직장내 전자우편의 감청에 대한 규율 방안

연구원 이 민 영*

최근 직장내 전자우편의 감청과 같은 사내감시에 대하여 사회적 관심이 증폭되고 있다. 이 문제는 사용자의 정당행위로 인정될 수 있는 범위를 벗어난 조치를 법테두리 안으로 이끌 수 있는 정책적 고려가 요구되는 사안임을 감안하여, 본고에서는 관련법제와 정책현황을 통해 대응방안을 도출하여 합리적인 감시원칙을 모색하고자 한다.

목 차

Ⅰ. 서 론

바야흐로 우리는 지식정보사회 속에 살아가고 있다. 구체적인 일례로 정보기술의 발달과 인터넷의 확산에 힘입어 이루어진 전자우편 사용의 일반화를 들 수 있다. 근로현장에서도 전자우편의 활용은 보편적 현상으로 나타나고 있다. 아울러 기업의 기밀유출방지와 보안유지강화 측면에서 근로자의 전자우편 열람을 사용자가 제한하는 것이 관행으로 자리잡고 있어, 사용자와 근로자의 상호이익이 충돌을 맺고 있다. 부당한 감시·통제라는 강변(强辯)과 정당한 지시감독권이라는 논박(論駁)은 쉽사리 조율(調律)되기 어려울 것으로 보인다.

이러한 시대적 난제와 상황적 배경을 등에 업고 직장내 전자우편 사용제한에 관한 법제도적 정책기준을 모색하는 작업이 주요 쟁점으로 대두되고 있기에, 이하에서는 현황파악을 통

연락처: * 미래한국연구실 (02) 570-4083, mylee@kisdi.re.kr

한 현안분석과 함께 대응방안으로서의 구체적 지침을 마련해 보기로 한다.

Ⅱ. 직장내 전자우편 감청

1. 전자우편과 전자감시

2002년 6월 현재 우리나라 인터넷 이용인구는 1994년 상용 인터넷접속서비스가 시작된 이래 급속히 증가하여 2,565만 명에 이른다.[1] 정보의 가상공간인 인터넷은 정보사회의 상징이며 인터넷의 부산물이 전자우편[2]임은, 다음과 같은 통계수치에서도 여실히 반영되어 있다. 즉 우리나라에서 인터넷의 이용 목적이 전자우편의 사용에 있다는 응답이 2001년 12월 현재 19%를 차지하고, 직업별로는 전문・관리직의 89.9%, 사무직의 89.2%, 서비스・판매직의 75.7%, 생산관련직의 75.4%, 학생의 87.7%가 평균 2개 정도의 전자우편을 보유하고 있는 것으로 나타났다.[3] 이는 근로현장에서도 전자우편의 활용이 보편적 현상으로 나타나고 있음을 보여준다.

이와 같이 직장내 전자우편 사용이 급증함에 따라 내부 직원에 의한 기업경영정보의 외부유출이 용이해졌다. 특히 전자우편을 통한 민감한 기업정보의 유출은 그 신속성 및 적발의 곤란성 등으로 기업의 경영전략에 방해요인으로 작용할 가능성이 커진다. 그러므로 업무전산화가 구축된 오늘날 기업에서 정보보호대책이 물리적 측면뿐만 아니라 관리적 측면에서도 강구되어지고 있으며, 전자감시가 기업의 정보보호대책으로 채택되고 있는 실정이다. 전자적 감시・검열(electronic surveillance or monitoring)이란 컴퓨터・전화・전신・무선・카메라・전자기(電磁氣), 광전자(光電子) 또는 광학시스템의 사용을 포함한 직접감시 이외에 모든 수단으로 근로자의 직무행위 또는 통신에 관한 정보를 수집하는 통신방해행위를 말한다. 이러한 감시로 인하여 사용자측이 근로자가 주고받은 전자우편의 내용을 알게 될 때 근로자의 프라이버시는 침해되기 쉽다.[4]

---

1) 정보통신연감, 전자신문사, 2003, 462쪽.

2) 전자우편이란, 인터넷과 같은 전산망(computer network)을 통하여 한 사용자로부터 다른 사용자에게 전자적으로 보내지는 편지 또는 메모 등과 같은 통신(correspondence; communication)을 말한다; June Jamrich Parsons and Dan Oja, Computer Concepts, 2nd ed. Cambridge, MA: Course Technology, Inc., 1996.

3) 인터넷연감, 전자신문사, 2003, 786~787쪽.

4) Mark S. Kende, *The Issues of E-mail Privacy and Personal Jurisdiction: What Clients Need to Know About Two Practical Constitutional Questions Regarding the Internet*, 63 Mont. L. Rev. 301, 302 (2002).

이러한 근로자에 대한 전자감시를 시행하는 이유로 사용자들은 ① 기업비밀유출 조사, ② 작업자가 고객의 데이터에 부적절하게 접근하는 것을 방지함으로써 고객의 프라이버시 보호, ③ 사적 용도로 시스템 사용에 따른 생산성 저하 방지,[5] ④ 유해환경 방지, ⑤ 작업장에서의 폭력 미연방지 등을 들고 있다. 반면에 근로자들이 전자감시에 대해 반대하는 이유는 ① 검열이 기본적 인권과 인간존엄성에 위배되는 것인데, 종종 이러한 관심에 대한 적절한 고려 없이 이루어지고 있음, ② 검열은 근로자들의 개인적인 생활을 전보다 더 쉽게 엿볼 수 있게 하는 반면, 근로자들이 이를 알아차리는 것은 더욱 어렵게 만듦, ③ 감시·감독은 근로자들에게 그들이 신뢰받지 못하고 있으며, 따라서 근로자와 사용자 모두에게 해가 되는 대립적인 정서를 키움, ④ 검열은 근로자들을 차별하고 보복하기 위해 사용될 수 있으며, 근로자들이 이를 발견하는 것은 어려움 등으로 요약될 수 있다.

우리나라의 경우 아직까지는 직장근로자들의 인터넷 사용에 따른 직무감시 인식은 상대적으로 약한 상태에 있다. 하지만 최근 선진 자본주의 국가와 마찬가지로 인터넷 감시를 둘러싼 논쟁이 점차 표면화되면서 노사갈등의 새로운 쟁점으로 부각되고 있기 때문에, 향후 이에 대한 감시인식은 점차 높아질 것으로 전망된다.[6]

2. 전자우편의 법적 귀속

근로자의 전자우편을 구성하는 디지털이 법적으로 근로자에게 귀속되는 것인가 아니면 사용자에게 귀속되는가의 문제에 대해 살펴보면, 회사의 재산을 구성하는 메일서버나 그 메모리 자체의 법적 소유권은 당연히 회사에 인정된다고 할 것이다. 그러므로 디지털자체의 소유권은 기업에게 귀속되고, 다만 근로자는 그 디지털을 이용할 권리만을 갖는다고 보아야 할 것이다.

그러나 근로자의 전자우편에 대한 사용자의 감청에서 보호되어야 할 법익은 재산권이 아니

5) 예컨대 느린 컴퓨터 동작, 시간 죽이기, 게임목적·증권투자·스포츠·음악·포르노 사이트 접근 방지 등을 거론할 수 있다.

