.Rd.2d 714(1987).

지지만 사용자의 방침이나 관행에 따라 그러한 기대는 부정될 수 있다.

나) Smyth v. Pillsbury Co.사건(1996년)

책상과 서랍에 대한 수색이 문제되었던 O'Connor사건과는 달리 근로자의 전자우편 감시나 인터넷활동 모니터링이 문제된 법적 분쟁에서는 대부분 사용자 측이 일방적인 승리를 거두고 있다. 근로자들이 전자우편 감시와 관련한 소송에서 주로 의지하는 것이 코먼로상 확립된 '폐쇄적 사적영역 침해(intrusion upon seclusion theory)'[25]에 관한 법리이다. 즉 사용자가 근로자의 사적인 문제나 관심에까지 개입함으로써 평균적인 보통사람들(reasonable person)에게 심한 불쾌감 또는 모욕감을 야기한다는 점을 강조한다.

그러나 뉴욕 등 일부 주에서는 코먼로상 '폐쇄적 사적영역 침해' 법리에 근거한 프라이버시 침해를 인정하고 있지 않을 뿐만 아니라, 설사 이를 인정하고 있는 주라고 하더라도 법원은 결코 근로자에게 우호적이지 않다. 대다수 법원이 전자우편 감시에 관한 리딩 케이스라고 할 수 있는 Smyth v. Pillsbury Co. 사건[26]의 판례를 따르고 있기 때문이다.

Smyth사건에서 법원은 작업환경과 전자통신의 성격과의 관계상 근로자는 전자우편에 대하여 프라이버시 보호에 관한 합리적인 기대를 가질 수 없다고 한다. 설사 근로자가 프라이버시 보호에 대한 기대를 가지고 있다고 하더라도 그러한 기대는 전자우편의 남용을 방지하고자 하는 사용자의 이익에 의해 양보되어야 한다는 것이다.

이 사건에서 원고는 회사 경영진을 비판하는 내용의 몇 가지 글을 자신의 집

25) 코먼로상 프라이버시 침해는 네 가지 이론, 즉 ① 폐쇄적 사적영역 침해 이론, ② 이름 등의 남용 이론(misappropriation of name or likeness), ③ 사적 사실 공개 이론(public disclosure of private facts), ④ 허위사실 공표(publicity which places another in a false light)에 입각해서 보호를 받는다. '폐쇄적 사적영역 침해'가 성립하기 위해서는 물리적이든 정신적이든 은둔상태(the solitude of seclusion) 또는 사적인 일이나 관심(private affairs or concerns)에 대하여 그 침해가 고의적(intentional)이어야 하고, 정보가 널리(at large) 공중에게 공개되어야 하며, 또한 그 정보가 합리적인 사람을 기준으로 볼 때 중요(substantial)하고 매우 공격적(highly offensive)이어야 한다(Morgan J. Bassett, *An Overview of E-Mail and Internet Monitoring in the Workplace*, Ford Marrin Esposito Witmeyer & Gleser, L.L.P., http://www.fmew.com/archive/monitoring 참조).

26) *Smyth v. Pillsbury Co*., 914 F.Supp. 97, 100 (E.D. Pa. 1996).

컴퓨터에서 회사의 전자우편 시스템을 이용하여 전송하였다. 얼마 후 사용자는 원고의 전자우편 내용을 이유로 그를 해고하였다. 원고는 자신의 프라이버시가 침해되었으며 불법적으로 수집된 정보를 가지고 한 해고는 공서양속 위반이라고 주장하였다.

이에 대해 법원은 사용자로부터 전자우편에 대한 비밀이 보장되어 있고 경영진에 의한 가로채기가 행해지고 있지 않음을—즉 전자우편감시에 대한 회사의 방침이나 규정이 없음을—확인하였음에도 불구하고, 일단 원고가 사용자측에서 제공한 전자우편시스템을 통해 통신을 하기로 마음먹은 이상 프라이버시 보호에 대한 합리적인 기대를 포기하였다고 보아야 한다는 입장을 보이고 있다.

추가적으로 법원은 프라이버시 보호에 대한 근로자의 합리적인 기대를 인정한다고 하더라도 전자우편을 이용한 근로자들의 부적절하고 비전문적인 코멘트나 불법적인 활동을 방지해야 할 사용자의 이익이 근로자의 프라이버시 이익을 압도하기 때문에 보통사람(a reasonable person)이라면 사용자에 의한 전자우편 감시행위를 근로자의 프라이버시에 대한 실질적이고도 중대한 침해라고 보지는 않을 것이라는 설명을 부연하고 있다.

유사 판례인 McLaren v. Microsoft Corp.사건[27]에서 법원은 "회사 소유의 컴퓨터를 이용해서 보낸 전자우편 메시지는 근로자 자신의 재산이 아니라 오히려 업무의 본질적인 일부로 보아야 한다."고 주장하면서 전자우편의 소유권 문제를 언급하고 있다. 법원은 근로자의 개인 폴더에 저장되어 있어서 비밀번호를 이용하지 않으면 접근할 수 없는 메시지라고 하더라도 그 메시지가 회사서버에 저장되어 있는 한, 그리고 사용자가 접근할 수 있는 네트워크를 통해 전송되고 있는 한 프라이버시 보호에 대한 합리적인 기대 가능성은 없다고 한다.

### 2) 전자통신프라이버시보호법(1986년)

사용자의 전자우편 감시에 대해서 근로자들은 코먼로상의 불법행위 소송 외에 연방 제정법인 전자통신프라이버시보호법(ECPA)[28]에 의해서도 권리 주장

---

27) *McClaren v. Microsoft Corp*., 1999 WL339015 (Tex.Ct.App. May 28, 1999).

28) Electronic Communications Privacy Act of 1986 (Pub. L. No. 99~508, 100 Stat. 1848). 이 법은 전자우편과 같은 새로운 형태의 통신수단으로까지 규제의 범위를 확대하기 위해 주로 불법적인 '전화도청' 금지를 목적으로 제정된 「the Omnibus Crime

이 가능하다. ECPA는 통신내용의 무단 가로채기(intercept of message), 가로채기를 통해 획득한 통신내용의 무단 공개(disclose) 및 이용(use), 전자통신시설 및 저장된 전자통신내용에 대한 무단 접근(Access), 저장된 전자통신내용의 공개를 금지하고 있다. 이 법은 사용자들이 사내에 설치·운영하고 있는 사적 통신시스템에까지 그 효력이 미치는 것으로 이해되고 있다.

따라서 표면상으로는 ECPA가 직장에서 사용자들에 의해서 행해지고 있는 전자우편 감시에 대하여 근로자에게 광범위한 보호를 주고 있는 것처럼 보인다. 그러나 현실적으로 근로자가 이 법에 의거해서 전자우편과 관련한 프라이버시를 보호받을 가능성은 거의 없어 보인다. 판례의 해석과 면제규정에 의하여 법적용에 광범위한 예외가 인정되기 때문이다. 대다수 주에서도 일반적으로 ECPA의 내용과 유사한 법률을 두고 있다.

가) 해석에 의한 적용제한

통신내용의 가로채기에 관한 판례의 입장은 결코 근로자에게 유리하지 않다. ECPA는 누구든지 통신내용을 무단으로 가로채기하거나 공개·이용하는 것을 금지하고 있다(§2511(1)).[29] 그러나 판례[30]는 대체로 전송중인 정보에 대해서만 가로채기를 인정하고 저장된 정보에 대해서는 가로채기를 인정하지 않고 있다.[31] 따라서 불과 몇 초만에 전송이 끝나 버리고 일단 서버나 컴퓨터에 저장이 된 후에만 다른 사람에 의한 획득이 가능한 전자우편의 특성상 전자우편 감

---

Control and Safe Streets Act of 1968」의 제3장(Title Ⅲ) 흔히 Federal Wire Tap Statute(18 U.S.C.A. §2510(West 1968))로 불리고 있는 법률을 개정한 것이다.

29) 여기서 보호되는 것은 통신의 내용만 보호되므로 송·수신자의 신원, 통신내용의 크기, 통신 제목 등과 같은 정보는 보호의 대상이 아니다.

30) 판례에 따르면 전자통신내용의 획득이 전송과 동시에 이루어지지 아니하는 한 ECPA상의 무단 가로채기는 성립되지 아니한다고 한다. *Steve Jackson Games Inc. v. United States Secret Service*사건(36 F.3d 457 (5th Cir. 1994))과 *Wesley College v. Pitts*사건(974 F. Supp. 375 (D. Del. 1997)) 참조.

31) 이에 반하여 *Fraser v. Nationwide Mutual Insurance Co.*사건 판결에서 법원은 가로채기를 '송신자가 정보를 전송하고 수신자가 그것을 수신하기 전'에 당해 정보를 획득해 간 것으로 정의함으로써 저장된 정보에 대해서도 가로채기가 적용된다고 보고 있다. 즉 수신자가 메시지를 받아본 후에 사용자가 정기적으로 근로자의 메일박스나 저장된 파일을 열어보았다면 가로채기가 성립되지 않으나, 수신자가 메시지를 열어보기 전에 그와 같은 행위가 발생했다면 메시지를 전송한 지 아무리 오랜 기간이 지난 후에 행해졌더라도 가로채기가 성립된다고 한다(135 F.Supp.2d 623(E.D.Pa. 2001)).

시에 대해서는 좀처럼 가로채기 금지 규정이 적용될 여지가 없다고 한다.[32]

나) 사전동의에 의한 면제(the Prior Consent Exception)

ECPA는 통신 당사자 중 한 사람의 사전 동의만 얻으면 범죄나 불법행위를 목적으로 하지 아니하는 한 자유롭게 통신내용을 가로채기하거나 공개·이용할 수 있다(§2511(2)(d)). 또, 전자통신시설이나 저장되어 있는 전자통신내용에 대해서도 사전 허가 또는 동의만 있으면 접근이 가능하다(§2701(a)). 근로자가 사용자의 동의 요구를 거부하는 것은 현실적으로 어렵기 때문에 이 규정은 사용자에게 전자우편 감시의 기회를 넓혀 주는 데 큰 기여를 하고 있다.

동의는 명시적인 동의(예, 동의서에 서명) 외에 묵시적인 동의도 포함된다. 근로자가 사용자로부터 전자우편을 감시한다는 통지를 받고도 사용자의 전자우편시스템을 이용했다면 묵시적 동의가 있는 것으로 본다. 그러나 사용자가 전자우편을 감시할 수도 있다는 것을 근로자가 알고 있었다는 사실만으로는 묵시적 동의는 성립하지 않는다. 또한 사용자가 스스로 정한 감시의 범위나 목적을 벗어난 경우에는 묵시적 동의가 인정되지 않는다. 예컨대, 송·수신자의 전자우편주소와 통신 빈도만을 조사하겠다고 해놓고 통신내용까지 감시한 경우 동의는 인정되지 않는다.

다) 업무상 이용의 면제(the Business Use Exception)

ECPA는 '업무상 이용의 면제(the Business Use Exception)'라고 하여 통신서비스를 제공하는 제공자의 임·직원이나 대리인이 통신서비스를 이행하기 위해 또는 서비스 제공자의 권리나 재산을 보호하기 위해 필연적으로 부수되는 활동의 일환으로 통상적인 업무처리 과정에서 통신을 가로채기하거나 공개 또는 이용한 행위에 대하여는 동법의 적용을 면제하고 있다(§2511(2)(a)(i)).

'업무상 이용면제'가 적용되기 위해서는 두 개의 요건이 필요하다. 첫째, 사

32) 그러나 최근 가로채기와 무단접근의 구분방법에 큰 변화가 일고 있다. *Konop v. Hawaiian Airlines, Inc.*사건(236 F.3d 1035(9th Cir. 2001))에서 법원은 수신자가 메시지를 열어보았는지 여부를 묻지 않고 전송된 메시지를 무단으로 획득해 갔으면 이를 '가로채기'로 보고 메시지를 획득해 갈 수 있는 상태에까지 접근한 경우를 '접근'으로 보고 있다. 양자 사이에 근본적인 차이는 없으나 가로채기가 무단 접근보다 위법성이 크다고 한다.

용자가 통신서비스의 제공자이어야 한다. 통상 판례는 전자우편시스템을 운영하고 있는 사용자를 당연한 전자우편 서비스 제공자로 보고 있다.[33] 둘째, 감시가 정상적인 업무처리 과정에서 행해진 것이어야 한다. 대다수 판례가 사용자에 의한 근로자의 전자우편 감시를 업무상 이익과 충분한 관련이 있는 것으로 인정해 주고 있다.[34]

그러나 단순히 전자우편이 사적인 것인지 업무적인 것인지를 탐색하거나 전자우편이 얼마나 자주 전송되고 있는지를 알아보기 위해서 행하는 감시와는 달리, 근로자의 '사적인' 전자우편내용을 감시하는 행위에 대해서는 업무상 이용 면제를 주장하기 어렵다고 한다.[35]

라) 서비스제공자 면제(the Provider Exception)

ECPA는 원칙적으로 저장된 전자통신 메시지의 무단 접근과 공개를 금지하고 있다(§2701(1) 및 §2702(1)). 전자우편 감시는 주로 저장된 정보에 대한 감시이므로 근로자의 전자우편 감시에 대해서 동조가 적용될 수 있을 것임은 의심의 여지가 없다. 그러나 ECPA는 동시에 동조의 적용을 가로막는 광범위한 예외 규정을 두고 있어서 사용자에 의한 근로자의 전자우편 감시에는 별 도움을 주지 못한다.

즉 동법 제2701조(c)항(1)호는 '통신서비스를 제공하는 개인 및 기관에 대한 면제(the Provider Exception)'라고 하여 통신서비스를 제공하는 개인 또는 기관의 허가를 받아서 저장되어 있는 전자통신 메시지에 접근하는 것에 대해서는 무단 접근금지 규정의 적용을 면제하고 있다. 통신서비스제공자에는 사내에 전자통신시스템을 설치·운영하고 있는 사용자도 포함된다. 따라서 사용자는 스스로 또는 그 임직원을 시켜서 자유로이 저장된 근로자의 전자통신내용에 접근할 수 있다.

