노동감시 대응 가이드

노동감시 대응 가이드

발행 2021년 11월 22일 펴냄

지은이 노동감시 대응 사업단
주소 (우)03745 서울특별시 서대문구 독립문로8길 23 3층
전화 02-774-4551
팩스 02-701-7104
홈페이지 guide.jinbo.net/workplaceSurveillance

펴낸곳 리시올
출판등록 2016년 10월 4일 제2016-000050호
주소 서울시 마포구 희우정로16길 39-6, 401호
전화 02-6085-1604
팩스 02-6455-1604
이메일 luciole.book@gmail.com

제작 상지사

ISBN 979-11-90292-13-9 00300

구체적인 방식과 양상은 시대에 따라 달라졌지만, 자본은 항상 노동자의 노동 과정을 통제하고자 했습니다. 노동자가 주어진 업무를 제대로 수행하고 있는지 파악하는 데는 노동자의 상태와 행위, 작업 과정과 결과물에 대한 감시가 필연적으로 수반됩니다. 디지털 기술의 발전은 노동 과정에 대한 감시를 더욱 은밀하고 체계적으로 수행할 수 있게 합니다. 그러나 노동자 입장에서 감시는 그 자체로 인간 자율성에 대한 제한이고 나아가 프라이버시권 등 기본권을 침해할 수 있습니다. 어디까지 허용될 수 있는 감시이고 어디서부터 그렇지 않은지에 대한 객관적 기준은 없습니다. 이 역시 노사간의 이해가 부딪히고 협상하고 싸워야 하는 또 하나의 공간입니다. 이를 위해 노동감시가 무엇이고 어떻게 이루어지는지 이해할 필요가 있습니다.

국내에서도 이미 2000년대 초반부터 노동감시에 대한 문제의식이 형성되었습니다. 최초로 '노동자감시 대응 지침서'가 나온 것이 2004년입니다. 당시 여러 노동·정보인권 단체들은 '노동자감시 근절을 위한 연대모임'을 구성하고 『노동

자는 감시를 거부할 권리가 있다』라는 제목의 지침서를 발간하였습니다. 당시에는 노동감시를 규율하는 법률은 물론이고 개인정보의 보호에 관한 일반법조차 없었습니다. 감시설비를 통해 수집되는 개인정보 처리에 대한 규율을 통해, 일정하게 노동감시 문제를 다룰 수 있는 개인정보보호법이 제정된 것은 2011년에 이르러서입니다. 개인정보보호법도 개인정보처리자와 정보주체의 대등한 관계를 전제로 하므로, 권력 관계가 불평등한 노사관계를 규율하는 데에는 한계가 있습니다.

기술은 더욱 고도화되고 있습니다. 빅데이터라 불리는 대규모 데이터를 처리할 수 있게 되었고, 인공지능이 사람을 대신하여 다양한 결정을 내립니다. 사물인터넷 등 인식기술의 발전으로 노동자와 노동과정의 미세한 움직임도 파악하여 데이터화할 수 있습니다. 그러나 2004년 지침서가 발간된 이후 거의 20년이 다 되어 가지만, 기술의 발전과 법제도의 변화를 반영하는 지침서의 개정은 없었습니다. 행정자치부와 고용노동부가 발간한「개인정보보호 가이드라인(인사·노무편)」이 있지만, 직장 내 개인정보 처리에 관한 설명만을 제공할 뿐 감시설비의 도입 원칙, 절차, 안전조치에 대한 내용은 다루고 있지 않습니다. 노동감시나 감시설비를 구체적으로 규율하는 법제 역시 아직 도입되지 않았습니다. 어쩌면 노동감시와 관련된 회사 내 관행은 20년 전과 크게 달라지지 않은 것 같습니다.

그러나 결국 중요한 것은 현장입니다. 현장에서 감시설비가 노동자의 권리를 침해하고 있는지 인식하고, 부당한 감시설비 활용에 대해 조직적으로 대응할 수 있어야 합니다.『노동감시 대응 가이드』는 현장에서 도입된 감시설비에 문제가 있는지를 인식하고, 이에 대응할 수 있는 법제도적인 혹은 전략적인 방향을 제시하려는 의도로 제작되었습니다. 이 가이드는 책자와 온라인으로 제작되며 기술과 제도 변화에 따라 업데이트될 것입니다. 이 가이드가 현장의 노동자와 노동조합이 노동감시 문제에 적극 대응하고 노동자의 권리를 보호하는 데 조금이나마 일조할 수 있기를 기대합니다.