6) 조사의 결과는 서비스판매 계통의 직업근로자들이 직무감시가 가장 높은 것으로 나타나고 있다. 그리고 예상했던 바와 같이 사적인 용도에서 인터넷을 이용하는 경우 직무감시에 대한 인식이 높은 것으로 나타나고 있다. 물론 서비스판매직이 사무직이나 관리직에 비해 인터넷을 더 많이 사용하고 있다는 증거는 제시되어 있지 않지만, 이들 직종의 근무자들은 고객을 직접 상대하고 관리한다는 점에서 인터넷을 통한 외부접촉이 여타 다른 직종에 비해 높을 것이며, 그들의 행위 하나하나가 직접 기업 이미지나 마케팅 등에 영향을 미친다는 점에서 그들에 대한 인터넷 통제가 심할 것이고, 따라서 그들의 감시인식이 높을 수 있다는 추론이 가능하다; 김왕배·이경용, 인터넷 사용과 직무감시－주관적 인식을 중심으로－, 경제와사회 통권 제57호, 한울, 2003, 221~222쪽.

라 전자우편의 수신자 혹은 작성자로서의 그 통신비밀이므로, 디지털자체의 법적 소유권은 기업에게 귀속되는가는 감청과는 관련이 없다고 보아야 할 것이다. 즉 전자우편을 구성하는 디지털자체의 재산권법상의 소유권은 기업에게 귀속되고, 전자우편의 내용을 구성하는 보호되어야 할 통신비밀 내지 정보 그 자체는 근로자에게 귀속된다고 보아야할 것이다. 이러한 법리는 마치 주택의 재산법상의 소유권은 소유자에게 귀속되나 주택 내에서의 프라이버시는 거주자에게 귀속됨으로써, 소유자라 할지라도 거주자의 프라이버시를 보호해야할 의무를 부담하는 것과 유사한 구조라 할 것이다.[7]

3. 전자우편 감청과 근로자의 프라이버시

가. 현안분석

인터넷이 주된 커뮤니케이션의 수단이 된 현대와 같은 정보사회에 있어서 사용자에 의한 근로자의 전자우편 감청은 간과할 수 없는 노동문제라고 할 것이다. 전자우편은 중앙 메일서버를 거치게 되지만, 외부의 전자우편 서비스를 이용하는 경우에는 회사의 서버를 거치지 않고 전자우편의 수신이나 발신이 이루어진다. 하지만 최근에는 서버를 이용하지 않는 전자우편의 수신 및 발신상황도 감시할 수 있는 기능을 갖춘 전자감시 프로그램들이 개발되어 사용되고 있기 때문에 모든 전자우편은 언제나 감시될 수 있다. 근로자는 자기의 컴퓨터에서 전자우편을 지워도 사용자의 서버에는 보낸 전자우편이나 받은 전자우편이 지워지지 않고 그대로 남아 있을 수도 있으며, 근로자가 회사의 컴퓨터를 이용하여 보내고 받은 모든 전자우편을 사용자가 따로 저장하고 있을 수 있다. 또한 컴퓨터를 이용한 전자우편의 감시는 아주 적은 비용으로 손쉽고 은밀하게 이루어질 수 있다. 사용자는 근로자가 전자우편을 받은 시간・보낸 시간・전자우편의 상대방・전자우편의 내용 등 모든 것을 실시간으로 무제한적으로 저장하고 분석하고 감시할 수 있으며, 손쉽게 원하는 정보만을 골라서 검색할 수도 있다. 그리하여 근로자는 전자우편을 감시하는 사용자에 대한 적절한 제한이 없이는 프라이버시 보호가 사업장에서 거의 사라지게 됨으로써 상시적으로 감시가 계속되는 '전자적 노동착취장(electronic sweatshop)'의 결과를 가져올 것이라는 두려움을 가지게 될 것이다.[8]

이러한 감시에서 주로 문제로 되는 것은 사용자에게 업무상의 전자우편에 한하지 않고 근

7) 오병철, 직장내 사용자에 의한 근로자의 전자우편 감청, 과학기술법연구 제6집, 한남대학교 과학기술연구소, 2000, 266~267쪽.

8) Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-mail Privacy*, 1 J. High Tech. L. 101, 107 (2002).

로자의 사적인 것에 대한 감청까지도 허용되는가의 여부라 할 것이며, 사용자가 근로자의 사적인 전자우편 내용을 무단으로 감청하는 것은 프라이버시의 침해에 해당한다고 평가된다. 그런데 업무상의 이유에서라고 하더라도 모든 전자우편의 내용을 감청하기 위해서는 사용자가 사전에 그러한 취지를 근로자에게 통지할 필요가 있다. 그러한 통지를 한 경우에도 부당한 목적으로 감시하는 것은 허용되지 않고, 또 특정의 근로자만을 대상으로 감시하는 것도 허용되지 않을 것이다. 다만 특정 근로자가 기업비밀의 누설 등 부정행위를 하였다는 구체적이고 합리적인 의심이 있는 경우에는 그러한 한도 내에서 예외적으로 인정될 수 있을 것이다.[9)]

직장에서 근로자의 사적인 전자우편의 비밀을 침해한다는 것은 사용자가 전자우편의 발신인・수신인・발송일자・발송회수・발송내용・제목 등 전자우편을 주고받는 것과 관련한 일체의 비밀을 알아내는 것을 말하지만, 감청을 통해서 얻은 개인정보를 근로자의 동의 없이 그 목적 이외에 이용하거나 제3자에게 개시하면 감시 자체의 문제와는 별도로 사용자는 프라이버시 침해의 법적 책임을 지게 된다.

나. 실태조사

최근 노동단체에서 지난 6월 한달 동안 전국 207개 사업장을 조사해 발표한 실태보고서에 따르면, 전체 조사대상의 89.9%에 해당하는 186개 사업장에서 CCTV 설치, PC하드디스크 내용검사 등 보안감시 시스템을 설치하고 있는 것으로 나타났다. 또한 특정 인터넷 홈페이지 방문차단(32.9%), 인터넷 접속내용 기록(20.3%), 전자우편이용 차단(17.9%), 전자우편이용 기록(15.9%) 등의 컴퓨터 관련 감시가 이루어진 것으로 조사되었다. 이에 따라 186개 사업장의 12.9%인 24곳에서 보안감시를 둘러싸고 근로자와 사용자측간 마찰이 빚어진 것으로 분석되었다.[10)]

한편 지난해에는 직장에서 해고된 3명의 간부가 통신비밀보호법 위반・비밀 침해・권리행사 방해 등 혐의로 회사 고위 간부 4명을 검찰에 고소한 사건이 있었다. 사건을 수사하던 검찰은 회사간부 한 명을 통신비밀보호법 위반혐의로 구속하기에 이르렀다. 당사자의 동의를 받지 않은 채 법적 근거나 절차 없이 타인의 전자우편을 무단으로 열어본 혐의가 검찰 수사 결과 드러난 것이다. 더구나 이 구속된 간부는 부하직원을 이용해 또 다른 회사 간부의 일일 동향을 정보보고 받았던 것이 검찰 수사 과정에서 추가로 밝혀졌다. 이 부분은 명백한 프라이

9) 이희성, 작업장내에서의 전자메일 및 CCTV의 감시와 근로자의 프라이버시보호, 비교사법 통권 제20호, 한국비교사법학회, 2003, 528쪽.