사용자가 근로자로부터 동의를 받았는지 여부에 관계없이, 또한 접근하고자 하는 메시지가 개인적인 것인지 업무적인 것인지 여부에 무관하게 저장된 메시지에 자유스럽게 접근할 수 있다.[36] 따라서 사용자는 근로자의 전자우편에 무

33) *Bohach v. City of Reno*, 932 F. Supp. 1232 at 1236 (D. Nev. 1996) 참조.
34) *Briggs v. American Air Filter Co*., 630 F.2d 414 (5th Cir. 1980) 참조.
35) *Watkins v. L.M. Berry & Co*., 704 F.2d 577 (11th Cir. 1993).

제한적으로 '접근'할 수 있다고 보아야 한다. 그러나 사용자가 근로자의 전자우편내용을 '가로채기'하기 위해서는 요건이 좀더 엄격한 '업무상 이용면제'의 요건을 갖추어야 한다.

### 3) 연방 수정헌법 제4조

수정헌법 제4조는 정부기관에 의한 불합리한 수색과 체포로부터 개인을 보호한다.[37] 원칙적으로 수정헌법 제4조는 연방 및 주 공무원, 정부기관의 대리인 및 그 직원, 형사사건의 피의자에게만 적용된다. 따라서 정부기관에 근무하고 있는 공무원들에 대한 전자우편 감시에 대해서도 표면상으로는 헌법 제4조에 의한 보호가 가능하다. 그러나 법원은 수정헌법 제4조를 근로자 감시와 관련한 소송에 적용함에 있어서 코먼로상의 판례 원칙을 대체로 그대로 적용하고 있다. 즉 일반적으로 판례는 공무원의 프라이버시 보호에 부정적이다.

시경 소속 경찰관들이 사용하고 있는 pager message(일종의 전자우편)에 대한 감시가 문제된 *Bohach v. City of Reno*사건[38]에서는 당국이 인터넷 감시에 대한 명시적인 정책을 가지고 있지 않았음에도 불구하고 법원은 경찰관들의 프라이버시 보호에 대한 기대 가능성을 부정하였다. 법원은 인터넷 감시에 관한 명시적인 정책이 있었더라면 경찰관들이 그와 같은 메시지를 전송하지 않았을 것이므로 프라이버시 보호에 대한 '주관적인' 기대는 가질 수 있었겠지만, 그런 정책이 없더라도 경찰관들은 자신이 보낸 메시지가 컴퓨터 시스템에 저장될 수 있고 저장된 메시지가 감시당할 수 있다는 사실을 이해할 수 있었으므로 프라이버시 보호에 대한 '객관적이고 합리적인' 기대는 가질 수 없다고 판시하고 있다.

---

36) *Bohach v. City of Reno*, 932 F. Supp. 1232 at 1236 (D. Nev. 1996).

37) The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

38) *Bohach v. City of Reno*, 932 F. Supp. 1232 at 1236 (D. Nev. 1996). 이에 비해 *United States v. Simon*, 206 F.3d 392 (4th Cir. 2000)에서는 사용자가 근로자들에게 그들의 온라인 활동이 감시될 수 있다는 사실을 알리는 명백한 방침을 채택하고 있었기 때문에 원고는 인터넷상에서 프라이버시 보호에 대한 합리적인 기대를 가지지 못한다고 판시하였다.

## 나. 영 국

영국은 미국, 캐나다 등과 함께 영미법계 국가에 속하지만 EU 회원국이라는 지위 때문에 개인정보보호제도에 대해서는 미국보다 유럽 쪽에 가깝다. 미국에서는 코먼로와 제정법이 모두 전자우편에 대한 근로자의 프라이버시 기대 가능성을 부정하고 있음에 반해 영국에서는 이를 제정법으로 보호하고 있다. 근로자의 사생활보호에 대해서는 개인정보보호에 관한 일반법으로서의 성격을 가지고 있는 1998년 데이터보호법(Data Protection Act 1998)[39]이 적용되며, 특별히 근로자의 사생활보호나 전자우편 감시만을 규율 대상으로 하는 개별법은 없다.

영국에서는 코먼로상 프라이버시 침해를 이유로 한 불법행위는 인정되지 않고 있다. 따라서 일찍부터 개인의 사생활 보호를 위한 포괄적인 법률의 입법 필요성이 논의되어 왔다. 그런 의미에서 1998년 데이터보호법은 영국의 개인정보보호 법제상 아주 중요한 의미를 갖는다고 할 수 있다. 그러나 영국은 아직도 이웃나라인 프랑스나 독일에 비해서는 여전히 근로자의 사생활 보호에 관한 수준이 떨어진다는 평가를 받고 있다.

예컨대, 프랑스와 독일에서는 전자우편 감시와 같은 근로자 감시수단을 직장내에 도입하고자 할 때에는 집단적 노사관계의 관점에서 사용자가 미리 직장협의회 등 근로자를 대표하는 기구와 협의를 하게 하거나 사용자에게 정보제공의무 또는 설명의무를 부과하고 있으나 영국에서는 전자우편 감시가 단체 협의나 협상의 대상이 아니다.

### 1) 판례 및 코먼로

영국의 코먼로는 원치 않는 신체적 침해에 대해서는 아무리 경미한 것이라도 불법접촉(battery)이라고 하여 이를 불법행위로 간주해 왔다. 따라서 직장에서 행해진 약물테스트나 유전자검사는 근로자의 명시적 동의가 없는 한 프라이버시 침해를 구성한다. 그러나 신체적 접촉을 포함하지 아니하는 검사나 조사, 예를 들어 책상이나 서랍의 조사행위는 일반적으로 불법행위를 구성하지 않는다.

39) 1995년 채택된 EU개인정보보호지침을 반영한 것으로, 1998년 7월 16일 제정되어 2000년 3월 1일부터 시행되었다.

따라서 사용자에 의한 근로자의 전화감청이나 전자우편감시도 코먼로상으로는 프라이버시 침해를 구성하지 않을 가능성이 크다. 오히려 사용자의 전자우편 이용 규정을 위반한 경우 코먼로상 계약불이행이 성립되어 예고 없는 해고의 사유가 될 수 있다.

가) Malone v. Commissioner사건(1979년)

영국 법원은 1979년 2월 28일 *Malone v. Commissioner*사건[40] 판결에서 "전화상에서 비밀정보(confidential information)를 발설한 사람은 전화라고 하는 통신수단의 특성상 자신의 통화내용이 제3자에게 노출될 수 있다는 위험을 감수해야 한다"고 판시하여 전화상의 통신비밀 보호를 부정하였다. 이 사건은 그 후 유럽인권법원에 제소되었고 유럽인권법원은 이에 대해 "전화통신의 도청은 유럽인권협약(European Convention for the Protection of Human Rights and Fundamental Freedoms) 제8조[41] 위반이며 이에 대한 국내법적 구제수단을 마련하지 아니한 것은 협약 제13조[42] 위반에 해당한다."고 판시함으로써 원고의 손을 들어주었다.[43] 이 사건 판결의 결과에 따라 영국 정부는 1985년 통신감청법을 제정하여 공적 통신 시스템을 통해 전달되는 통신을 감청하는 행위를 범죄로 처벌하고 있다.

나) John Lewis plc v. Coyne사건(2000년)

한편, 전화감청을 직접적인 소송원인으로 한 사건은 아니지만 직장에서 개인

40) *Malone v. Commissioner of Police of the Metropolitan*, [1979] 2 All ER 620 (Ch).

41) ARTICLE 8 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

42) ARTICLE 13 Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

43) *Malone v. United Kingdom* (1985) 7 EHRR 14.

적 용무의 전화 이용을 문제삼아 근로자를 해고한 사건에서 사용자의 행위를 불공정 해고로 본 판례가 있다. 2000년 11월 7일 *John Lewis plc v. Coyne*사건[44]에서 사용자는 Coyne이 "개인적 용무로 점 내의 전화를 이용해서는 안 된다. 이를 위반한 경우 해고될 수 있다."라고 되어 있는 회사 방침을 위반하여 1년간 111건, 통합 13.5시간의 전화를 이용하였으므로 해고는 정당하다고 주장하였다. 이에 대해 법원은 Coyne이 전화를 한 목적, 전화를 이용할 수밖에 없는 사정 등에 대한 충분한 조사 없이 취해진 해고조치는 불공정행위에 해당한다고 판시하였다.

2) 1998년 데이터보호법

코먼로와는 달리 제정법은 사용자에 의한 무절제한 전자우편 감시로부터 근로자를 보호하기 위한 장치들을 마련해 놓고 있다. 2000년부터 시행되고 있는 「1998년 데이터보호법(Data Protection Act 1998)」은 직장 근로자에 대해서도 소비자나 일반시민과 동일한 수준의 프라이버시를 보호하고 있다. 데이터보호법은 근로자끼리 또는 근로자와 제3자 사이에 주고받은 전자우편에 대한 사용자측의 감시를 전적으로 금지하고 있는 것은 아니지만, 사용자가 전자우편을 감시하고자 할 때에는 이 법에서 정하고 있는 엄격한 데이터보호원칙을 준수해야 한다.

데이터보호법상 근로자의 전자우편에 대한 감시가 허용되는 경우로는 해당 근로자의 사전 동의가 있는 경우와 데이터취급자·제3자·당사자의 정당한 이익을 추구하기 위하여 사용자에 의한 감시가 필요로 하는 경우이다(부칙2 제1조 및 제6조). 그러나 어느 경우에도 근로자의 권리·자유 및 정당한 이익을 침해하는 것은 안 된다. 어떤 경우에 프라이버시를 침해하지 않고 근로자의 전자우편을 감시할 수 있는 것인가? 이에 대한 구체적인 행동지침으로 영국 정보보호 커미셔너는 2003년 6월 11일 「직장감시지침」[45]과 이를 보충하기 위한 「소기업을 위한 직장감시지침」[46]을 작성하여 발표하였다.

---

44) *John Lewis plc v. Coyne* [2001] IRLR 139(EAT).

45) The Employment Practices Data Protection Code : Part3 Monitoring at Work. www.informationcommissioner.gov.uk 참조.

46) Monitoring at Work : Guidance for Small Businesses. www.informationcommissioner.gov.uk

2003년 직장감시지침은 근로자의 전자우편에 대한 감시를 위해서는 원칙적으로 근로자의 '자발적 동의'가 있어야 하고 공개적으로 실시할 것을 요구한다.[47] 그러나 예외적으로 프라이버시 영향평가를 통해 전자우편감시가 정당화된 경우—근로자에게 끼친 불이익보다 사용자와 다른 사람의 이익이 더 큰 경우—에는 동의가 불필요하다. 앞에서 설명한 데이터보호법 부칙2 제6조에서 규정한 '다른 사람의 정당한 이익'이 이에 해당한다. 그러나 이 경우에도 다음과 같은 원칙에 따라 수행되어야 한다.

첫째, 전자우편 감시에 대한 사용자의 방침을 확실히 세워야 한다. 방침과 실제 관행이 다를 경우 이를 재검토해야 하고 근로자들이 방침을 숙지하도록 지속적으로 노력해야 한다(지침 3.3.1).

둘째, 감시에 통신내용의 가로채기(interception)가 포함된 경우에는 1998년 데이터보호법 외에 2000년 조사권한규제법에서 요구하고 있는 사항도 함께 준수하여야 한다(지침 3.3.2).

셋째, 해킹, 바이러스 등으로부터 전자우편시스템의 안전을 지키기 위해서 전자우편 감시가 필요하다면 그 같은 필요성의 범위 내에 그쳐야 하고 자동화 시스템의 사용을 고려해야 한다(지침 3.3.3).

넷째, 전자우편에 대한 감시를 하기 전에 프라이버시영향평가를 실시하여 감시의 부정적인 영향을 상쇄하고도 남을 만큼의 다른 이익이 있는지를 살펴야 한다. 이익이 있다고 판단되면 근로자에게 감시의 종류·정도·이유를 알리고 이를 인지하도록 해야 한다(지침 3.3.7).

다섯째, 전자우편의 개인적인 이용이 금지되어 있는 경우에도 가능한 한 전자우편을 열어보는 것은 피해야 하며, 특히 개인적인 전자우편이 분명해 보이는 경우—예컨대 건강상담, 노조활동 등—에는 개봉을 피해야 한다. 분명하고도 제한적인 이유 때문에 내용 확인이 꼭 필요한 경우를 제외하고는 전자우편의

---

참조.

47) 은밀한 전자우편 감시는 거의 정당성을 인정받을 수 없다. 비밀감시는 범죄행위나 그에 상당한 불법행위를 의심할 만한 충분한 근거가 있고 감시사실을 알리는 것이 불법행위의 조사 또는 예방을 오히려 방해하는 경우에만 가능하다. 비밀감시는 특별조사의 일부로서만 행해져야 하며 그 조사가 끝나면 즉시 감시를 중단해야 한다. 화장실이나 개인사무실에 대한 비밀감시는 중대한 범죄혐의가 있고 경찰관의 입회의사가 없는 한 행해져서는 안 된다. 주 45)의 「소기업을 위한 직장감시지침」, 6쪽 참조.

주소나 송·수신처만을 감시해야 한다. 사용자는 근로자가 자신이 보내는 전자우편뿐만 아니라 상대방이 자신에게 보내는 전자우편에 대해서도 업무상 메시지인지 개인적인 메시지인지를 구분하도록 독려해야 한다. 만약 근로자가 직장에서 개인적인 전자우편계정을 이용할 수 있도록 허락을 받은 경우에는 예외적인 경우에만－예컨대 성희롱, 스토킹, 인종차별, 비밀누설 등의 상당한 의혹이 있는 경우－감시를 할 수 있다(지침 3.3.8).

여섯째, 가능하다면 근로자뿐만 아니라 근로자에게 전자우편을 보낸 상대방도 전자우편의 감시사실과 감시목적을 알 수 있도록 해야 한다(3.3.9).

일곱째, 근로자의 부재중에 전자우편계정을 체크할 필요가 있을 때에는 미리 그 사실을 해당 근로자에게 알려야 한다. 그리고 근로자에게 사적 통신을 보호받기 위한 표시 시스템의 이용을 권장해야 한다. 또한 사적인 통신으로 보이는 전자우편을 열어보는 것은 가능한 한 피해야 한다(3.3.10).

마지막으로 전자우편시스템상에서 전자우편이 보관되는 크기와 기간에 대해 근로자에게 알려야 한다. 근로자에게 전자우편의 보유기간을 알리는 시스템을 도입해야 하며, 근로자가 전자우편의 보유기간을 알고 있는지를 점검해야 한다(3.3.11).

### 3) 2000년 조사권한규제법

근로자의 전자우편 프라이버시보호와 관련된 또 다른 제정법으로 「2000년 조사권한규제법(Regulation of Investigatory Powers Act 2000)」이 있다. 이 법은 공적 및 사적 전화시스템에 있어서 통신비밀을 보호하고 가로채기(interception)를 방지하기 위하여 1985년 통신감청법을 전문 개정한 것이다. 이 법의 또 다른 중요 목적 중 하나는 수사 당국에게 전자우편과 인터넷상의 암호화된 정보에 접근할 수 있는 권한을 부여하는 것이다.

조사권한규제법은 법적 권한 없이 '전송중'인 통신을 '가로채기'하는 것을 불법으로 규정하고 있다. 가로채기는 감시의 일부이기 때문에 가로채기에 대해서는 이 법뿐만 아니라 1998년 데이터보호법[48]의 조항도 중첩적으로 적용된다.

48) 1998년 데이터보호법은 가로채기뿐만 아니라 통신에 대한 체크, 접근, 저장 등과 같은 행위에 대해서도 적용된다.

이 법은 1985년 통신감청법과는 달리 공적 통신시스템에 연결된 사적 통신시스템에도 적용된다.[49] 따라서 인트라넷과 같은 순수한 사적 통신시스템에는 적용되지 않는다.

그러나 이 법은 가로채기 등의 금지에 대하여 너무 광범위한 예외를 인정하고 있다는 비판을 받고 있기도 하다. 즉 송신자와 수신자 쌍방이 명시적으로 동의한 경우뿐만 아니라 가로채기 등을 실시해야 할 정당한 이유가 있는 경우, 그리고 하위법인 「2000년 전화통신규칙(Telecommunications Regulations 2000)」 일명 「적법한 업무집행 규칙(Lawful Business Practice Regulations)」에서 정한 사항에 대해서도 가로채기 등을 허용하고 있다. 특히 송·수신자 쌍방의 명시적인 동의가 있는 경우에는 업무 관련성이 존재하는 한 사용자에게 꽤나 광범위한 가로채기 등이 허용된다.

2000년 전화통신규칙이 근로자나 송·수신자의 동의 없이 전자우편을 가로채기·감시·저장할 수 있게 허용하고 있는 조건은 다음과 같다. 첫째, 업무와 관련된 사실의 존재를 입증하기 위한 경우, 둘째, 강제규범 또는 자율규범의 준수 여부를 확인하기 위한 경우, 셋째, 근로자의 업무실적을 확인하기 위한 경우, 넷째, 범죄를 예방 또는 탐지하기 위한 경우, 다섯째, 허가받지 아니한 통신시스템의 사용을 조사 또는 탐지하기 위한 경우, 마지막으로 시스템의 보안과 효율적 운영을 확보하기 위한 경우이다.

다만, 이상의 경우에도 사용자는 근로자에게 전자우편 시스템을 이용할 때에는 감시의 가능성이 있다는 것을 충분히 설명하지 않으면 안 된다. 또한, 업무와 관련없는 사적인 전자우편의 내용까지 감시할 경우에는 1998년 데이터보호법 위반과 1998년 인권법 제8조가 규정하고 있는 통신프라이버시권 침해를 구성할 수 있다.

---

49) 경찰서 내에서 경찰관에 대하여 행해진 전화감청이 문제가 되어 유럽인권법원에 제소된 *Halford* 사건(1992년) 변론에서 영국 정부는 1985년 통신감청법은 공적 통신시스템에만 적용되므로 경찰서 내에서 이루어진 통신감청에 대해서는 동법이 적용되지 않는다. 따라서 원고 Halford 양은 경찰서 내에서의 전화통화와 관련하여 사생활 보호에 대한 합리적인 기대를 가질 수 없다고 주장하였다. 이에 대해 유럽인권법원은 "판례법으로 볼 때 유럽인권협약 제8조제1항에서 말하는 사생활과 통신에는 직장 또는 가정에서 행해진 전화통화도 포함된다..... Halford 양에게는 직장내 전화통화가 도청될 수 있다는 사실에 대한 경고가 없었다."고 판시하며 Halford 양의 프라이버시 침해를 인정하였다(*Halford v. The United Kingdom*, (1997) 24 EHRR 523 참조).

### 다. 프랑스

프랑스는 유럽국가 중에서 매우 강력한 개인정보보호정책을 채택하고 있는 나라들 중 하나이다. 무엇보다 인상적인 것은 1970년 법개정시 프랑스 민법과 형법에 사생활에 관한 권리를 '일반적인 권리'로서 명시하였다는 점이다. 민법 제9조는 "각인은 그 사생활이 존중될 권리를 가진다(chacun a droit au respect de sa vie privee ; Everyone has the right to respect for his private life.)."라고 규정함으로써[50] 영미법상 프라이버시권의 개념에 해당하는 '사생활 존중을 요구할 권리(droit au respect de la vie prive)'가 있음을 선언하고 있다. 형법 제226-1조도 본인의 동의없이 개인적인 대화나 영상을 기록하여 사생활의 내면을 침해하는 것을 처벌하고 있으며,[51] 그 결과 사용자에 의한 근로자의 전화 또는 전자우편의 은밀한 감시는 불법으로 간주되고 있다.

1978년에는 공공부문과 민간부문 전역에 걸쳐 개인데이터의 수집·이용 및 처리에 적용되는 「1978년 정보처리·파일및자유에관한법률」이 제정되어 정보취급자의 개인정보처리원칙과 정보주체의 개인정보자기결정권이 입법화되었으며, 1982년에는 노동법의 대폭적인 개정으로 직장내 근로자의 프라이버시 보호가 한층 강화되는 계기를 맞이하게 되었다. 노동법은 크게 세 가지 기본원칙을 이념적 기초로 하고 있는데, 투명성(transparency), 비례성(propotionality) 그리고 근로자대표의 자문(the consultational of employee representatives)[52]이 그것이다.

이에 따라 프랑스에서는 사용자는 근로자의 직무와 직접 관련이 없는 정보는 수집할 수 없다고 하는 대원칙이 확립되어 있다.[53] 또한, 사용자가 근로자의 개

---

50) Without prejudice to compensation for injury suffered, the court may prescribe any measures, such as sequestration, seizure and others, appropriate to prevent or put an end to an invasion of personal privacy; in case of emergency those measures may be provided for by interim order.

51) 1970년 법개정으로 새로 추가된 구형법 제368조는 '사적 장소'에서의 대화나 영상을 무단 기록한 행위만을 처벌하였으나 1993년 형법 대개정시 구형법 제368조를 신형법 제226-1조로 옮기면서 '사적 장소'라고 하는 제한을 삭제하여 어떠한 장소라도 사적인 대화이면 모두 보호의 대상으로 하였다.

52) 집단적 협상(collective bargaining)의 원칙 또는 집단적 검토(collective deliberation)의 원칙이라고도 한다.

53) 1992년 노동법 L121-6조 제2항.

인정보를 수집하려고 하는 경우에는 첫째, 정당한 이유가 있어야 하고, 둘째, 근로자의 사생활에 대한 침해가 최소한에 그치는 방법이어야 하며, 셋째, 법에서 정하고 있는 법정 직원대표조직인 기업위원회(comite d´entreprise) 등과 미리 협의를 해야 하고, 마지막으로 실제 개인정보를 수집하려고 할 때에는 정보주체에게 사전에 개별 통지를 해야 한다.

판례와 학설도 개인의 내면의 권리를 인격권(droit de la personalite)의 한 내용으로 보호하고 있다. 따라서 근로자의 개인정보보호에 매우 적극적이다. 프랑스의 최고법원에 해당하는 파훼원은 전자우편 감시를 통신비밀의 관점에서 파악함으로써 개인적 용무의 전자우편을 무단으로 개봉하는 사용자의 행위를 프라이버시 침해로 보고 있다.

1) 노동법

프랑스에서 노동법(CODE DU TRAVAIL)[54]은 근로자 프라이버시 보호에 매우 중요한 역할을 수행하고 있다. 노동법 제L121-8조는 근로자에게 알리지 않은 방법으로 근로자에 관한 개인정보를 수집하는 것을 명문으로 금지하고 있다(투명성 원칙). 이는 근로자가 자신의 사용자에 의해 도입된 감시장치의 존재를 반드시 알아야 한다는 것을 의미한다. 사용자는 근무시간 중 근로자의 활동을 감독·감시할 권한을 가지지만, 비밀수단을 이용한 감시는 언제든지 위법이라는 것이 파훼원의 확고한 입장이다.[55] 따라서 위법한 방법에 의해 수집된 증거는 증거로서의 효력이 없다. 예컨대, 은밀한 감시를 통해 알아낸 노동조합 활동을 근거로 해서 근로자에게 해고·징계와 같은 불이익을 주지 못한다.

또한, 노동법 제L120-2조는 "수행해야 할 직무의 성질에 의해 정당화되지 않거나 추구하고자 하는 목적과 균형을 이루지 아니하는 한, 누구도 개인의 권리와 개인적·집단적 자유를 제한할 수 없다."라고 규정하고 있다(비례성 원칙). 이 조항은 1980년 Corona사건 판결[56]에서 확립된 원칙을 노동법에 그대로 반

54) http://www.legifrance.gouv.fr/WAspad/UnCode?code=CTRAVAIL.rcv

55) Soc. 20 novembre 1991, Droit social, 1992, p.31; Soc. 22 mai 1995, Bull. civ. V. n°164. 특히 파훼원은 근무시간 중 내기에 빠져 있는 근로자나(Soc. 14 mars 2000, Bull. civ. V. n°101) 절도행위라는 무거운 비행을 저지른 근로자(Soc. 15 mai 2001, Bull. civ. V. n°167)에 대해서도 비밀감시로 획득한 증거에 의한 해고라는 이유로 사용자 패소를 인정하고 있다.

영한 것으로서 직장에서 근로자의 자유를 보장하는 '헌장'으로 생각되고 있다. 여기서 말하는 개인의 권리와 자유에는 직장에서의 통신비밀 등 근로자의 사생활권도 포함된다는 것이 통설이며, 판례에 따르면 근로자는 민법 제9조의 해석에 의해서도 근무중 자신의 사생활을 존중받을 권리가 있다고 한다.

한편, 노동법 제L432-2조와 L432-2-1조에 의하면 사용자는 근로자의 업무환경에 영향을 미치는 새로운 기술을 도입하거나 근로자의 활동을 감시할 수 있는 수단 또는 기술을 도입하고자 할 때에는 '사전에' 근로자위원회에 그 사실을 알리고 자문을 구해야 한다. 특히 중요하고 급진적인 변화를 추구하고자 하는 경우에는 미리 그 시스템의 도입계획을 근로자위원회에 제출해서 정보제공과 함께 자문을 구해야 하며, 그 계획의 시행에 있어서도 정기적으로 정보를 제공하고 주기적으로 자문을 구해야 한다(집단적 협상의 원칙). 사용자가 근로자에게 개별적으로 감시 계획을 알렸다고 하더라도 집단적 교섭절차가 면제되는 것은 아니다. 근로자 대표위원은 사용자가 도입하고자 하는 감시 시스템이 사생활침해라고 판단한 경우에는 사용자에게 문제를 제기할 수 있고, 이 경우 사용자는 즉시 사실을 조사한 후 필요한 조치를 취해야 한다. 만약 사용자의 조치가 부적절하거나 견해차가 있어 합의에 이르지 못한 경우에는, 해당 근로자의 반대가 없는 것을 조건으로, 근로자대표위원은 노동심판소에 조정을 신청할 수 있다. 근로자 대표위원에게 부여된 이 같은 권한을 경고권(droit d´alerte)이라고 한다.

2) 1978년 정보와 자유법

「1978년 정보처리·파일및자유에관한법률(Loi n° 78-17 du 6 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés)」은 프랑스 노동법과 더불어 모든 공·사 영역에 있어서 근로자 프라이버시 보호에 매우 중요한 법이다. 이 법은 사기적이거나 불성실하거나 위법한 방법에 의한 개인정보의 수집을 금지하는 한편(제25조), 자기에 관한 정보처리에 대해 알 권리(제3조), 이의를 제기할 권리(제26조), 자기정보에 대한 접근권·정정권·삭제권(제34조 내지 제40조) 등을 규정하고 있다. 또한, 사용자가 근로자 감시 시스템을 도입하고자

56) C.E. 1er fevrier 1980. *Droit social*, 1980, p.317.

하는 경우에는 미리 이를 국가정보처리자유위원회(CNIL)에 신고하여야 한다(제16조). 명백히 사생활 침해 가능성이 없는 경우에도 사용자는 개인정보를 처리하기 위해서는 간편한 서식(norme simplifiee)에 의한 약식신고(declaration simplifiee)를 해야 한다(제17조).

근로자는 CNIL에 불만이나 진정을 제기할 수 있고 이에 대해 CNIL은 문제해결을 위한 화해를 시도할 수 있다. CNIL은 이 법률의 준수 여부를 감시·감독할 의무를 지며, 근로자의 신청이나 제보가 없어도 직권에 의해 사용자의 정보시스템을 출입·검사할 수 있다. 이 밖에 CNIL은 법률적으로 구속력 있는 의견제시와 권고를 할 수 있고, 임무수행에 필요한 규칙을 제정할 권한을 가진다(제6조, 제14조 및 제21조). 이상과 같은 권한과 의무에 근거해 CNIL은 2003년 2월 5일 「직장에서의 사이버감시(La cybersurveillance sur les lieux de travail)」[57]라고 하는 안내서를 작성하여 공표한 바 있다.