10) 노동감시실태 조사결과 발표 및 노동감시근절대책 촉구 기자회견, 근로자감시근절을위한연대 모임, 2003. 7. 31.

버시 침해행위에 해당하지만 현재로서는 이를 처벌할 명확한 법규정이 없어 기소 대상에서 제외되었으나 다른 혐의로 구속되었다. 회사직원들의 전자우편을 불법열람하도록 지시하여 통신비밀보호법위반교사 등의 혐의로 기소된 이 간부에 대하여는 징역1년에 집행유예 2년이 선고되었다. 그리고 그의 지시를 받고 전자우편을 불법열람한 회사직원에 대해서도 징역 6~8월에 집행유예 2년이 선고되었다. 재판부는 판결문에서 "피고인들은 직원의 전자우편 열람이 회사의 신용과 명예를 훼손하는 행위를 밝히기 위한 정당방위였다고 주장하지만, 현행법은 그 목적에 상관없이 통신비밀을 보호하려는 데 그 취지를 두고 있다"고 밝혔다.[11]

다. 관리원칙

원칙적으로 사용자는 전자우편관리체계를 근로자에게 공개하고 근로자나 노동조합의 동의를 얻어야 한다. 전자우편의 관리체계는 근로자의 프라이버시와 통신의 자유에 직결되며, 단결권·단체교섭권·단체행동권을 그 내용으로 하는 노동3권과 같은 근로조건에 관한 중대한 결정이기 때문이다. 따라서 회사의 서버를 이용하여 근로자가 사적인 전자우편을 보내고 받거나 그밖에 회사의 컴퓨터 시스템을 이용하여 근로자가 사적인 통신을 할 때, 회사의 서버나 컴퓨터 시스템에서 중개를 위하여 전자우편이나 기타 통신을 저장해야 하는 경우에는 근로자의 통신비밀을 보호하기 위하여 순간적인 저장만을 하여야 할 것이다. 그리고 사용자는 근로자의 사적인 전자우편이나 기타의 통신에 대해서 암호처리할 수 있는 수단을 제공하도록 해야 하겠다.

4. 전자우편 사용제한기술과 정보유출대책

국내외에 출시되어 현재 사용가능한 전자우편감시 소프트웨어로는 Spector, Cyber Snoop, WinWhatWhere Investigator, Desktop Surveillance, VENUS/EMASS, NeoWatcher, Webkeeper, Mail-i, SessionWall-3 등이 있으며, 비교적 저렴한 가격으로 구입하여 활용할 수 있다. 인터넷 전자우편은 인터넷의 공개특성으로 인하여 언제든지 제3자가 열람하거나 자료가 유출될 가능성이 존재하므로 제3자의 전자우편 열람이나 유출에 대한 방지대책은 메시지의 송·수신 및 저장 처리시 암호화하여 송수신자만이 알아볼 수 있도록 할 수 있는 안전한 전자우편시스템의 이용이어야 한다.

11) 한겨레, 2002년 9월 11일자 14면 기사.

가. 전자우편에서 정보유출의 방법

1) 데이터 네트워크 트래픽 감시도구인 스니퍼를 이용한 내용 유출

스니퍼(Sniffer)란 LAN을 경유하는 이용자의 데이터를 감시하여 ID, 비밀번호, 전자우편 내용 등을 알아내는 해킹도구로서, 전자우편을 포함한 암호화되지 않은 일반적인 메시지는 전송로상에서 감청될 가능성이 있다. 스니퍼에는 sniffit, solsniffer, linsniffer 등 다양한 네트워크 모니터링 도구가 존재한다.

일반적인 스니퍼는 사용자들의 ID 및 비밀번호를 감청하기 위한 용도로 개발된 해킹도구로 전자우편 내용을 감청하기 위해서는 수정이 필요하다.

2) 전용 전자우편감시 소프트웨어 사용 이용

이는 내부직원들이 주요 기업정보 등을 대외로 유출하는 전자우편을 막고 감시하기 위한 전문소프트웨어를 악용하여 유출하는 것을 말한다.

3) 메일 전송 및 교환서버에서 열람 및 유출

전자우편서버에 접근권한이 있는 관리자는 이용자의 전자우편함에 대한 열람이 가능하다.

4) 해킹 및 바이러스를 통한 메일 유출

개인 컴퓨터상의 개인정보 및 전자우편이 해킹 프로그램이나 바이러스 등에 의해 유출될 수 있다.

나. 전자우편 정보유출대책

전자우편 정보유출은 주로 네트워크를 감청하는 방법을 사용하므로 전자우편의 내용을 암호화하여 송·수신함으로써 방지가 가능하다. 전자우편 정보유출에 대한 기술적 대책으로 PGP(Pretty Good Privacy)나 GNU Privacy Guard와 같은 안전한 전자우편 보안제품이 이용될 수 있으며, 그밖에 전자우편 서버의 보안방식을 취할 수도 있다.[12)]

Ⅲ. 관련 법제와 정책 현황

1. 국제적 기준

가. OECD 지침

1970년대 이후 국가간의 경제적 협력이 증가하면서 경제협력개발기구(OECD)는 여러 나

12) 한국정보보호센터, 전자우편 사용자 보호방안에 관한 연구, 정책연구 00-4, 한국정보보호센터, 2000, 91~92쪽.

라가 합의하는 통일된 개인정보보호지침을 마련하였다. 그리하여 1980년에 채택된 것이 '사생활보호 및 개인정보의 국제유통에 관한 지침(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)'이다. 세계각국의 개인정보보호와 관련된 법과 제도들은 권고안에 제시된 ① 수집제한의 원칙, ② 목적명확화의 원칙, ③ 정보내용정확성의 원칙, ④ 이용제한의 원칙, ⑤ 안전보호의 원칙, ⑥ 공개의 원칙, ⑦ 개인참가의 원칙, ⑧ 책임의 원칙과 같은 8가지 원칙에 기초하고 있다.[13)]

나. EC 권고

유럽연합 의회(Council of Europe)는 1989년 1월 18일 '고용목적으로 사용된 개인정보의 보호에 관한 권고'를 채택하였다. 여기서는 사용자가 개인정보의 수집이나 이용을 위한 자동시스템 또는 종업원의 행동이나 생산성의 감시를 위한 기술적 장치의 채택에 앞서 근로자 또는 그의 대표자에게 완전한 통지 또는 협의를 할 것, 근로자는 사용자가 보유하고 있는 자기에 관한 모든 개인정보에 접근할 권리를 가지며 보유하고 있는 개인정보의 정정 또는 말소를 청구할 권리를 가질 것, 개인정보의 축적은 정당한 기간을 넘지 않도록 제한되어야 할 것 등을 규정하고 있다.