안내서 중 전자우편 감시와 관련된 주요 내용은 다음과 같다. 첫째, 직장에서 근로자가 사용하고 있는 컴퓨터는 사용자 소유이며 업무처리를 위한 것이지 근로자의 사적인 이용을 위한 것이 아니다. 따라서 전자우편 이용에 관한 사용자 측의 요구와 근로자의 프라이버시를 조화시키기 위해서는 노사간 집단교섭을 통해 전자우편 감시에 관한 원칙을 수립해야 한다. 정보기기에 대한 이용제한은 근로자의 행위에 대한 제약을 부과하는 것이므로 취업규칙으로 정할 필요가 있다.

둘째, 사용자의 전자우편 시스템에서 송·수신되어 사용자가 접근할 수 있는 전자우편은 일반적으로 업무적인 성질을 가진 것으로 추정된다. 따라서 전자우편의 제목이나 수신자가 저장해 둔 디렉토리 이름 등을 통해 사적 통신임을 가리키는 특별한 표시가 있는 경우에만 사적 통신으로 통신비밀의 보호를 받을 수 있다.

셋째, 사용자가 근로자에게 전자우편 감시 계획에 대해 고지만 하면 모든 형태의 감시를 할 수 있다고 생각하는 것은 잘못이다. 사생활 침해 위험을 배제하기 위해서는 종합적인 보안 계획(the total security plan)을 수립해 CNIL에 신고

57) http://www.cnil.fr/thematic/index.htm. 이 안내서의 작성 작업은 2001년 3월부터 시작되어 공개적인 자문을 거친 후 2002년 5월 최종적으로 채택되었다.

해야 한다. 다시 말해 감시 시스템을 도입하고자 하는 경우에는 근로자와 근로자위원회 외에 CNIL에도 신고하여야 한다. 사용자의 필요성과 근로자의 사생활 보호를 비교형량하여 최종적으로 감시의 타당성과 균형성을 판단하는 것은 행정 및 사법 당국의 몫이다.

넷째, 사용자는 네트워크의 보안·보호 및 통제를 위해 전자우편에 첨부되어 있는 파일의 빈도·크기를 측정하기 위한 장치나 주고받은 전자우편의 내용을 저장하기 위한 장치를 도입할 수 있다. 특히 송·수신자가 자신의 컴퓨터에서 전자우편을 삭제한 후에도 그 전자우편은 시스템에 저장되어 있을 수 있다. 이와 같은 통제장치나 백업장치를 이용하기 위해서는 근로자에게 미리 통지를 해야 하며 저장된 정보의 보존기간을 정해야 한다.

마지막으로 사용자가 근로자의 컴퓨터 시스템에 전자우편의 기능을 통제하는 장치를 도입하려고 할 때에는 미리 CNIL에 이를 신고하여야 하고, 메시지의 보존기간을 특정해야 한다. 신고서에는 근로자 대표 조직의 자문을 받은 내용과 그 일자가 기록되어 있어야 한다.

3) 판 례

파훼원에서 사용자에 의한 근로자의 전자우편 감시가 최초로 다루어진 사건은 2001년 10월 2일 Nikon France사건[58]이다. 결론부터 말하면 이 사건에서 파훼원은 '근로자가 자신의 사생활을 존중받을 권리가 있다'라고 하는 것은 근무시간 중 직장에서 자신이 송·수신한 전자우편의 내용에 대해서 사용자의 무단접근이 금지된다는 것을 의미하는 것이라고 판시하고 있다.

사건의 논점은 사용자가 전자우편시스템의 개인적인 사용을 명시적으로 금지하고 있다고 하더라도 업무를 처리하는 과정에서 회사의 컴퓨터를 이용해 근로자가 송신한 '사적인' 전자우편을 감시하는 것은 정당화될 수 없다는 것이다. 부수적으로 판례는 전자우편이나 인터넷의 제한적이고 일상적인 이용은 근로자의 직장생활에 큰 영향을 미치지 않기 때문에 이러한 일상적인 전자우편의 이용은 허용되어야 한다고 보고 있다.

파훼원 사회부는 "근로자는 직장에서 근무시간 중이라도 사생활의 내면의 존

58) Soc. 2 octobre 2001, *Droit social*, 2001, p.920.

중을 요구할 권리를 가진다. 특히 여기에는 통신비밀(secret des correspondances)이 포함된다. 근로자가 업무처리를 위해서 사용하고 있는 정보통신기기를 이용해 송·수신한 자신의 사적인 전자우편을 사용자가 조사하는 것은 기본적인 자유를 침해하는 것이 된다. 이것은 업무처리 활동 이외에는 컴퓨터의 사용을 금지하고 있는 경우에도 마찬가지이다..... 사용자가 조사한 근로자의 전자우편에는 '사적인' 우편임을 나타내는 제목이 붙은 파일이 포함되어 있다. 이것은 원심이 유럽인권규약 제8조, 민법 제9조, 민사소송법 제9조 및 노동법 제L120-2조의 규정에 위반한 것을 의미한다."라고 판시하고 있다. 아울러 파훼원은 전자우편에는 업무적인 것인지 사적인 것인지를 구분할 수 있는 표시가 포함되어야 한다고 제안하고 있다.

그러나 이 판결이 어떤 경우에도 사용자는 근로자의 '사적인 전자우편'을 조사·감시할 수 없다는 것을 인정한 판례로 해석되어서는 안 된다. 사용자에 의한 전자우편의 열람·개봉이 정당한지 여부에 대해서는 사안별로 그 구체적인 타당성 여부를 검토해야 한다. 이 사건에서 파훼원은 노동법 제L120-2조에서 규정하고 있는 근로자의 기본적 자유와 권리에 대한 제한을 문제삼고 있다. 동조의 해석상으로도 직무의 성질에 의해 정당화되는 경우에는 근로자의 자유나 권리도 제한이 가능하다고 해석되어야 한다.[59] 또한 통신비밀 보호도 기업의 불가결한 이익과 어울리지 않으면 안 된다. 따라서 근로자의 자유보다도 더 중요한 다른 이익—예컨대, 기업의 영업비밀보호 등—이 있다면 근로자의 권리는 양보되어야 한다. 여기에 적용되는 원칙이 바로 앞에서 설명한 비례성의 원칙 또는 균형의 원칙이다.

다만, 프랑스에서는 근로자의 권리와 자유에 대한 제한을 인정하는 예외에 대해서는 엄격하게 해석되고 있다는 사실을 잊어서는 안 된다. 예컨대 '회사에게 중대한 지장을 줄 위험이 있다'라고 하는 판단은 매우 한정적으로만 인정된다. 따라서 근로자의 개인적인 전자우편을 열어볼 수 없다고 하는 것이 어디까지나 원칙이며 '열어볼 수 있다'고 하는 것은 매우 예외적이라는 인식이 강하다는 것을 알 수 있다.

---

59) ANTONMATTEI(P.-H.), NTIC et vie personnelle au travail, *Droit social*, 2002, p.41.

### 라. 일 본

일본은 지금까지 다른 선진국에 비해 개인정보보호의 중요성에 대한 인식이 상대적으로 낮고 개인정보보호제도도 상당히 뒤처져 있었다고 할 수 있다. 1988년 「행정기관이 보유하는 전자계산기처리에 의한 개인정보보호에 관한 법률(行政機關の保有する電子計算機處理に係る個人情報の保護に關する法律)」이 제정된 이래, 민간부문에서의 개인정보처리에 대해서는 이렇다고 할 제도적 발전이 없었다. 대부분 행정지침, 시·정·촌의 조례, 그리고 기업의 자율규제에 의존해 오다가 2003년 5월 민간·공공부문 양 영역에 걸쳐 개인정보보호제도에 큰 변화가 있었다.

민간부문과 공공부문에서의 개인정보처리를 모두 규율의 대상으로 하면서도 특별히 민간부문의 개인정보처리에 초점을 둔 「개인정보보호에 관한 법률(個人情報のに保護關する法律)」이 제정되었으며, 공공부문의 개인정보처리를 대상으로 한 「행정기관이 보유하는 개인정보보호에 관한 법률(行政機關の保有する個人情報の保護に關する法律)」과 「독립행정법인 등이 보유하는 개인정보보호에 관한 법률(獨立行政法人等の保有する個人情報の保護に關する法律)」도 제정되었다. 또한, 이들 법률의 시행을 지원할 조직법으로서 「정보공개·개인정보보호심사회설치법(情報公開·個人情報保護審査會設置法)」도 제정되었다.

한편, 판례는 사용자에 의한 근로자의 감시, 미행, 촬영 등이 직장에서의 인간관계 형성의 자유를 침해한다거나 사생활의 자유를 침해할 수 있다고 하여 근로자에게 유리한 판결을 내린 적도 있으나,[60] 사용자에 의한 개인정보의 수집 방법이나 수단이 아주 악질적이거나[61] 지극히 중요한 개인정보의 누설인 경우[62]를 제외하고는 근로자에게 우호적이지 않다. 따라서 판례법상 근로자의 개인정보를 보호하기 위한 법리의 발전은 거의 없었다고 할 수 있다.

---

60) 關西電力事件, 最3小判平成7·9·5勞働判例680号29쪽.

61) 근로자 대기실에 도청장치를 설치한 사건(岡山電氣軌道事件岡山地判平成3·12·17勞動判例606号50쪽) ; 자동차 교습용 차량에 녹음기를 무단 설치한 사건(廣澤自動車學校事件德島地判昭和61·11·17勞働判例488号46쪽) 등.

62) HIV 감염자 해고 사건(東京地判平成7·3·30勞動判例667号14쪽).

1) 2003년 개인정보보호에 관한 법률

2003년 5월 시행된 「개인정보보호에 관한 법률」은 일본에 있어서 개인정보보호에 관한 기본법이라고 할 수 있다. 비록 근로자의 개인정보보호만을 대상으로 하는 법률은 아니지만 사용자에 의한 근로자의 전자우편 감시도 이 법에 의해 규율받게 된다. 이 법은 유럽이나 다른 선진 제국과는 달리 개인정보보호 시책의 수립·집행 업무를 독립된 전문·전담조직에 맡기지 않고 각 행정부처가 소관업무에 대해서 각자 시책을 추진하도록 하고 있다. 이에 따라 근로자의 개인정보보호에 관해서는 후생노동성이 2004년 4월 2일 「고용관리에 관한 개인정보의 적정한 취급을 확보하기 위해 사업자가 강구해야 할 조치에 관한 지침」을 제정·고시하였으나 동 지침은 선언적 규정만 담고 있어 여기서는 2000년 제정·고시된 「노동자의 개인정보보호에 관한 행동지침」을 중심으로 살펴본다.

2) 2000년 노동자의 개인정보보호에 관한 행동지침

2000년 지침은 구 노동성이 「1995년 EU 개인정보보호지침」과 「1996년 ILO 근로자 개인정보보호 실행규약」의 영향을 받아 제정한 것으로 법적인 효력을 가지는 것은 아니다. 그러나 노동관계에 있어서 근로자의 개인정보보호를 위하여 채택된 일본 최초의 행정지침이라는 점에 그 의의가 있다.

이 지침은 직장 내에서 근로자들의 개인정보가 적정하게 처리되도록 하기 위하여 필요한 사항을 규정함으로써 개인정보의 원활한 처리를 배려하고 동시에 근로자의 프라이버시를 보호하기 위한 사내 규정 등의 정비를 지원·촉진하는 것을 목적으로 제정된 것이다. 원칙적으로 민간기업에 종사하는 근로자들을 대상으로 하므로 공공부문에 종사하는 근로자들에 대하여는 이 지침이 적용되지 아니한다.

지침은 전자우편 감시를 포함하여 컴퓨터 등에 의한 모니터링을 실시할 때에는 사용자가 미리 근로자에게 감시이유, 감시시간대, 수집되는 정보의 내용 등을 통지하여야 하고 개인정보보호에 대한 근로자의 권리를 침해하지 않도록 배려할 것을 요구하고 있다(제2절제6조제4항). 또한 컴퓨터 등의 자동처리시스템이나 비디오 등에 의한 모니터링 시스템을 도입하고자 하는 경우에는 미리 노

동조합 등에 통지해서 협의를 하도록 요구하고 있다(제4절제1조).

3) 판 례

최근 사용자에 의한 근로자의 전자우편 감시와 관련한 판례가 종종 등장하고 있으나 근로자의 프라이버시 보호라고 하는 관점에 있어서는 충분한 검토가 이루어지지 않고 있다는 비판이 있다.

가) F사 Z사업부 사건(2001년)

동경지방재판소 민사 40부는 2001년 12월 3일 근로자의 사적인 전자우편을 직장상사가 무단으로 열람한 사건[63]에서 프라이버시침해를 이유로 한 근로자의 손해배상청구를 기각하였다. F사의 사업부장 겸 이사인 피고는 영업부장 보조인 원고(여)가 남편에게 보내려다 잘못하여 자신에게 전달한 전자우편을 통해 자신을 상대로 한 성희롱 고소 움직임이 있음을 간파하고 원고의 비밀번호를 이용해 서버에 남아 있는 원고의 전자우편을 열어보았다. 원고가 비밀번호를 변경해 버리자 이번에는 회사 IT부서에 의뢰해 원고의 전자우편이 자동적으로 피고에게 전송되도록 조치하여 감시를 계속했다.

당시 F사는 근로자 각자에게 전자우편 주소와 비밀번호를 하나씩 부여하고 있었고 전자우편은 주로 사내 연락수단으로 이용되고 있었다. 근로자들의 전자우편 주소는 사내에 공개되어 있었으며 비밀번호는 통상 자신의 이름을 사용하도록 되어 있었다. F사의 미국 본사는 전자우편의 개인적인 이용을 금지하는 방침을 정해 근로자들에게 이를 주지시키고 있었지만 F사는 이런 절차가 없었다. 개인적인 이용에 대한 금지도 철저하지 못했으며, 개인적 이용에 대한 조사·감시 지침도 없었고 열람 가능성에 대한 고지도 없었다.

법원은 "업무를 방해하지 않고 회사에 끼친 경제적 부담도 경미한 경우 사회생활상 필요한 외부로부터의 연락에 즉응하기 위해 필요한 합리적인 범위 내에서 전자우편을 수·발신하는 것은 사회통념상 허용된다. 이는 회사의 전화장치와 다를 바가 없다."고 밝히고 있다. 그러나 전자우편은 전화와 똑같은 정도의 프라이버시 보호를 기대할 수는 없고 해당 시스템의 구체적인 상황에 따라 합

63) F社Z事業部(電子メール)事件東京地判平成13·12·3勞働判例826号76쪽.

리적인 범위 내에서의 보호를 기대할 수 있음에 그친다고 한다.

전화에서는 보수(保守)·점검이 법적인 수비의무(守秘義務)를 지고 있는 전기통신사업자에 의해서 행해지고 대화의 내용도 즉시 사라져버림에 반해서, 전자우편은 일정 범위 내에서 통신내용이 사내 통신시스템상의 서버나 단말기에 저장되어 있고 사내 통신시스템은 당해 회사의 전산관리자가 네트워크 전체를 감시하면서 보수(保守)하는 것이 일반적이기 때문이라고 한다. 특히 이 건에서는 전자우편 주소와 비밀번호가 이미 사내에 공개되어 있었기 때문에 근로자가 사내 네트워크를 이용해 전자우편을 개인적인 용도로 이용할 경우 기대할 수 있는 프라이버시의 보호 범위는 전화장치에서 통상 기대할 수 있는 것보다 상당한 정도로 축소된다고 한다.

또한 감시의 목적, 수단 및 그 태양 등을 종합적으로 고려해 감시를 받는 측에게 발생한 불이익을 비교형량한 다음, 사회통념상 상당한 범위를 일탈한 감시가 행해진 경우에 한해 프라이버시권의 침해가 인정된다. 상당한 범위를 일탈한 감시의 예로는 전자우편의 이용을 감시할 책임이 없는 자가 감시한 경우, 감시 책임이 있는 자라도 업무상 필요성에서가 아니라 개인적인 호기심 등에서 감시한 경우, 관리부서나 사내의 제3자에 대해 감시사실을 비밀로 한 채 개인의 자의에 기초한 수단과 방법으로 감시를 행한 경우 등을 들고 있다.

이상의 상황을 종합적으로 검토한 후, 동경지방재판소는 감시 적격자로서 피고의 지위와 감시의 필요성을 인정하였다. 비록 피고가 성희롱 혐의를 받고는 있었지만 사업부의 최고책임자로서 달리 적당한 다른 감시자를 찾기 어렵고, IT부서에 의뢰해서 감시를 행하였으므로 전적으로 개인적인 감시활동을 한 것도 아니라는 것이다. 이에 비해 원고의 사내 전자우편 이용 정도는 사회적으로 허용되는 수준을 넘어섰고, 원고가 피고의 전자우편 감시를 유발한 책임이 있으므로, 피고에 의한 감시행위가 사회통념상 상당한 범위를 넘어선 것이라고 할 수 없을 뿐만 아니라 원고가 법적인 보호를 받아야 할 정도로 중대한 프라이버시 침해를 받았다고 할 수도 없다고 결론지었다.

이러한 판례의 입장에 대해서는 재판부가 전자우편을 단지 개봉 엽서처럼 생각하고 있다는 등의 여러 비판과 함께, 일본 근로자들의 근무환경을 토대로 사무실 배치방법상 상사나 동료들에 의한 엿듣기가 쉬운 전화보다 그럴 위험이

적다고 믿고 있는 전자우편에 대해서 프라이버시 보호에 대한 근로자들의 기대가 더 큰 것이 아닌가 하는 의문이 제기되고 있다.[64]

나) 日經 퀵정보 사건(2001년)

이 건 역시 동경지방재판소가 다룬 직장내 전자우편 감시와 관련된 사건[65]으로, 사용자의 직장내 전자우편 감시의 정당성을 강력하게 옹호한 판례이다. 피고 회사는 사원들에 대한 비방·중상 사건을 조사하던 중에 의심스럽게 여겨진 원고들의 전자우편을 뒤졌지만 비방·중상의 증거는 찾을 수 없었다. 그러나 조사과정에서 원고들의 전자우편 서버에 다량의 사적인 전자우편이 저장되어 있는 것을 발견하게 되었고 이를 근거로 피고 회사는 원고들에게 견책이라고 하는 징계를 내렸다.

원고들은 프라이버시 침해라고 반발하였지만, 동경지방재판소는 후지(富士) 중공업사건[66]에 대한 최고재판소 판결의 법적 판단을 인용하여 사용자는 기업질서유지 권한에 근거해 질서위반행위에 대한 조사를 실시할 수 있다고 밝혔다. 그러나 이 경우 사용자의 조사가 적법한 행위로서 불법행위를 구성하지 않기 위해서는 첫째, 조사가 필요하고 합리적일 것, 둘째, 조사의 방법이나 행태가 근로자의 인격이나 자유에 대한 지나친 지배나 구속이 아닐 것이라는 두 가지 요건을 구비하여야 한다고 한다.

이 사건에서 재판소는 근로자가 직장에서 개인적인 전자우편을 주고받는 것은 "업무전념의무에 대한 위반이며..... 기업질서 위반행위"에 해당하여 징계처분의 대상이 된다고 판시하였다. 또한 조사의 상당성이 있었는지에 관해서도 파일 서버상에는 "무엇인가 업무와 관련된 정보가 보존되어 있다고 판단되기 때문에..... (파일서버의 데이터에 대한 조사는) 사회적으로 허용될 수 있는 한계를 넘어 원고의 정신적 자유를 침해한 위법한 행위였다고는 할 수 없다."는 것이 판례의 입장이다.

---

64) 眞嶋理惠子, NBL 제734호(2004.4.1), 6~7쪽.
65) 日經くいっく情報(電子メール)事件東京地判平成14·2·26勞働判例825号50쪽.
66) 最3小判昭和52·12·13民集31卷7号1037쪽.

# Ⅲ. 전자우편감시 규제에 관한 국내 법제도 및 판례 현황

우리나라에서는 전자우편의 이용 및 규제와 관련한 법률의 수가 적지 아니하고, 최근 인터넷의 급속한 보급 확대로 전자우편 도·감청과 관련한 소송도 심심치 않게 발생하고 있다. 이 중 전자우편의 도·감청을 직접적으로 규율하고 있는 법률로는 통신비밀보호법, 정보통신망이용촉진및정보보호등에관한법률, 전기통신사업법 등이 있다.

그러나 전자우편이 가지고 있는 기술적 특성이나 업무환경에 미칠 수 있는 영향에 대한 충분한 고려 없이 입법이 추진된 결과, 전자우편을 전화 또는 봉함서신과 동일한 수준에서 엄격하게 보호하고 있다. 판례 역시 실정법의 규정을 엄격하게 해석하여 근로자의 사생활보호를 기업의 이익보다 우선적으로 보호하고 있는 경향이다.

이로 인해 사용자가 근로자의 전자우편을 적법한 방법으로 감시하는 것이 사실상 어려우며, 게다가 직장에서의 전자우편 감시를 위한 행정지침이나 업계의 자율적 가이드라인도 전무한 상태여서 비밀스럽고 음성적인 감시가 급속히 늘고 있다.

## 1. 법적 규제

### 가. 통신비밀보호법

현행 통신비밀보호법 제3조제1항은 "누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다."라고 규정하고 있다. 여기서 말하는 전기통신에는 전화, 팩스, 무선호출 등의 유·무선 통신 외에 명문의 규정으로 전자우편도 포함된다(제2조제3호).

전기통신이 행해진 시설의 소유, 전기통신이 행해진 장소, 전기통신의 주체 등에 대하여 특별한 제한을 두고 있지 아니하므로 당연히 직장 내에서 근로자 상호간 또는 근로자와 제3자 간에 이루어진 전자우편도 이 법에 의해 보호를 받는다. 즉 이 법에서 말 하는 '누구든지'에는 국가기관뿐만 아니라 제3자, 사용자, 동료 근로자도 포함된다. 제3조제1항 단서는 통신비밀보호 규정의 적용이 제한될 수 있는 몇 가지 예외사항을 규정하고 있지만, 미국, 영국 등과는 달리 당사자의 동의에 의한 예외, 서비스제공자의 예외, 사실의 입증을 위한 예외, 규범 준수 여부를 확인하기 위한 예외, 범죄탐지를 위한 예외, 시스템의 보안과 효율적 운영을 위한 예외 등은 인정되고 있지 않다. 원칙적으로 범죄수사, 국가안전보장 등 공공 목적으로만 예외가 인정된다.

다만, 이 법 제2조제7호가 "감청이라 함은 전기통신에 대하여 '당사자의 동의 없이' 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다."라고 규정하고 있으므로 이를 역으로 해석하면 '당사자의 동의가 있으면' 전자우편의 감시가 가능하다는 해석이 가능하다.[67] 그러나 문제는 동의 방법에 대한 명확한 규정이 없기 때문에 이 경우 당사자 쌍방의 동의를 다 받아야 하는 것인지, 일방의 동의만 받아도 되는 것인지에 대해서 학설상 다툼이 일고 있다.[68] 우리나라 통신비밀보호법의 모델이었던 미국의 「전자통신프라이버시보호법」(§2511(2)(d))과 1999년 공포된 일본의 「범죄수사를 위한 通信傍受에 관한 법률」(제2조제2호)[69]은 당사자 일방의 동의만 있으면 되는 것으로 되어 있고, 이에 비해 영국과 독일은 당사자 쌍방의 동의를 요구하고 있다. 통신은 그 성격상 상대방의 존재를 전제로 한 것이기 때문에 명문의 규정이 없는 이상 당연히 당사자 쌍방의 동의를 받아야 되는 것으로 해석해야 할 것이다.[70]

---

67) 황성기, 「통신제한조치의 헌법적 한계와 구체적 통제방안」, 한국정보법학회 제14차 세미나, 1999.11.23.

68) 학설간의 다툼에 대해서는 황성기, 앞의 논문, 각주 6) 참조.

69) 犯罪捜査のための通信傍受に關する法律(http://www.shugiin.go.jp/itdb_housei.nsf/html/housei/h14137.htm)

70) 대법원은 통신의 일방 당사자가 상대방의 동의를 얻지 않고 일방적으로 통화내용을 녹음한 행위는 통신비밀보호법 제3조제1항이 금지하고 있는 불법감청에 해당하지 아니하나,

이 법에 의해 보호를 받은 통신비밀의 범위에는 통신내용 그 자체뿐만 아니라 통신사실확인자료, 예컨대 가입자의 전기통신일시, 전기통신개시·종료시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수, 컴퓨터통신 또는 인터넷의 로그기록자료, 발신기지국의 위치추적자료 등도 포함된다.

이 법이 가지는 특징 중 하나는 불법감청에 의해 채득한 전기통신내용을 증거로 사용하는 것을 금지하고 있다는 점이다. 우리나라에서는 일반적으로 불법적으로 수집된 증거도 재판과정에서 증거로 채택될 수 있다. 그러나 이 법은 "제3조의 규정에 위반하여 불법감청에 의해서 지득 또는 채록된 전기통신 내용은 재판 또는 징계절차에서 증거로 사용할 수 없다."(제4조)고 규정함으로써 불법감청 금지에 대한 입법 의지를 강하게 표시하고 있다. 이 규정은 해고, 감봉, 견책 등 사용자에 의한 징계절차에도 동일하게 적용된다고 보아야 할 것이다.

### 나. 정보통신망이용촉진및정보보호등에관한법률

현행 「정보통신망이용촉진및정보보호등에관한법률」은 정보통신기술의 발달과 이용 확대로 인한 이용자들의 프라이버시 침해에 적절히 대응하고 권리를 보호하기 위해 OECD 프라이버시 8원칙에 준해서 개인정보의 수집·처리 및 이용에 관한 원칙을 규정하고 있다(제22조 내지 제40조). 오늘날 개인정보의 처리가 대부분 컴퓨터와 정보통신망을 통해 이루어지고 있기 때문에 이 법은 민간부문의 개인정보를 보호하는 우리나라의 대표적인 법률로 이해되고 있다.

그러나 이 법은 정보통신서비스제공자와 그 이용자 사이에서 발생한 개인정보의 수집·처리 및 이용 행위에 대해서만 적용되므로 사용자와 근로자 간에는 적용되지 않는다. 다만, 법 제49조가 "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니된다."라고 규정하고 있어 사용자에 의한 근로자의 전자우편

---

제3자가 전화통화 당사자 일방으로부터만 통화내용 녹음에 대한 동의를 얻고 상대방에게는 동의를 얻지 않은 경우에는 위와 달리 봐야 할 것이라면서 사생활 및 통신의 불가침을 국민의 기본권의 하나로 선언하고 있는 헌법규정과 통신비밀의 보호와 통신의 자유신장을 목적으로 제정된 통신비밀보호법의 입법취지를 고려할 때 이는 동법 제3조제1항이 금지하고 있는 불법감청에 해당된다고 해석하여야 한다고 판시하고 있다(대법원 2002. 10. 8., 2002도123; 이창범·장민영, 「국내외 개인정보판례분석」, 개인정보분쟁조정위원회, 2003, 40~41쪽).

감시에 대해서도 이 규정을 적용할 수 있을지가 문제이다. 우선 동조는 침해주체를 한정하지 아니하고 '누구든지'라고 규정하고 있기 때문에 침해자라는 측면에서는 사용자도 포함됨이 분명하다. 그러나 훼손·침해·도용·누설 등의 행위로부터 동조에 의해서 보호받는 정보는 '타인의 것'에 한정된다. 따라서 사용자가 제공하는 전자우편시스템을 이용해 업무중에 주고받은 전자우편의 소유가 여기서 문제될 수 있다.

근로자에게 개인별로 제공되고 비밀번호에 의해서 보호되는 전자우편계정으로 주고받은 전자우편이라 하더라도 업무와 관련된 것이라면 사용자의 소유라고 할 수 있을 것이다. 그러나 사용자의 전자우편시스템을 이용해서 주고받은 전자우편이라도 그 내용이 근로자의 신변과 관련된 개인적 성격의 것일 때에는 그 전자우편의 소유가 사용자의 것인지 근로자의 것인지가 불분명해진다. 전자우편은 보안이나 시스템의 안정적 운영을 위해 상시적인 감시가 불가피하기 때문에 검열이 엄격히 금지되고 있는 우편물과는 달리 개인적인 전자우편이라고 해서 무조건 근로자의 소유라고 단정짓기는 어려운 측면이 있기 때문이다. 더구나 전자우편 내용 중에 업무적인 것과 개인적인 것이 혼합되어 있는 경우에는 더욱 문제가 복잡해진다.