다. ILO 규약

국제노동기구(ILO)에서 1996년 10월 7일 마련한 '사용자의 프라이버시 침해로부터 근로자를 보호하기 위한 규약'은 근로자의 신상정보 수집에 관한 사용자의 필요성과 개인정보 유통을 제한할 권리를 갖고 있는 근로자의 입장을 조화시킨 것이라는 평가를 받고 있다. 그 주요 내용으로는 ① 사용자는 근로자정보를 반드시 작업과 관련한 범주에서 본인에게 직접 얻어야 하며, ② 사용자는 근로자의 정치·종교적 신념 및 성생활에 관한 정보를 얻으려 해서는 아니되고, ③ 근로자는 프라이버시에 관한 권리를 포기하지 말아야 하며, ④ 사용자가 특정 근로자를 감시할 경우 본인에게 그 사유와 방법 그리고 시간을 통보해야 하고 비밀감시는 형사범죄 용의자에게만 해당한다는 일반원칙을 천명하고 있다. 또한 이 규약에서는 ① 사용자의 권리와 근로자의 프라이버시 권리를 모두 존중하되, ② 검열의 범위와 기간 등은 투명하고 명확하게 근로자에게 미리 사전에 고지하고, ③ 검열된 자료에 대하여 해당 근로자에게 열람권이 보장되는 등 인간적인 방식으로 동기를 유발시키는 요소로서 전자감시가 이루어지도록 권고하고 있다.

---

13) 이에 대한 자세한 내용은 김철완·이민영, 인터넷 개인정보보호에 관한 법제도 연구, 정책연구 00-10, 정보통신정책연구원, 2000, 52~53쪽 참조.

2. 미국의 현황

가. 법 률

근로자의 전자우편을 감시함으로써 근로자의 프라이버시를 침해하는 행위에 대하여 적용되는 유일한 연방법률로 Electronic Communication Privacy Act of 1986(이하 ECPA로 약칭한다)이 존재한다. ECPA는 전자우편 내용의 발신지와 의도된 수신자 이외의 어떠한 다른 자가 고의적으로 전자통신을 가로채거나(intercept),[14] 저장된 전자통신을 권한 없이 획득하거나,[15] 전자통신의 내용을 공개하는 것[16]을 일반적으로 금지하고 있을 뿐만 아니라 범죄시하고 있다.[17] ECPA에서 규정한 통신수단의 프라이버시 보호범위에 전자우편이 포함되는 것은 분명하지만, '전자통신(electronic communication)'의 개념에서 주간통상(州間通商: interstate commerce)에 사용되는 것으로 범위가 한정됨으로써 근로자의 전자우편에 관해서 논란의 여지가 남게 되었다. 견해의 대립은 있으나 위와 같은 개념정의에 벗어남으로써 근로자의 전자우편은 ECPA의 보호대상이 아니라는 주장이 대두되고 있으며, ECPA가 다양한 예외를 인정하고 있으므로 사업장에서의 전자우편 프라이버시에 대한 일반적 권리를 수립하고 있는 것으로 보이지는 않는다. 특히 ECPA는 이해관계당사자에게 공개하는 것을 제한하고 있지 않으며, 적절하게 가로채기된 내용이 누구에게 공개될 수 있는가에 대하여도 침묵을 지키고 있다.

1) ECPA의 전자우편보호

ECPA의 제1편은 정부·사용자·제3자가 전송중인 유선·음성 혹은 전자통신의 내용에 대하여 고의적인 가로채기와 공개를 금지하고 있다.[18] 다만 ECPA는 송신자 및 수신자의 신원, 내용의 길이, 전자우편의 제목 등과 같은 전자우편의 전달정보는 사용자가 자유롭게 감시할 수 있도록 하는 반면, 전자우편의 내용을 보호할 뿐이다.[19] 제1편이 적용되기 위해서는 '전자적·기계적 혹은 다른 장치'를 통한 통신내용의 '음성 혹은 다른' 획득으로서의 불법적 '가로채기'가 있어야 한다는 법정요건을 만족시켜야 한다.[20] 한편 제2편은 저장된 통신을 관장하

14) 18 U.S.C. 2510 (2000)는 가로채기에 대한 정의를 '어떠한 전자적·기계적 혹은 다른 장치를 통하여 어떤 유선·음성 혹은 전자적 통신의 내용을 음성 또는 다른 방식으로 획득하는 것'이라 규정하고 있다.

15) 18 U.S..C. 2701 (2000).

16) 18. U.S.C. 2511, 2702 (2000).

17) Title 18 Crimes and Criminal Procedure, Part I Crimes.

18) 18 U.S.C. 2511 (2000).

19) 18 U.S.C. 2510(8) (2000).

여, 전자통신서비스를 제공하는 시설에 권한 없이 접속하여 저장된 내용을 고의적으로 획득하는 자에 대하여 책임을 부과한다.[21]

ECPA의 제1편과 제2편에서의 프라이버시 보호내용을 비교해 보면, 제1편이 제2편보다 더 엄격한 예외조항으로 인하여 더 넓게 보호하고 있다. 또한 제2편은 가로채기하여 저장된 내용을 공개하는 것을 벌하지 않는다. 중요한 것은 제2편이 프라이버시 침해에 대하여 침해의 결과로 침해자에 의해 행해진 실제 손해의 배상만을 인정하고 있는 반면,[22] 제1편은 침해의 결과로 발생한 실제 손해의 배상뿐만 아니라 법정 및 징벌적 손해배상도 인정하고 있다는 점이다.[23]

2) ECPA의 법정예외조항(Exception)

사업의 정상적 과정(Ordinary Course of Business) 예외조항은 감시를 통한 전자우편의 획득이 정상적인 사업의 과정 범위 내에서 사용된 전화설비나 시설과 관련되어 이루어지면 서비스공급자로 하여금 통신을 가로채고 사용하거나 공개하는 것을 허용한다.[24] 이 예외조항은 사용자에게 근로자가 기대할 수 있는 프라이버시의 수준을 결정하는 데 상당한 재량을 허용하고 있으므로, ECPA로 하여금 사업장에서 근로자의 프라이버시를 정하지 못하게 만드는 결과가 된다.[25]

서비스공급자(Service Provider) 예외조항은 서비스공급자로 하여금 가로채기·사용·공개에 대한 ECPA 제1편과 제2편의 책임을 면제하기 때문에, 사용자가 서비스를 제공하는 한 어떠한 형태로든 내용을 감시·가로채기·공개할 기회를 넓게 인정한다.[26]

또한 ECPA의 제1편과 제2편은 사용자가 통신을 어떤 범죄나 불법행위를 행할 목적으로 가로채기하는 것이 아닌 한, 근로자가 사용자의 감시에 동의함으로써 사용자를 책임에서 면제하는 사전동의(Prior Consent) 예외조항을 포함하고 있다.[27]

---

20) 18 U.S.C. 2510 (2000).
21) 18 U.S.C. 2701(a)(1) (2000).
22) 18 U.S.C. 2707(a)-(c) (2000).
23) 18 U.S.C. 2520(b)-(c), 2707(b)-(c) (2000).
24) 18 U.S.C. 2510(5)(a) (2000).
25) Peter J. Isajiw, *COMMENT: Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 Temp. Envtl. L. & Tech. J. 73, 87 (2001).
26) 18 U.S.C. 2511(2)(a)(i) (2000).
27) 18 U.S.C. 2511(2)(d), 2701(c)(1)-(2) (2000).

나. 판 례

1993년 캘리포니아 항소법원의 Bourke vs. Nissan Motor Corp.사건[28]도 사용자가 근로자의 전자우편에 접근할 권리가 있음을 인정하고 있다. 이 판례에서 법원은 '프라이버시의 기대가 있다고 할지라도 그러한 피용자의 프라이버시보다는 사업을 적절하게 이끌어야 하는 사용자의 이익이 더 중요하다'고 하였다. 1994년에 선고된 Shoars vs. Epson America, Inc.사건[29]에서도 사용자의 감청권을 허용하고 있다.