전자우편의 제목 등을 통해 명백히 개인적인 통신임을 나타내는 표시가 없는 한 사용자의 소유로 보는 것이 타당할 것이다. 그러나 명백한 개인적 통신에 대해서는 사용자가 제공한 통신시스템상의 전자우편에 대하여도 제49조가 적용될 수 있다고 본다.

### 다. 전기통신사업법

전기통신사업법 제54조는 "누구든지 전기통신사업자가 취급중에 있는 통신의 비밀을 침해하거나 누설하여서는 아니된다."(제1항)라고 규정함과 동시에, 전기통신업무에 종사하는 자 또는 종사하였던 자에게도 그 재직중에 통신에 관하여 알게 된 타인의 비밀을 누설하지 못하도록 하고 있다(제2항). 업무처리를 위해 전자우편시스템을 설치·운영하고 있는 사용자를 '전기통신사업자' 또는 '전기통신업무에 종사하는 자'라고는 볼 수 없을 것이므로 사용자에게는 제2항의 규정은 적용되지 않는다.

그러나 제1항은 누구든지 '전기통신사업자가 취급중에 있는 통신'에 대한 침해·누설을 금지하고 있으므로 인터넷을 통한 전자우편에 대해서도 동조가 적용될 수 있는지가 문제될 수 있다. 사내 통신망, 즉 인트라넷을 이용한 전자우편의 송·수신에 대해서는 전기통신사업자가 관여할 여지가 없지만, 인터넷을 이용한 전자우편의 송·수신시에는 전기통신사업자가 제공한 통신망을 이용할 수 밖에 없다. 따라서 전기통신사업자의 통신망을 통과중에 있는 전자우편은 전기통신사업자가 취급중인 통신이라고 할 수 있다.

그러나 사용자에 의한 전자우편의 감시는 일반적으로 자신이 설치·운영하고 있는 통신시스템 내에서 행해지므로 이 단계에서의 전자우편은 이미 '전기통신사업자가 취급중에 있는 통신'이라고 보기는 어렵게 된다.

## 2. 판 례

대다수 나라에서 법원은 전자우편과 전화를 가능한 한 구분해서 취급하려고 노력한다. 예컨대, 미국, 영국, 일본은 물론 유럽 국가들 중에서도 근로자의 사생활을 가장 철저히 보호하고 있다고 하는 프랑스에서조차도 전자우편은 전화에 비해 프라이버시에 대한 기대 가능성이 상대적으로 낮은 것으로 인식되고 있으며, 사용자에 의한 전자우편 감시 자체를 금지하고 있지는 않다.

그러나 우리나라의 법원들은 원칙적으로 전자우편을 전화와 거의 같은 것으로 취급하고 있는 것으로 보이며, 양자를 구분해서 취급해야 할 필요성을 별로 느끼지 못한 것으로 생각된다. 비록 대부분의 사건이 업무적인 전자우편과 관련된 사건이 아니고 개인적인 전자우편에 대한 감시와 관련된 것이긴 하지만 통신비밀보호에 대한 법원의 엄격한 잣대를 확인할 수 있다.

전자우편의 무단 열람 또는 감청과 관련한 최근의 판례 몇 개를 살펴보기로 한다.

### 1) 회사 간부가 다른 간부의 전자우편 등을 열람·감청한 사건(2002년)

이 사건[71]은 우리나라에서는 처음으로 법원에서 직장내 전자우편에 대한 감

71) 서울지법 2002. 9. 10., 2002고단3514 및 대법원 2003. 8. 22, 2003도3344.

시가 다투어진 사건이다. S사의 감사 A1은 원고1이 회사의 신용과 명예를 훼손하는 것으로 의심하여 이를 밝히기 위해 회사 사무실에서 원고1의 노트북 컴퓨터의 전자우편계정에 침입하여 전자우편을 열어보고 노트북 컴퓨터 내에 저장되어 있는 개인적인 문서를 열람하였다. 한편 S사의 간부인 A2는 다른 간부인 원고2가 회사의 어려운 사정을 언론에 유출하여 회사를 어렵게 만들었다고 생각하고 해고할 근거를 찾기 위해 직원 A3를 시켜 원고2의 전자우편과 컴퓨터 내의 문서를 열람하도록 지시하였고 그 직원으로부터 여러 차례 원고2에 관한 보고를 받았다.

이에 대해 서울지방법원은 피고 A1, A2, A3가 원고의 전자우편을 열람한 행위는 구 통신비밀보호법(2001.1.8 법률 제06346호) 제2조제7호의 감청에 해당되는바, 비록 회사의 신용과 명예를 훼손하는 것을 밝히기 위한 것이었다 할지라도 전자우편과 전자문서를 무단으로 열람하는 것은 전기통신의 무단 감청을 금지하고 있는 동법 제3조의 규정에 위반한 것이며, 동시에 정보통신망에 의하여 처리·보관·전송중인 타인의 비밀에 대한 침해를 금지하고 있는 정보통신망이용촉진및정보보호등에관한법률 제49조의 규정에도 위반된다고 판시하였다.

이에 대해 항소심 재판부는 "구 통신비밀보호법에 의하면 감청행위는 통신행위와 동시에 이뤄질 것이 요구된다고 해석되므로 송·수신이 완료된 전기통신의 내용을 지득·채록하는 것은 감청에 해당되지 않는다."고 하여 통신비밀보호법 제3조제1항 위반 혐의에 대해서는 무죄를 선고하고 정보통신망이용촉진및정보보호등에관한법률 제49조 위반 혐의에 대해서만 유죄를 인정하였다.

한편, 상고심인 대법원 형사2부 역시 피고에 대해 정보통신망이용촉진및정보보호등에관한법률 위반 혐의만을 인정하고 원심의 형을 확정하였다.

2) 사립학교 교장 등이 교사들의 전자우편을 열람·감청한 사건(2003년)

대법원의 확정판결과는 달리, 앞 사건의 1심 판례에 이어 본 사례[72]에서도 1심법원은 전자우편 열람·감청행위를 통신비밀보호법 제3조제1항 위반으로 다루고 있다.

K학교재단 소속의 T중·고등학교는 2003년 5월 교사와 학생의 컴퓨터를 연

72) 인천지방법원 부천지원 2004. 5. 14., 2003고단2107.

결하여 개별 또는 그룹별 교육이 가능하도록 고안된 교육용 원격강의시스템인 일명 '넷오피스쿨'이라는 컴퓨터 프로그램을 재단 소속 85명의 교사들이 사용하는 학교 컴퓨터에 일괄 설치하였다. 이 프로그램은 교장, 교감, 정보교사 등이 사용하는 컴퓨터를 주 컴퓨터로 지정하도록 되어 있었다. 또한, 주 컴퓨터를 사용하는 사람은 다른 교사들의 인터넷 통신내용을 임의로 열람·지득할 수 있게 프로그램화되어 있었다.

이를 기화로 T중학교 교장 A1과 T고등학교 교장 A2 그리고 그 고등학교 행정실장 A3는 상호 공모하여 2003년 5월부터 지속적으로 위 학교 교사 85명이 사용하는 컴퓨터에 무단 접근하여 개인적인 통신내용을 감청하였으며, 6월 중순경에는 O모 교사가 근무시간 중 남편과 인터넷 통신을 하였다는 이유로 그 교사를 학교 징계위원회에 회부한 후 통신내용을 징계위원들에게 공개하였다.

이에 대해 인천지방법원 부천지원은 A1, A2 및 A3의 감청행위는 누구든지 전기통신을 감청하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못하도록 규정하고 있는 통신비밀보호법 제3조에 위반한 불법적인 감청임을 인정하였으며, 동시에 감청된 통신내용을 공개한 행위에 대해서는 누구든지 지득한 통신 또는 대화의 내용을 공개하거나 누설할 수 없다고 규정하고 있는 통신비밀보호법 제16조제1항제2호의 규정에 위반한 통신내용의 불법적인 누설이라고 판시하였다.

3) 애인의 전자우편 이용내역을 무단으로 열람한 사건(2001년)

이 사건[73]은 개인 사이에 전자우편이 불법 감청된 사례이다. 피고는 자신의 여자친구가 다른 남자와 사귀는지를 감시하기 위하여 2000년 2월부터 같은 해 7월까지 이미 알고 있던 여자친구의 전자우편 계정과 추측으로 알아낸 비밀번호를 이용하여 여자친구의 전자우편 83통을 무단으로 열람하였고, 2001년 1월부터 같은 해 7월까지는 평소 알고 있는 여자친구의 ID와 주민등록번호 그리고 추측으로 알아낸 비밀번호를 이용하여 7회에 걸쳐 여자친구가 사용하고 있는 이동통신사의 웹사이트에 접속하여 여자친구의 이동전화 사용내역을 열람하였다.

---

73) 서울지법 2001. 4. 1., 2001고단9396.

이에 대해 서울지방법원은 피고가 이미 알고 있거나 추측으로 알아낸 전자우편 계정과 비밀번호를 이용하여 여자친구의 전자우편, 이동전화 사용내역 등을 무단으로 열람한 행위는 당사자의 동의없이 전기통신을 감청한 것이므로 통신비밀보호법 제3조 위반이며, 동시에 보호조치를 침해하여 정보통신망에 의해 처리·보관 또는 전송되는 타인의 비밀을 침해한 것이므로 구 정보통신망이용촉진등에관한법률 제19조 및 제22조(현행 정보통신망이용촉진및정보보호등에관한법률 제49조)의 위반에 해당한다고 판시하였다.[74]

# Ⅳ. 사업장내 전자우편 감시제도 개선방안

## 1. 전자우편감시에 대한 법적 규제의 재검토

앞에서 살펴본 것처럼 미국, 영국, 프랑스, 일본 등 대다수 선진국에서는 전자우편 감시를 전화 도·감청과는 구분하고 있으며, 전자우편에 대해서는 사용자에게 상당한 정도의 감시를 허용하고 있다. 그러나 이들 국가간에도 감시를 허용하는 조건, 근로자의 보호수준 등에는 큰 차이가 있다. 미국의 경우 사용자의 컴퓨터 시스템을 이용한 전자우편에 대해서는 프라이버시 보호에 대한 근로자의 기대 가능성이 없다는 입장이다. 따라서 사용자가 근로자의 전자우편을 감시하겠다는 입장을 발표한 이상 근로자의 명시적인 동의가 없더라도 전자우편 감시는 가능하다고 본다. 이런 전제하에 있기 때문에 미국에서는 전자우편 감시에 관한 법적 요건이나 기준이 개발되어 있지 않다. 그만큼 사용자에 의한 전자우편 감시의 오·남용이 문제되고 있다. 일본도 상황은 미국과 매우 유사하다. 판례는 단지 감시가 필요하고 합리적일 것, 감시의 방법이나 행태가 근로자의 인격이나 자유에 대한 지나친 지배나 구속이 아닐 것이라고 하는 단서를 붙이고 있을 뿐이다.

이에 비해 프랑스에서는 전자우편 감시에 대해서 상당히 엄격한 조건과 절차를 요구하고 있다. 원칙적으로 사용자에 의한 비밀감시는 허용되지 아니하며,

74) 유사 사례로는 부산지법 2002. 1. 3., 2001고단5494 등 참조.

근로자의 사생활에 대한 침해가 최소한에 그치는 범위 내에서 정당한 이유가 있는 경우에만 합법화될 수 있다. 직무와 직접 관련이 없는 전자우편 감시는 근로자의 동의가 있어야만 가능하다. 또한 근로자 감시 시스템을 도입하기 위해서는 미리 법정 근로자대표에게 고지하고 협의를 해야 함은 물론 개인정보커미셔너(CNIL)에게도 신고하여야 한다. 이런 제도적 장치를 통해 사업장내 전자우편 사용과 관련한 사용자와 근로자의 이익을 조화시키고 있다. 영국도 전자우편 감시에 관한 정부기준은 전반적으로 프랑스와 유사하나 판례는 사업자에 다소 우호적이며 근로자대표와의 사전 협의의무도 없다.

반면, 우리나라는 실정법상 근로자의 전자우편 감시에 대한 예외가 거의 인정되지 않고 있다. 판례도 통신비밀보호에 매우 엄격한 입장을 보이고 있기 때문에 사용자가 기업의 영업비밀보호, 근로자의 불법행위 예방, 근무시간 중 무분별한 인터넷 이용억제 등과 같은 제한된 목적으로 근로자의 전자우편을 감시한다고 하더라도 법원에 의해서 불법감청, 정보통신망상의 비밀침해 등으로 처벌을 받게 될 가능성이 없지 않다. 그러나 근로자의 전자우편을 일반적인 통신비밀보호 또는 정보통신망상의 비밀보호와 같은 수준으로 보호하는 것은 문제가 있다. 사용자의 감독권에 기한 합리적인 전자우편 감시까지 금지할 경우 오히려 사용자에 의한 비밀감시를 조장할 우려가 있으며, 반대로 근로자들이 회사에서 제공한 전자우편 계정을 불법정보를 유포하거나 산업정보를 유출하는 수단으로 악용할 수도 있다.

따라서 사업장내 전자우편에 대해서는 일정한 조건하에서 감시를 허용하되, 투명하고 공개적으로 행해지도록 방법과 절차를 구체화 하여야 한다. 이 경우 입법자, 정책담당자 및 사용자들은 전자우편 내용에 대한 사후적 감시보다는 바람직스럽지 못한 전자우편의 이용을 사전에 차단하는 예방적 시스템의 도입에 보다 큰 관심을 가져야 할 것이다. 이하에서는 사용자의 정당한 이익을 보호하면서 동시에 근로자의 프라이버시 침해를 최소화하기 위한 몇 가지 방안을 제시하고자 한다.