근로자의 전자우편에 대한 프라이버시에 관한 대표적인 판례 중 하나가 펜실베니아 주법이 적용된 1996년의 Smyth vs. The Pillsburry Co.사건[30]이다. 필스버리 회사는 그 피용자 즉 사원들간의 의사소통의 편의를 위하여 회사 내부적인 전자우편 및 전자우편 시스템을 유지하여 오면서, 사원들에게 모든 전자우편통신의 비밀성(confidential)이 유지되며 그렇게 비밀을 유지할 권리(privileged)가 있음을 확인하였다. 즉 절대로 전자우편통신을 방수(傍受: interception)하지 않을 것이며, 피용자에 반하여 사용하지 않을 것을 보증하였다. 그런데 1994년 한 사원이 자기의 집에서 그 감독자(supervisor)로부터 전자우편을 받았다. 회사의 전자우편 프라이버시 정책을 믿은 이 사원은 회사와 그 사원들을 비판하는 전자우편을 회신하였는데 회신 내용에는 "Kill the backstabbing bastards(뒤에서 중상모략하는 개자식들을 죽여라)" 등의 말이 포함되어 있었고, 이 사원의 전자우편은 중간에 방수가 되었으며 후에 그의 고용관계를 종료케 하는 근거로 사용되었다. 이 사건에 대하여 법원이 결정하여야 할 쟁점은 그러한 상황에서 사용자의 행위가 '안온침범(安穩侵犯)'이라는 불법행위를 구성하느냐의 문제였다. 즉 그 방수행위가 사원의 프라이버시에 대한 실질적인 침해가 되느냐의 여부 및 일반적으로 합리적인 사람에게 고도의 침해를 가져오는 것인가의 여부였다. 법원은 그러한 프라이버시에의 합리적인 기대가 '전자우편 통신이 피용자가 그 감독관에게 회사의 전자우편 시스템을 통하여 자발적으로 이루어진 것'이라는 점을 들어, 프라이버시의 침해를 가져오지 않는다고 하였다. 법원의 논리는, 일단 회사 전체가 사용하는 전자우편 시스템을 통하여 피용자가 그 의사를 소통하였다면 프라이버시에 대한 합리적인 기대는 소실되었다고 한 것이다. 더 나아가 법원은, '전자우편 시스템을 통한 부적절하고 직장에서는 해야 될 말이 아닌 언사들 또는 심지어 불법적인 행위를 막기 위한 회사의 이익이 피용자가 스스로의 언사에 관하여

28) Bonita P. Bourke et al. v. Nissan Motar Corporation, No. B068705 (Cal. Ct. App. July 26, 1993)
29) Alana Shoars v. Epson America, Inc., No. B073234 (Cal. Ct. App. Apr. 14, 1994)
30) 914 F. Supp. 97 (E.D. Pa. 1996); 이에 대한 평석으로는 권영설, 사용자의 근로자 이메일전자감시와 사업장에서의 사생활권, 개인정보연구 제2권 제1호, 한국정보보호진흥원, 2003, 313~326쪽 참조.

지니는 프라이버시라는 이익보다 중요하다'고 하였다. 결국 이 사건에서는 근로자가 자신의 상급자로부터 받은 전자우편에 대해 공격적인 언사와 협박을 담은 답장을 한 것을 사용자가 임의로 감청한 데 대해, 법원은 회사가 갖는 부적절하고 비업무적인 언행이나 불법한 행동을 방지할 이익이 근로자의 프라이버시보다 우월하다고 하여 감청을 용인하고 있다.

3. 우리의 법제

가. 통신비밀보호법

사용자가 근로자의 전자우편을 열람하는 행위와 관련하여 먼저 통신비밀이라는 프라이버시의 보호측면에서 접근하면, 통신비밀보호법이 우선적으로 적용된다. 통신비밀보호법 제2조 제9호는 전자우편을 '컴퓨터 통신망을 통해서 메시지를 전송하는 것 또는 전송된 메시지'로 정의하고 있다. 한편 통신비밀보호법 제2조 제3호에서 "전기통신이라 함은 전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말한다"고 개념정의하고 있으므로, 전자우편은 통신비밀보호법상의 전기통신에 해당된다 할 것이다. 동조 제4호에 따르면 전기통신의 송·수신인을 당사자라 할 것이므로, 근로자는 당사자에 해당하지만 사용자는 설령 그 메일서버가 기업시설이라 할지라도 당사자에 해당되는 것은 아니다. 동조 제7호에서는 "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 규정하므로, 당사자인 근로자의 동의 없이 사용자가 근로자를 송·수신인으로 하는 전자우편을 공독하여 그 내용을 지득하는 행위는 통신비밀보호법상의 감청행위에 해당된다.

통신비밀보호법은 이러한 감청행위에 대해 제3조 제1항에서 "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 명시하고 동조 제2항에서 "우편물의 검열 또는 전기통신의 감청(이하 '통신제한조치'라 한다)은 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다"고 규정함으로써 감청행위를 금지하고 있다. 물론 동조 제1항 단서에서 "다만, 다음 각호의 경우에는 당해 법률이 정하는 바에 의한다"고 하고 제1호에서 제5호까지의 예외규정을 두고 있으나 사용자가 근로자의 전자우편을 감청하는 행위에 대해서는 해당사항이 없다.

따라서 사용자가 근로자의 전자우편을 감청하거나 지득한 통신 또는 대화의 내용을 공개하거나 누설하는 것은 통신비밀보호법 제3조에 위반하는 위법한 행위이며, 동법 제16조 제1항의 벌칙에 의거 10년 이하의 징역과 5년 이하의 자격정지에 처해지는 행정형벌(行政刑罰)이 부과될 수 있다.

나. 정보통신망이용촉진및정보보호등에관한법률

정보통신망이용촉진및정보보호등에관한법률 제49조에서는 "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다"라고 규정하고 있다. 근로자의 전자우편은 정보통신망이용촉진및정보보호등에관한법률의 개념정의에 따르면 '개인정보'는 아니지만 '정보통신망에 의하여 처리·보관 또는 전송되는 개인비밀'이며, 동조는 '정보' 뿐만 아니라 '타인의 비밀'도 보호객체로 명시하고 있으므로 동조의 적용에 영향을 주지는 않는다고 보인다. 따라서 사용자가 근로자의 전자우편을 열람하는 행위는 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 비밀을 침해하는 행위가 되며, 결국 동법 제62조 제6호에 의거하여 5년 이하의 징역 또는 5,000만원이하의 벌금이라는 처벌을 받게 될 것이다.

다. 노동관계법

현행 노동관계법에서는 사용자가 근로자의 개인정보나 프라이버시를 보호해야 할 의무를 구체적으로 명시하고 있지 아니하다. 그러나 노동법이론에 따를 경우, 사용자의 부수적 의무로서 사용자의 배려의무가 인정되고 있으며, 구체적인 내용으로는 신체안전 배려의무, 물건이나 인격·인권의 침해를 방지할 배려의무 등이 인정되고 있다. 따라서 사용자가 근로자의 전자우편을 열람하는 행위는 사용자의 배려의무에 위반하는 인격 내지 인권침해행위가 될 것이고, 그 효과로는 근로자의 사용자에 대한 채무불이행으로 인한 손해배상청구가 인정될 것이며, 또한 사용자에게 적절한 조치를 강구할 것을 청구할 수 있다고 할 것이다. 반면에 사용자는 근로자에 대해 업무지시감독권을 갖는 것으로 이론상 정립되어 있으므로, 회사의 업무시설인 전자우편시스템을 오직 업무용으로만 사용하고 사적인 용도로 사용하지 못하도록 지시·감독할 권한이 있으며, 그러한 지시가 존재하는 경우에 업무상의 전자우편을 감청하는 것은 허용될 수도 있을 것이다.[31]

라. 형식적 법적용

우리나라의 법규정은 통신비밀침해에 관해 미국과 달리 매우 포괄적인 금지를 원칙으로 하

31) 오병철, 같은 글(註 7), 265~266쪽.

고 있다. 즉 불법감청에 대한 통신비밀보호법 제3조 위반 및 동법 제16조 적용의 경우와 비밀침해에 대한 정보통신망이용촉진및정보보호등에관한법률 제49조 위반 및 동법 제62조 적용의 경우가 그러하다. 보다 구체적으로는 통신비밀보호법은 다섯 가지의 예외를 규정하고 있으나 극히 제한적인 경우만을 열거하고 있으며, 정보통신망이용촉진및정보보호등에관한법률에서는 예외조차 명시되어있지 아니하다. 결국 법적용 범주는 매우 넓고 광범위하게 정해져 있다.[32)]

형식적으로 적용해보면, 근로자의 전자우편을 사용자가 감청하는 것은 어떠한 경우에도 통신비밀보호법 제3조와 정보통신망이용촉진및정보보호등에관한법률 제49조를 위반하는 위법행위가 성립된다고 할 수 있다. 그러므로 법조경합이 이루어지며, 처벌규정에 따라 통신비밀보호법의 10년 이하 징역 및 5년 이하 자격정지와 정보통신망이용촉진및정보보호등에관한법률의 5년 이하 징역 또는 5,000만 원 이하의 벌금 가운데 중한 형인 10년 이하 징역 및 5년 이하 자격정지의 처벌이 가능할 것으로 생각된다.

Ⅳ. 결 론

사내 문서보안 및 정보유출방지 등의 이름으로 기업 내부에 각종 보안제품이 구축되면서, 직장내 전자감시가 고도화되고 있다. 산업스파이로부터 재산권을 지키려면 어느 정도의 전자감시는 어쩔 수 없지 않겠느냐는 합의 속에서, 근로자의 프라이버시는 소홀하게 다뤄져 왔다. 하지만 직장내 전자감시가 직원 동의 없이 이뤄질 경우 사기저하는 물론 경영진과 분열로 이어져 결국 경영성과에도 부정적인 영향을 미칠 것이라는 주장이 제기된 바 있다. 이러한 시각에서 불가피한 경우에 이뤄지는 감시기술과 프라이버시 사이에 균형점을 찾기 위한 법제도적 대응이 시급하다. 결국 정당한 감시・감청・검열을 노사간의 합의 내에 이끌어내면서 근로자의 존엄성과 프라이버시를 지킬 수 있는 방향으로 법제정비가 마련되어야 할 것이라 본다.

1. 감시원칙

일반적으로 사용자의 감청이 허용되지 않아야 함에도 불구하고, 사용자의 사실상 경제적으로 우월한 지위나 사용자의 기업시설관리권 그리고 업무지시감독권을 근거로 하여 전자우편의 감청이 성행할 우려가 있다. 뿐만 아니라 기존 법률규정의 추상성・포괄성을 기화로 침해행위발생의 위험성이 남아 있다. 또한 기업으로서는 사용자가 갖는 시설관리권의 행사로써

32) 한국정보보호센터, 같은 책(註12), 90쪽.

근로자의 전자우편에 대한 일정한 범위의 통제가 가능하게 된다. 또한 사용자의 업무감독권을 근거로 한 감청 또한 일정한 한도에서는 일률적으로 위법이라고 단정할 수 없을 것이다.

따라서 다음에 대하여 기준을 설정하는 것은 매우 의미 있는 일이 될 것이다.[33]

첫째로 사용자가 근로자와의 근로계약 혹은 근로규칙이나 단체협약을 통해 근로자가 개인적인 용도로 회사의 전자우편을 사용할 수 없도록 금지할 수 있을 것인가의 문제에 대해 살펴볼 필요가 있다. 이 경우는 전자우편의 사적 용도의 사용자체를 금지하는 것이므로, 통신비밀의 보호라는 측면의 프라이버시와 충돌되지 않는다. 또한 기업의 시설을 여하한 방법과 내용으로 사용하도록 할 것인가는 사용자의 시설관리권과 업무지시권의 핵심적인 내용을 구성하므로, 근로자는 그러한 관리권의 행사와 지시에 복종하여야 할 것으로 생각되어진다. 따라서 근로자가 사적 용도로 회사의 전자우편을 사용할 수 없도록 하는 것은 허용된다고 보아야 할 것이다.

둘째로 사용자가 근로자에 대해 사적 용도로 전자우편을 이용할 수 없도록 금지하여 근로자가 업무용으로만 사용하는 전자우편에 대해서 감청이 허용되는가의 문제가 존재한다. 이 경우에는 근로계약이나 근로규칙 또는 단체협약 등을 통해 전자우편을 사적으로 이용하지 않도록 금지하고 있으므로, 업무용의 전자우편을 사적 용도로 사용하는 것 자체가 사용자의 업무지시권을 위반하는 것이 될 것이다. 또한 업무용의 전자우편은 그 정보내용의 보호법익이 기업을 위해 존재하는 것이므로 사용자는 근로자의 업무용외 전자우편을 감청하는 것이 허용된다고 보아야 할 것이다.

셋째로 사용자와 근로자 사이에 전자우편의 이용에 관한 어떠한 특약도 존재하지 않는 경우에 사용자는 근로자의 전자우편을 감청할 수 있을 것인가의 문제가 존재한다. 이 경우에는 전기(前記)한 바처럼 우리 법규에 따라 사용자의 감청권은 허용되지 않는다고 보아야 할 것이다. 또한 전자우편의 용도에 관한 약정 없이 일반적 감청권을 사용자에게 부과하는 근로계약이나 근로규칙 또는 단체협약은 허용되지 않는다고 보아야 할 것이다.

무엇보다 사용자가 자신이 결정하는 방식으로 사업을 운영할 권리만을 내세워 일방적으로 할 것이 아니라, 서로간의 신뢰를 바탕으로 양자의 이익을 극대화하는 방향으로 근로자를 참여시켜 근로자가 동의하는 정책을 수립하여야 한다. 이때 사용자는 감시정책에 맞는 실행수단을 모두 공개하고, 그 실행은 감시정책에 따라 행해질 것이라는 사용자의 보증이 있는 것이 바람직하다.[34] 감시정책이란 언제・어떻게・왜 감시가 행하여지며 누구에게 전자우편의 내용

33) 오병철, 같은 글(註 7), 267~268쪽.

34) Jay P. Kesan, *Cyber-working or Cyber-shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 Fla. L. Rev. 289, 322-323 (2002).