## 2. 전자우편감시의 적법성 확보 방안

사용자가 근로자의 전자우편을 감시하기 위해서는 먼저 감시를 통해서 달성하고자 하는 궁극적인 목적이 무엇인지를 확정해야 한다. 영업비밀 등 업무상 비밀을 보호하기 위한 목적이라면 통신내용까지도 열람해 보아야 하기 때문에 매우 사생활 침해적인 방법을 도입할 수밖에 없다. 그러나 바이러스 유포, 스팸메일 발송, 명예훼손, 성추행, 차별행위 등과 같은 근로자들의 불법행위를 단속하거나 근로자들의 업무전념의무를 확보하기 위한 목적이라면 가능한 한 전자우편 내용을 열람하는 행위는 피해야 한다.

### 가. 절차상의 적법성 확보

어떤 경우에도 전자우편에 대한 비밀감시는 불법이다. 통신비밀보호법 제4조는 불법적인 감청으로 수집된 자료는 재판이나 징계절차에서 증거로 사용할 수 없도록 하고 있기 때문에(제4조) 근로자의 비행이 아무리 크더라도 비밀스런 방법으로 수집된 자료를 가지고는 근로자를 징계할 수도 없다. 따라서 사용자는 감시에 앞서 반드시 개별 근로자들의 동의를 구해야 하며 공개적으로 해야 한다.

업무적인 전자우편은 전자우편의 소유가 사용자에 속하고 근로자의 사생활과도 무관하므로 근로자의 동의가 없더라도 열람이 가능하다고 보아야 하겠지만, 아직 이에 관한 판례가 없으므로 안전한 감시를 위해서는 이 경우에도 가능한 근로자의 동의를 구하고 최소한 사전 고지가 필요하다고 본다. 특히 사적인 전자우편과 업무적인 전자우편이 뒤섞여 있을 경우 사적인 전자우편의 내용을 개봉해 보지 않았다 하더라도 제목의 열람만으로도 사생활 침해가 성립될 수 있으므로 주의해야 한다.

영국의 판례는 사용자가 근로자에게 전자우편에 대한 감시 방침을 분명히 고지했고 이를 알고도 근로자가 전자우편을 이용했다면 묵시적 동의가 있는 것으로 보고 있지만, 우리나라에서는 묵시적 동의가 인정될 가능성이 낮기 때문에 사용자는 사전에 근로자로부터 서면 형태의 동의서를 받는 것이 바람직하다.

그러나 적법한 절차에 의하여 전자우편의 이용과 제한에 관한 취업규칙이 제정되어 있다면 전자우편 감시에 대한 근로자의 동의가 있었다고 보아야 할 것이다. 가능한 한 근로자 대표에게 감시시스템의 도입 계획을 미리 알리고 자문을 구하는 것이 좋을 것이다.

문제는 근로자가 전자우편 감시에 대한 사용자의 동의 요구를 거부한 경우이다. 근로자가 동의를 거부한 경우 이를 해고 또는 징계의 사유로 삼을 수 있을 것인가? 해당 근로자가 맡고 있는 업무의 성질상 감시가 불가피한 경우라면 동의 거부를 해고사유로 삼을 수 있다고 본다. 그렇지 않은 경우는 근로자가 부당해고나 부당징계를 주장할 가능성이 높다. 따라서 이런 경우에는 해당 근로자에게 전자우편계정의 배급을 중단하거나 사적인 전자우편 사용금지에 관한 회사의 방침을 확인시킨 후 사적인 전자우편을 사용한 경우에는 그 정도에 따라 업무전념의무(충실의무) 위반으로 해당 근로자를 징계 또는 해고할 수 있을 것이다.

사용자가 근로자의 동의를 받을 때에는 사전에 ①사적인 용도의 전자우편 사용이 허용되는지 여부, ②송·수신이 허용되는 전자우편과 금지되는 전자우편의 유형, ③사용자가 업무용으로 배급한 전자우편계정 외에 다른 전자우편 계정의 사용이 허용되는지 여부, ④사적인 전자우편의 사용이 제한되고 있다면 송·수신이 허용되는 시간과 금지되는 시간, ⑤감시목적, ⑥감시방법(감시시스템의 특징을 포함한다), ⑦감시 시간대(또는 시기), ⑧감시장소, ⑨수집되는 정보의 내용 ⑩감시업무를 수행할 부서 및 담당자, ⑪감시를 통해 얻은 데이터의 보존기간 ⑫송·수신된 전자우편의 서버내 보존기간(삭제시기), ⑬근로자의 권리 등을 구체적으로 제시하고 상세히 설명해야 한다. 그리고 주기적으로 근로자들에게 전자우편 감시와 관련하여 사용자가 채택하고 있는 방침을 교육하고 주지시켜야 하며 전자우편 시스템에도 이를 게시하여야 한다. 또한, 이러한 내용들은 가능한 한 취업규칙에 반영되는 것이 바람직하다.

그러나 제3자가 송신자이고 근로자가 수신자로 되어 있는 전자우편을 감시하고자 하는 경우에는 근로자의 동의만으로는 부족하다. 통신비밀보호법 제2조 제7호가 '당사자'의 동의없이 통신의 내용을 지득 또는 채득하거나 전기통신의 송·수신을 방해하는 것을 감청이라고 정의하고 있고, 우리나라 대법원도 이 경

〈표 1〉 송·수신이 허용/금지된 전자우편의 예

| | |
|---|---|
| 금지된 전자우편 | 영업비밀이 포함된 내용, 회사의 명예·신용과 관련한 내용, 성희롱·성차별적 내용, 국적·인종차별적 내용, 장애인에 대한 모욕·모독, 음란·폭력물, 허위사실, 명예훼손적 표현, 반인륜적 표현, 저작권침해, 스팸메일, 해킹·바이러스 프로그램 등 |
| 허용된 전자우편 | 회사에서 공식적으로 인정한 홍보·광고물, 업무와 관련된 사람들에 대한 인사장·연하장, 상사(또는 보안담당자)의 사전 승낙은 얻은 문서·자료, 가족·친지·지인간의 순수한 사적 통신 등 |

우 당사자의 의미를 당사자 쌍방을 의미하는 것으로 해석하고 있기 때문이다.[75] 따라서 제3자로부터 근로자에게 수신된 전자우편은 근로자의 동의가 있더라도 원칙적으로 열람하거나 개봉해서는 안 된다.

다만, 업무상의 전자우편이 분명한 경우 또는 업무상의 전자우편으로 간주될 만한 특별한 사유가 있는 경우에는 제3자로부터 근로자에게 수신된 전자우편이라도 열람이 가능하다고 보아야 할 것이다. 또한 사적인 전자우편이라 하더라도 해킹이나 바이러스 감염 여부를 확인하기 위한 점검이나 감염된 전자우편, 스팸메일의 차단은 사용자의 시설관리권 행사 차원에서 적법하다. 그러나 수신된 전자우편의 내용을 보기 전에는 어떤 전자우편이 업무상의 것인지 사적인 것인지를 알기 어려운 경우가 많으므로 사용자는 다양한 방법을 통해 제3자에게도 전자우편 감시에 관한 회사의 방침을 공개하고 가능한 한 사적인 전자우편과 업무상의 전자우편을 구분해서 보내도록 권장해야 한다.

### 나. 방법상의 적법성 확보

절차적으로 근로자의 동의를 받았다고 해서 근로자의 전자우편에 대한 감시가 무제한적으로 허용되거나 자의적인 감시가 허용되는 것은 아니다. 최대한 근로자의 사생활을 보호하는 수준에서 이루어져야 하며, 감시의 목적·필요성과 근로자가 받게 되는 불이익이 균형을 이루어야 한다.

첫째, 사용자는 가능한 한 전자우편의 '내용'을 열람하는 것은 삼가해야 한

75) 앞의 주 71) 참조.

다. 내용 열람은 최후의 수단이 되어야 한다. 특히 근로자의 동의가 있더라도 근로자의 노동조합활동, 건강상담 등 개인적인 활동이 분명한 경우에는 내용 열람을 삼가해야 한다. 먼저 전자우편의 사용횟수, 빈도, 분량(문서의 크기), 문서의 형식, 송·수신처 등을 모니터링하여 문제성이 있다고 판단되는 전자우편만 가려서 내용검색을 실시해야 한다.

둘째, 일상감시와 정밀감시를 구분하여 정밀감시는 일상감시를 통해 어느 정도 의문점이 확인된 경우에 한해 예외적으로 실시하여야 한다. 일상감시는 사람에 의한 감시보다는 기계적 장치에 의한 감시나 필터링 방법을 채택하는 것이 바람직하다. 예컨대, 제품설계도에 사용되는 문서형식, 경쟁회사들의 전자우편주소, 주제어(키워드) 등을 자동 필터링 시스템에 등록하여 영업비밀이나 불법적인 정보가 외부로 새나가는 것을 사전에 차단할 수 있다.

셋째, 감시의 범위·정도·방법을 개인별 또는 업무별로 차별화하여야 한다. 해당 근로자가 맡고 있는 업무의 성질에 따라 감시의 정도를 달리해야 한다는 것이다. 제품설계실 또는 경리부서에 근무하고 있는 근로자와 영업사원에 대한 전자우편의 감시방법을 똑같이 할 필요는 없다. 그러나 범죄행위에 대한 상당한 의혹이 있는 경우 등 합리적인 근거가 있는 경우를 제외하고는 특정 근로자에 대한 감시를 다른 근로자에 비해 차별적으로 강화해서는 안 된다.

넷째, 전자우편에 대한 감시업무를 담당하는 자를 특정하여야 한다. 담당자에게는 전자우편 감시와 관련한 권한과 의무를 명확히 하여야 하며, 어떤 경우에도 개인적인 호기심이나 공개된 목적 이외의 용도로 전자우편을 열어보게 해서는 안 된다. 또한, 동료나 상사 또는 사용자의 부당한 감시요구에 불응할 수 있는 권한과 근거를 마련해야 한다. 그리고 전자우편시스템 관리자들에 대해서는 정기적인 교육과 감독이 필요하다.

마지막으로 사용자는 사후적인 징계보다는 범죄행위를 사전에 예방하는 것이 더 효과적이라는 점을 인식하고 근로자들로 하여금 회사가 금지하고 있는 전자우편의 사용을 자제하도록 유도해야 한다. 근로자가 전자우편을 전송하기 전에 개인적인 것인지 업무적인 것인지를 선택할 수 있게 하면 사용자는 전자우편에 대한 감시활동을 훨씬 효과적으로 수행할 수 있을 것이다.

### 다. 이용상의 적법성 확보

전자우편 감시를 통해 수집된 정보는 당초 정해진 목적으로만 이용되어야 한다. 대개의 경우 사용자는 이용목적을 넓게 규정하려고 할 것이다. 그러나 전자우편에 대한 폭넓은 감시와 감시결과의 폭넓은 이용이 꼭 사용자의 이익에 부합하는 것만은 아니다. 필요 이상으로 전자우편을 감시하고 감시결과를 이용할 경우 회사의 이미지에 부정적 영향을 미쳐 우수 인재의 확보가 어려워질 수 있고 근로자들의 사기를 저하시킬 수 있다.

주의해야 할 것은 불가피한 경우를 제외하고는 전자우편 감시를 통해 지득한 정보를 제3자는 물론 회사 내의 다른 사람에게도 공개해서는 안 된다는 점이다. 근로자가 감시에 동의했다고 하더라도 전자우편에 대한 감시와 감시결과의 공개는 별개의 것이기 때문이다. 불가피한 경우란 수사기관, 법원, 회사 경영자 등에게 공개하는 경우이다. 전자우편의 내용이 징계사유로 된 경우에도 징계위원회에 회부할 때에는 가능한 한 당해 근로자의 인적사항을 가리는 등 사생활 보호에 주의해야 한다.

### 라. 전자우편감시 및 필터링 기술

자동화 기술에 의한 전자우편의 상시적인 감시는 근로자들의 사생활 보호에 치명적인 위험을 내포하고 있다. 그러나 해킹·바이러스에 취약한 인터넷 환경의 특성상 그리고 전자우편이 가지고 있는 태생적인 보안상의 취약점 때문에 어느 정도 상시적인 감시는 불가피하다. 한편, 사용자가 수집된 정보를 잘 관리하기만 한다면 사람에 의한 감시보다는 기계적 시스템에 의한 감시가 근로자의 사생활을 덜 침해할 수 있다. 예컨대, 사용자가 주제어를 통한 필터링 시스템을 도입할 경우 필터링에 의해 기업비밀정보의 유출을 유효하게 차단하면서 사용자는 굳이 그 정보의 유출을 시도한 발신자를 확인하지 않고 곧장 그에게 경고 메시지를 보낼 수 있도록 기술을 설정할 수 있다.

따라서 사용자는 전자우편 자동감시 시스템을 도입하고자 할 때에는 감시의 목적을 달성하면서 근로자의 사생활 침해를 최소화할 수 있는 방법을 강구하여야 한다. 필터링은 공개적으로 하는 것이 근로자들의 비행을 예방하는 데 효과

적이며 추후 발생할지도 모르는 법률분쟁을 피할 수 있다. 해킹·바이러스 프로그램이나 스팸메일 등을 차단하기 위한 경우를 제외하고, 당사자의 동의없이 주제어를 통해 전자우편을 필터링하거나 전자우편의 내용, 통신일시, 통신개시·종료시간, 발·착신주소, 로그기록 등을 모니터링하는 행위는 현행법상 불법적인 통신제한조치에 해당한다.

현재 시중에는 전자우편 모니터링을 목적으로 한 다종의 소프트웨어가 개발되어 시판되고 있다. 그러나 이들 소프트웨어들은 대부분 바이러스의 감염여부 확인, 스팸메일 차단 기능은 기본이고, 전자우편내용의 실시간 검색, 송·수신자, 송·수신IP, 송·수신 날짜 및 시간, 파일크기, 파일종류, 주제어 검색 등 매우 다양한 기능을 동시에 선택할 수 있고, 다수의 관리자가 모니터링에 참여할 수 있도록 구성되어 있어 감시의 남용이 우려된다. 따라서 사용자는 모니터링 시스템을 도입하기 전에 모니터링 사실을 공개하고 동의를 받아야 하며, 관리자의 수를 최소화하여야 하고 관리자에 대한 주기적인 교육과 감독을 통해 자의적인 모니터링이 일어나지 않도록 해야 한다.