이 공개될 것인지에 관하여 구체화하는 것을 의미하는데, 포괄적인 감시정책은 근로자에 의하여 인터넷과 관련된 기술이 잘못 사용되거나 근로자가 전자우편시스템을 오·남용하는 것에 대하여 사용자가 스스로 보호하고 문제가 발생하기 전에 그것을 발견하여 법적 책임의 가능성을 감소시키기 위한 효과적인 수단이 된다. 사용자가 감시정책을 수립할 때에는 사용자의 이해관계가 균형이 이루어지도록 수립하는 것이 바람직할 것이다.[35]

이와 같은 감시정책을 통하여 사용자의 책임은 감소될 뿐만 아니라 프라이버시 침해에 관한 근로자의 요구에 대하여 강력한 방어를 할 수 있게 될 것이다.[36] 이처럼 명백하고 상세한 정책을 통하여 감시의 범위를 근로자에게 통지함으로써 근로자로 하여금 사용자의 감시정책의 실제가 어떠한지 알게 하여, 전자우편시스템을 계속해서 잘못 사용하거나 남용하는 것이 근로자의 전자우편 프라이버시를 감소시키게 될 것이라는 사실을 근로자에게 경고하는 효과가 있을 것이다.[37] 그리고 감시에 관한 사용자의 이유를 설명하는 정책이 존재함으로써 사용자에 의한 전자우편 가로채기에 관하여 근로자의 우려를 감소시키는 데 기여한다. 또한 감시정책은 법규가 애매할 때 기업 행위의 합리성 여부를 법원이 결정하는 데도 도움이 된다.[38]

2. 정책제언

가. 근거법규 제시

결론적으로 전자우편의 용도에 관한 근로자와의 합의를 통해 사용자는 사적인 용도로의 이용을 금지할 수 있으며, 이러한 금지의 합의가 존재하는 경우에는 일반적인 감청권이 허용된다고 보아야 할 것이다. 반면에 전자우편의 용도에 관한 합의가 존재하지 않는 경우에는 감청권 부여의 합의는 위법하다고 보아야할 것이며, 사용자의 감청행위도 위법한 행위가 된다고 보아야 할 것이다. 하지만 근로자의 전자우편을 감청하는 사용자의 행위는 현행법에 의해서도 위법행위로 처벌할 수 있는 충분한 법적 근거가 마련되어 있다. 상술(上述)한 통신비밀보호법과 정보통신망이용촉진및정보보호등에관한법률의 관련규정만으로도 불법행위로 구성되는 전자우편의 감청에 대하여 행정형벌이 부과될 수 있기 때문이다.

---

35) Larry O. Natt Gantt, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 Harv. J. Law & Tec 345, 346 (1995).

36) Gantt, *supra note35*, at 405.

37) Jarrod J. White, *COMMENTARY, E-mail@work.com: Employer Monitoring of Employee E-mail*, 48 Ala. L. Rev. 1079, 1103 (1997).

38) Laurie T. Lee, *Watch Your E-mail!: Empoyee E-mail Monitoring and Privacy Law in the Age of the Electronic Sweatshop*, 28 J. Marshall L. Rev. 139, 173 (1994).

하지만 당해 전자우편이 근로자를 수신자로 할 경우에는 직장이라는 공간적 특수성과 사용자와의 관계를 함께 고려해야 한다. 따라서 원천적으로는 처벌근거를 따지는 규범설정의 문제 이전에 노동현장에서 이루어져야 할 규준정립의 과제가 선행되어져야 한다. 다시 말해 사용자와 근로자가 함께 논의하여 감시정책을 수립함으로써 불법감청이 지양되도록 원만한 노사합의를 이끄는 현실적 절충 역시 중요하다는 뜻이다. 이러한 연유에서 근로현실에 국한된 사용자와 근로자의 과제는 정보통신관련법령에 규정하기보다 근로기준법 등 노동관계법에 규정되어야 적절할 것으로 생각되어진다. 다만 정보통신망을 이용한 전자우편의 감청 혹은 통신비밀보호의 대상이 되는 전자우편에 대해 적절한 감시정책을 유도하는 정보통신부 고시의 지침을 마련하는 것은 전자우편감청에 대한 사용자와 근로자의 상호이익을 조율하는 데 도움을 주리라 여겨진다. 따라서 적정한 입법방향을 수용하는 범위에서, 중복입법문제를 고려하여 정보통신망이용촉진및정보보호등에관한법률 또는 통신비밀보호법의 개정에 따라 근거규정을 신설하고 보호지침을 제정하는 방안은 실효성을 지닐 수 있을 것으로 사료된다. 판단컨대 통신의 비밀이라는 프라이버시에 주안점을 두고 전자우편에 대한 정의규정을 갖고 있는 통신비밀보호법에 그러한 내용을 담아내는 것이 합당하리라 본다. 이러한 견지에서 통신비밀보호법 제3조 제3항으로 "정보통신부장관은 노동부장관과의 협의를 거쳐 근로자의 통신비밀보호를 위해 작업장에서의 통신제한조치에 대응하는 보호지침을 정하여 고시하고 사용자에게 그 준수를 권고할 수 있다"는 보호지침의 근거규정을 새로이 도입하고 이에 따라 적정한 내용을 수용하는 보호지침을 제정하는 것이 근로자와 사용자 상호간의 이익균형에도 상응할 것으로 보인다.

나. 보호지침 제안

전술(前述)한 바와 같이 통신비밀보호법에 근거규정을 신설한다면, 이에 따라 고시되어야 할 전자우편비밀보호지침은 다음과 같은 내용으로 구성하여 고시한 날부터 시행하도록 하여야 할 것이다.

1) 목 적

이 지침은 통신비밀보호법[39] 제3조 제3항의 규정에 의하여 사용자가 근로자의 전자우편을 감청함에 요구되는 통신비밀의 보호에 대한 구체적 내용을 정하는 것을 목적으로 함을 밝히도록 한다.

2) 정 의

이 지침에서 사용하는 용어의 정의를 다음과 같이 규정하도록 한다.

39) 이하 "법"이라 약칭(略稱)하도록 한다.

첫째, "근로자"라 함은 근로기준법 제14조의 규정에 의해 직업의 종류를 불문하고 사업 또는 사업장에 임금을 목적으로 근로를 제공하는 자를 말하며, 동의 및 협의의 당사자로서 노동조합을 포함한다.

둘째, "사용자"라 함은 근로기준법 제15조의 규정에 의해 사업주 또는 사업경영담당자 기타 근로자에 관한 사항에 대하여 사업주를 위해 행위하는 자를 말한다.

셋째, "전자우편"이라 함은 법 제2조 제9호의 규정에 의해 컴퓨터 통신망을 통해서 메시지를 전송하는 것 또는 전송된 메시지를 말한다.

넷째, "감청"이라 함은 법 제2조 제7항의 규정에 의한 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.

3) 원 칙

전자우편 감청에 있어 원칙적인 일반규정을 다음과 같이 두도록 한다.

첫째, 전자우편에 대한 감청은 법 제3조 제1항에 의거 원칙적으로 금지되며, 근로자의 동의절차를 거치지 아니한 어떠한 감청도 불법행위를 구성하며 법 제16조 제1항의 규정이 적용된다.

둘째, 사용자는 위 첫째 내용의 원칙에 부합하도록 근로자와의 사전동의(事前同意)를 얻는 협의를 하여 사내 전자우편감청원칙을 사규 또는 단체협상에 반영할 수 있다.

셋째, 사용자는 개인용도로 전자우편시스템을 사용하는 것을 금하는 지시를 할 수 있으므로 근로자에게 업무와 관련된 전자우편만을 열람하도록 할 수 있다. 다만 이에 대한 근로자와의 협의 및 동의절차가 준수되어야 한다.

넷째, 상법 등의 규정에 의하여 사내 보존해야 할 문서에 근로자의 전자우편이 해당할 경우에는 근로자에게 해당 전자우편이 보존됨을 공지하고 법률에 정해진 바에 따라 보존되거나 이용되어야 한다. 다만 이에 대한 구체적 절차는 근로자의 사전동의를 얻어 협의할 수 있다.

4) 근로자의 동의

협의에 필수조건인 근로자의 동의에 대하여 다음과 같이 규정하도록 한다.

첫째, 근로자의 동의는 반드시 사전동의로 하여야 하고 동의는 철회될 수 있다.

둘째, 사용자는 전자우편의 보존 목적·전자우편의 보존 기간·전자우편의 보존에 대한 책임부서 및 책임자·전자우편의 보존에 대한 방법 및 처리과정 그리고 보존장소·보존된 전자우편의 이용목적과 사용범위 등의 사항을 서면으로 명확하게 근로자에게 고지하여야 한다.

셋째, 보존된 전자우편은 본래 목적을 위해서만 사용될 수 있다.

넷째, 보존된 전자우편은 업무수행의 내용과 관련해서만 근로자의 직무평가에 이용될 수 있으며, 특정한 근로자에 대한 감시의 목적으로 보존되거나 이용되어서는 아니된다.

다섯째, 보존된 전자우편은 어떠한 경우에도 업무와 직접적으로 관련 있는 목적 이외에는 이용될 수 없다.

5) 관리책임자의 지명

전자우편의 보존 및 관리에 책임을 지는 자를 지명하는 내용으로 다음과 같이 정하도록 한다.

첫째, 사용자는 사내 전자우편의 보존 및 관리를 담당할 관리책임자를 지명하여야 한다.

둘째, 관리책임자는 사용자를 대리하여 전자우편 감청에 대한 협의를 할 수 있으며 사용자의 부당한 감청지시에 불응할 권한이 있다.

6) 관리책임자의 책무

전자우편에 관한 관리책임자의 수행업무범위를 다음과 같이 규정하도록 한다.

첫째, 관리책임자는 사내 전자우편의 보존 및 관리에 대한 지시·감독 업무를 행한다.

둘째, 관리책임자는 전자우편시스템의 장애 등으로부터 정보를 보호하기 위하여 적절한 조치를 취하여야 한다.

7) 전자우편의 검색

정당한 감청이 되기 위한 적법절차에 대하여 다음과 같이 두도록 한다.

첫째, 사용자가 소프트웨어를 통해 검색어를 이용하는 것은 원칙적으로 허용된다.

둘째, 위 첫째 내용의 검색에서 사용자가 필요하다고 판단하여 열람할 경우에는 전자우편의 수신자인 근로자에게 그 검색결과와 열람필요성을 고지한 후에만 열람할 수 있다.

셋째, 위 첫째 및 둘째 내용의 검색에 있어 검색어는 노동조합활동·근로자의 단결권 등과 같은 근로자의 노동법상 권리행사와 관련되어서는 아니 되며, 이러한 검색어를 사용하는 경우에는 부당노동행위가 성립한다.

8) 사용자와 근로자의 협력

업무와 관련된 전자우편만을 근로자가 사용하도록 합의한 경우라도 근로자에게 보호되어져야할 통신의 비밀이 존재함을 사용자는 인식하고 이 지침에 따라 제한적인 경우에만 근로자의 동의를 얻어 업무와 직접 관련된 목적으로만 보존하거나 이용하도록 할 것이며, 근로자는 합의를 준수하여 업무이외의 사적 용도로 전자우편을 사용하지 않도록 노력해야 한다.

9) 예 외

사용자가 이 지침으로부터 특별한 예외를 적용받으려면, 사내 특별한 상황이 일반적으로 적용되는 원칙으로부터 예외적으로 취급받을 수 있는지 합리적인 설명을 제공할 수 있어야만 한다. 이러한 예외의 적용은 근로자와의 협의·동의에 대하여 구속된다.

10) 권 고

권고사항에 대하여 다음과 같이 규정하도록 한다.

첫째, 사용자는 이 지침의 내용에 저촉되지 않는 범위 내에서 사규 혹은 단체협약 등에 전자우편 감청에 대한 원칙을 천명하도록 한다.

둘째, 위 첫째 내용의 원칙이 업무목적 이외의 사적 용도의 전자우편 사용도 근로자에게 인정되는 내용을 포함한다면 전자우편의 감청은 통신제한조치로서 불법행위를 구성하므로 사용자는 원칙을 준수하도록 한다.

셋째, 사용자와 근로자 사이의 전자우편 사용원칙이 정해지면 근로자는 전자우편의 사용범위를 유월하지 않는 한도에서 이용하도록 한다.

참 고 문 헌

[1] 권영설, 사용자의 근로자 이메일전자감시와 사업장에서의 사생활권, 개인정보연구 제2권 제1호, 한국정보보호진흥원, 2003.

[2] 김왕배 · 이경용, 인터넷 사용과 직무감시－주관적 인식을 중심으로－, 경제와사회 통권 제57호, 한울, 2003.

[3] 김철완 · 이민영, 인터넷 개인정보보호에 관한 법제도 연구, 정책연구 00-10, 정보통신정책연구원, 2000.

[4] 오병철, 직장내 사용자에 의한 근로자의 전자우편 감청, 과학기술법연구 제6집, 한남대학교 과학기술연구소, 2000.

[5] 이희성, 작업장내에서의 전자메일 및 CCTV의 감시와 근로자의 프라이버시보호, 비교사법 통권 제20호, 한국비교사법학회, 2003.

[6] 한국정보보호센터, 전자우편 사용자 보호방안에 관한 연구, 정책연구 00-4, 한국정보보호센터, 2000.

[7] 노동감시실태 조사결과 발표 및 노동감시근절대책 촉구 기자회견, 근로자감시근절을위한연대모임, 2003. 7. 31.

[8] Jarrod J. White, *COMMENTARY, E-mail@work.com: Employer Monitoring of Employee E-mail*, 48 Ala. L. Rev. 1079 (1997).

[9] Jay P. Kesan, *Cyber-working or Cyber-shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 Fla. L. Rev. 289 (2002).

[10] Larry O. Natt Gantt, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 Harv. J. Law & Tec 345 (1995).

[11] Laurie T. Lee, *Watch Your E-mail!: Empoyee E-mail Monitoring and Privacy*

Law in the Age of the Electronic Sweatshop, 28 J. Marshall L. Rev. 139 (1994).

[12] Mark S. Kende, *The Issues of E-mail Privacy and Personal Jurisdiction: What Clients Need to Know About Two Practical Constitutional Questions Regarding the Internet*, 63 Mont. L. Rev. 301 (2002).

[13] Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-mail Privacy*, 1 J. High Tech. L. 101 (2002).