사용자를 위한 전자우편감시 가이드라인

**【1】 전자우편 시스템의 관리·운영에 관한 사항**

1. 전자우편시스템과 전자우편계정이 사용자(회사)의 소유임을 분명히 밝힐 것
2. 전자우편상에서는 개인의 사생활이 보장되지 않는다는 사실을 주지시킬 것
3. 전자우편 관리를 위해 배급한 비밀번호에 대해서 비밀성이 보장되지 아니함을 명시할 것
4. 사용자가 승인하지 아니한 비밀번호의 사용이나 비밀번호의 임의적 변경을 금지할 것
5. 자신의 컴퓨터에서 전자우편을 삭제하더라도 시스템상에서는 전자우편이 삭제되지 않고 그대로 남아 있다는 것을 근로자에게 알릴 것
6. 송·수신된 전자우편이 서버(시스템) 내에 보존되는 기간(삭제시기)과 정보의 크기를 명시할 것

**【2】 전자우편의 이용에 관한 사항**

1. 개인적인 용도의 전자우편 사용이 허용되는지 여부를 분명히 밝힐 것. 사용자는 ⅰ) 사적이용의 완전금지, ⅱ) 업무에 지장이 없는 범위 내에서 사적 이용의 허용, ⅲ) 사적이용의 전면 허용 중 하나를 선택해야 한다.
2. 개인적인 사용을 허락할 경우 송·수신이 허용되는 전자우편(정보)과 허용되지 않는 전자우편(정보)을 구체화할 것
3. 개인적인 전자우편의 사용이 제한되고 있다면 송·수신이 허용되는 시간과 금지

되는 시간을 고지할 것
4. 업무상의 전자우편과 개인적인 전자우편을 구분하게 할 것. 사용자는 가능한 한 근로자가 업무상 전자우편과 개인적인 전자우편을 구분할 수 있는 도구를 제공하여야 한다.
5. 사용자가 업무용으로 배급한 전자우편계정 외에 다른 전자우편계정의 사용이 허용되는지 여부를 밝힐 것
6. 불법적인 전자우편(정보)을 수신한 경우에는 사용자에게 즉시 알리도록 할 것

**【3】 전자우편의 감시방법에 관한 사항**

1. 전자우편의 사용이 감시받고 있음을 근로자에게 알릴 것. 이 경우 감시목적, 감시방법, 감시시간대, 감시장소, 수집되는 정보의 내용, 감시업무를 수행할 부서 및 담당자, 감시를 통해 얻은 데이터의 보존기간, 근로자의 권리 등을 알기 쉽게 설명하여야 한다.
2. 전자우편 내용에 대한 열람은 최후의 수단으로만 이용할 것. 전자우편의 사용횟수, 사용빈도, 문서양식, 문서의 양, 송·수신처 등의 모니터링이나 주제어 검색을 통해 의심할 만한 사항이 발견된 경우에 한해 내용을 열람한다.
3. 아래와 같은 전자우편은 내용 열람을 피할 것. ⅰ) 근로자가 외부로부터 수신한 개인적인 전자우편, ⅱ) 근로자의 노동조합활동, 건강상담 등과 관련한 전자우편
4. 근로자의 부재중(휴가, 출장, 회의 등)에 전자우편계정을 감시해야 할 필요가 있을 때에는 미리 그 사실을 고지할 것
5. 감시의 범위·정도·방법을 근로자가 맡고 있는 업무별로 차별화할 것
6. 감시를 통해 지득한 정보를 함부로 공개하지 말 것. 통신일시, 통신개시·종료시간, 착·발신주소 등도 통신사실확인자료로서 통신비밀보호법에 의해 무단 제공이 금지되므로 신중하게 취급해야 한다.
7. 전자우편에 대한 감시업무를 담당하는 자를 특정하고 권한과 의무를 분명히 할 것. 서버관리자는 시스템 보전이 주요 임무이므로 원칙적으로 전자우편 감시에 관한 권한이 없다.

**【4】 전자우편의 사용·감시에 관한 홍보 및 교육**

1. 전자우편의 사용 조건 및 방법을 근로자에게 주기적으로 교육시키고 전자우편 감시에 대한 회사의 방침을 인식하도록 할 것
2. 전자우편 시스템 관리자 등에 대한 교육을 정기적으로 실시하여 불법적인 감시를 차단할 것. 상사의 부당한 감시지시에 불응할 권한을 부여하여야 한다.
3. 전자우편사용방침을 어긴 경우 근로자가 받게 될 불이익 조치(징계 등)를 명시하고 이의제기 절차를 마련할 것
4. 근로자에게 전자우편을 보낸 상대방도 전자우편의 감시 사실과 목적을 알 수 있게 하고 사적인 전자우편은 구분해서 전송하도록 권고할 것

**【5】 전자우편 감시를 위한 근거의 확보**

1. 가능한 한 근로자대표와 사전 협의를 하고 근로자대표의 자문을 구할 것. 반드시 노동조합이어야 할 필요는 없고 직장협의회, 노사협의회 등도 좋다
2. 근로자들에게 전자우편의 사용조건을 알리고 감시에 대한 서면 동의를 받을 것
3. 전자우편의 사용조건, 감시방법, 감시절차, 이용목적, 부당한 이용시의 불이익 조치 등을 취업규칙화할 것

# Ⅴ. 맺음말

앞에서 살펴본 것처럼 현재의 법과 판례는 근로자의 자발적 동의가 없는 한 개인적인 전자우편은 물론 업무적인 전자우편에 대해서도 감시에 상당한 제약이 따르게 된다. 특히 근로자가 제3자로부터 수신한 개인적인 전자우편에 대해서는 근로자의 동의가 있어도 판례상 열람이 불가능하다. 이에 비해 선진국에서는 전화와 전자우편을 구분하여 전자우편에 대해서는 일반적으로 근로자에 대한 사전 고지와 필요성·비례성 등의 원칙이 충족되면 원칙적으로 사용자에 의한 감시를 허용하고 있다. 상대적으로 우리나라의 사용자들이 전자우편을 이용한 기업비밀유출이나 전자우편의 오·남용행위, 그 밖의 불법행위를 통제하기 어려운 입장에 있다고 할 수 있다.

이 같은 문제는 전기통신에 대한 획일적인 보호와 포괄적 감청금지 위주로 규정되어 있는 현행법에 있다. 따라서 사용자의 업무지시권과 시설관리권에 기초한 필요하고도 합리적인 감청까지 금지하고 있는 현행 「통신비밀보호법」 제3조와 「정보통신망이용촉진및정보보호등에관한법률」 제49조를 각각 선진국 수준으로 개정하여야 한다. 즉 사용자가 업무용으로 근로자에게 제공한 전자우편계정에 대해서는 사전 고지만으로 송·수신 전자우편을 열람·저장할 수 있도록 예외를 인정하여야 한다. 이 경우 사용자에 의한 감시의 남용을 방지하기 위해 영국의 「2000년 조사권한규제법」을 고려할 필요가 있다. 동법은 첫째, 업무와 관련된 사실의 존재를 입증하기 위한 경우, 둘째, 강제규범 또는 자율규범의 준수 여부를 확인하기 위한 경우, 셋째, 근로자의 업무실적을 확인하기 위한 경우, 넷째, 범죄를 예방 또는 탐지하기 위한 경우, 다섯째, 허가받지 아니한 통신시스템의 사용을 조사 또는 탐지하기 위한 경우, 마지막으로 시스템의 보안과 효율적 운영을 확보하기 위한 경우에 한해 사용자의 전자우편 감시를 허용하고 있다.

그러나 전자우편 감시를 허용할 경우 미국에서와 같이 사용자에 의한 감시의 오·남용이 생길 수 있다. EU 회원국에서는 개인정보보호법에 의해 독립적

이고 전문적인 개인정보보호기구가 설립되어 있어 프라이버시 커미셔너(Privacy Commissioner)가 감시의 방법, 절차, 이용 등에 관한 기준을 제시하고 사용자와 근로자 간에 다툼이 생길 때에는 이를 중재하거나 재정하는 기능을 수행하고 있기 때문에 사용자에 의한 과도한 감시는 규제를 받게 된다. 또한 감시와 관련한 제반 사항을 사용자는 미리 커미셔너에게 신고하여야 한다. 더구나 프랑스, 독일 등 일부 국가에서는 사용자가 전자우편 등을 감시하고자 하는 경우에는 사전에 감시계획을 근로자대표에게 통지하여 협의를 하거나 근로자대표의 자문을 구하도록 되어 있다. 사용자가 근로자대표기관의 의견을 받아들이지 않은 경우 근로자대표는 프라이버시 커미셔너에게 조정을 요청하거나 재정(또는 구제명령)을 신청할 수 있다. 근로자는 노동심판소에 구제를 신청할 수도 있다.

사용자에 의한 과도한 전자우편 감시를 예방하기 위해 우리나라에서도 「노동조합및노동관계조정법」이나 「근로자참여및협력증진에관한법률」을 개정하여 사용자에게 사전 협의의무를 부여하고, 사용자와 근로자 사이에 분쟁이 발생한 경우 이를 원만하게 해결할 수 있는 분쟁해결절차가 마련되어야 한다. 우리나라는 EU 제국과 달리 독립적인 개인정보보호기구가 아직 없다. 현재 정부에서 추진하고 있는 개인정보보호법의 제정 방안에 이와 같은 정부의 기능과 역할이 고려되어야 할 것이다. 개인정보보호법이 제정될 때까지는 노동위원회가 이와 같은 기능을 수행할 수도 있을 것이다.

## 참고문헌

김형배. 『노동법』. (2002) pp.242.

노동자감시 근절을 위한 연대모임. 「2003 노동자감시 실태조사 결과 보고서」 (www.nodong.org). (2004).

이병태. 『최신 노동법』. (2003) pp.778.

이창범. 「전자우편감시를 위한 법적 구비요건」. 『산업보안연구논총』. 국가정보원, (2004) pp.103~182.

이창범 · 윤주연. 「각국의 개인정보피해구제제도 비교연구」. 개인정보분쟁조정위원

회, (2003) pp.164~165.
이창범・장민영.「국내외 개인정보판례분석」. 개인정보분쟁조정위원회, (2003) pp. 40~41.
이희성.「직장내에서의 전자메일 및 CCTV의 감시와 근로자의 프라이버시보호」. 개인정보분쟁조정위원회 워크숍 자료, (2002.10) pp.14.
황성기.「통신제한조치의 헌법적 한계와 구체적 통제방안」. 한국정보법학회 제14차 세미나. (1999.11).
<경향신문> 2004.5.20, pp.22.
<매일경제신문> 2004.5.19, pp.1.
<부산타임즈>, 2002.8.20.(www.inews.org/Snews/section.php?Domain=dsnb&SeqCode=35&Ho=8854).

AMA, *2001 AMA Survey Workplace Monitoring & Surveillance*, New York(http://www.amanet.org/research/specials/elecmont.htm).
Morgan, Charles. “Employer Monitoring of Employee Electronic Mail and Internet Use”, *McGill Law Journal* 44. (1999) pp.889~890.
EU Data Protection Working Party. *Working Document on the Surveillance of Electronic Communications in the Workplace.* (2002) pp.4.
Dütz. *Arbeitsrecht*, Rdn. (1990) pp.180.
Söllner. *Grundriβ des Arbeitsrechts*, 10. Aufl., (1990) S.269.
Zöllner & Loritz. *Arbeitsrecht*, 5. Aufl., (1998) S.204f.

<주요 법령 및 가이드라인>
CODE DU TRAVAIL(http://www.legifrance.gouv.fr/WAspad/UnCode?code=CTRAVAIL.rcv)(프랑스)
Council of Europe’s Recommendation (89) 2 on the Protection of Personal Data Used for Employment Purposes.
Directive 95/46/EC on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data.
Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.
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.

Electronic Communications Privacy Act of 1986 (Pub. L. No. 99-508, 100 Stat. 1848) : Omnibus Crime Control and Safe Streets Act of 1968.(미국)

Electronic Monitoring in the Workplace Act : SB 1016(1999년), SB 1822(2000년).(미국)

European Convention for the Protection of Human Rights and Fundamental Freedoms.

Federal Wire Tap Statute(18 U.S.C.A. §2510(West 1968).(미국)

Loi n° 78-17 du 6 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés(프랑스)

Monitoring at Work : Guidance for Small Businesses. (www.informationcommissioner. gov.uk.)(영국)

Opinion 8/2001 on the processing of personal data in the employment context (13 September 2001).

Regulation of Investigatory Powers Act 2000(영국)

Safe Harbor, OJ L 215 dd. 25 August 2000.(미국)

Telecommunications Regulations 2000 : Lawful Business Practice Regulations(영국)

The Employment Practices Data Protection Code : Part3 Monitoring at Work.(www. informationcommissioner.gov.uk.)(영국)

Working document on the surveillance of electronic communications in the workplace (29 May 2002).

個人情報のに保護關する法律(일본)

犯罪捜査のための通信傍受に關する法律(http://www.shugiin.go.jp/itdb_housei.nsf/html/housei/h14137.htm(일본)

abstract

# Study on E-mail Surveillance in the Workplace

Chang-beom Yi

As informatization in business has been accelerated with widespread diffusion of information and communication equipment including internet and Personal Computer, there have been so many changes in the work condition and environment. For surely, usage of information and communication equipment increased effectiveness and convenience in business. However it also caused increase in time that employees spend on private email and messenger activities during working hours, which led accidents of leaking or disclosing secret information of businesses through email happen.

Even though many Employers feel the necessity of monitoring online activities of employee, adverse criticism over privacy intrusion just don't let them put themselves forward aggressively. Meanwhile, some business entities recklessly monitor online activities of employee in public or in secret. Therefore, there's strong need to provide rational standard for legal monitoring of employee's online activities in the workplace.

This study aims at providing theoretical ground and limitation of surveillance and establishing standard for email monitoring based on those. Guideline provided in this study can also be applied in the field of monitoring employee by RFID, smartcard, CCTV, etc.

Keywords: email surveillance, protection of trade secret, personal information on employee, workplace privacy, employer's right to monitor