차례

1장
개요

1. 노동감시란

노동감시란 사업장 내에서 노동자의 작업상황이나 행동을 모니터링하는 것을 의미한다. 노동자 감시 혹은 사업장 감시라고도 하며, 이러한 감시가 디지털 전자기술을 통해서 주로 이루어지는 것에 주목하여 사업장 전자감시, 전자적 노동감시라는 용어가 사용되기도 한다. 국가인권위원회는 '사업장 전자감시'를 "사업장 내 작업상황 및 근로자 행동의 모니터링 또는 감시를 목적으로 한 전자장비의 설치·운영"으로 규정한 바 있다.[1]

디지털 전자기술이 도입되기 이전부터 사용자(이 가이드에서 '사용자'란 근로기준법상의 사용자로서 근로자와 고용관계를 맺고 있는 고용주 혹은 회사를 의미한다)는 노동자들이 근무 시간 동안 성실히 일을 하고 있는지 감시하고 노동을 통제해 왔다. 그러나 CCTV, 스마트카드, 인터넷 모니터링 등 디지털 감시설비를 도입함으로써 사용자는 보다 정밀하고 은밀하게 노동자를 감시할 수 있다. 물론 비단 노동자 감시를 목적으로 뿐만 아니라 영업비밀 보호, 시설이나 노동자 안전, 업무 효율성 등을 명분으로 디지털 전자기술이 도입되기도 한다. 그러나 정당한 명분으로 도입된 전자기술 역시 노동자를 감시하기 위한 목적으로 활용될 수 있다.

이러한 노동감시는 근로자의 개인정보자기결정권, 인격권, 사생활의 비밀과 자유 등 기본권을 침해할 수 있다. 사용자의 지휘·감독 권한을 인정하더라도 사업장 내에서 노동자의 기본권 침해가 정당화되는 것은 아니다. 예를 들어 사업장 내에서도 노동자는 일정하게 자신의 사생활을 보장받을 권리가 있다. 또한 노동감시는 노동조합의 설립이나 활동을 위축시킴으로써 노동자의 단결권·단체행동권·단체교섭권 등을 제약할 수 있다.

그러므로 사업장 내에서 노동자의 기본권 보호를 위해서 사업장 전자감시를 적절하게 통제할 필요가 있다. 즉 디지털 감시설비의 도입 절차, 운영의 범위 및 양태, 노동자의 권리와 구제 절차 등이 제도적으로 마련될 필요가 있다.

2. 본 가이드의 구성

현재 국내에는 노동감시를 규율할 수 있는 법제가 일부 존재한다. 2장에서는 노동감시와 관련된 법률이 무엇인지 개략적으로 설명한다. 해당 법률이 구체적인 사례에서 어떻게 적용되는지에 대해서는 이후 장에서 관련된 항목이 나올 때 다룰 것이다. 물론 현행 법제의 한계도 존재한다. 따라서 본

가이드에서는 노동감시와 관련된 법제가 무엇인지, 구체적인 사례에 어떻게 적용되는지뿐만 아니라, 현행 법제의 한계는 무엇이고 어떻게 개선되어야 하는지도 언급할 것이다. 장기적으로 노동감시가 없는 사업장을 만들기 위해서는 우리가 함께 현행 법제를 개선해 나가야 하기 때문이다.

3장은 노동감시에 개인정보보호법이 어떻게 적용되는지 설명한다. 노동감시에 사용되는 기술의 종류와 상관없이 노동감시를 통해 일정하게 노동자의 개인정보가 수집·활용되며, 따라서 기본적으로 개인정보보호법이 적용될 수밖에 없기 때문이다. 이후 4장에서는 활용되는 전자기술의 종류에 따라 개인정보보호법 및 다른 법률이 어떻게 적용되고 해석되는지, 그리고 노동자들이 전자기술의 도입에 어떻게 대응해야 하는지 설명한다. 5장에서는 인공지능, 플랫폼 등 신기술이 노동감시에 어떠한 영향을 미칠지, 이에 어떻게 대응해야 할지를 다룬다.

2장

노동감시 관련 법제

2장에서는 노동감시와 관련된 법제를 개략적으로 소개한다. 이를 알아야 법적인 근거를 갖고 노동감시에 대응할 수 있기 때문이다. 해당 법률이 구체적인 사례에 어떻게 적용되는지는 3장과 4장에서 설명할 예정이다.

1. 헌법

사업장 내에서도 노동자의 헌법적인 권리는 보장되어야 한다. 우리나라 헌법 제17조는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다"라고 규정하고 있다.

근로자의 인격과 노동이 밀접한 관계라는 관점에서 노동감시는 근로자의 인격권 침해도 될 수 있다. 인격권이란 헌법 제10조에서 도출되며 자신과 분리할 수 없는 인격적 이익을 누릴 권리이다. 헌법 제10조는 "모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다"고 규정하고 있다.

헌법에 명시되어 있지는 않지만 헌법재판소는 2005년 결정에서 개인정보자기결정권을 헌법상의 권리로 인정하였다.[2] 개인정보자기결정권은 자신에 대한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보 주체가 스스로 결정할 수 있는 권리이다.

2. 개인정보보호법

개인정보보호법은 개인정보의 처리에 관한 일반법이다. 기업이 수집하는 소비자의 개인정보든, 정부가 수집하는 국민의 개인정보든, 사용자가 수집하는 노동자의 개인정보든 다른 법에 특별한 규정이 없는 한 개인정보보호법이 적용된다.

디지털 감시설비가 개인정보만을 다루는 것은 아니지만, 이를 통해 이루어지는 노동감시는 노동자의 개인정보 수집에 기반할 수밖에 없기 때문에 개인정보보호법이 적용될 가능성이 크다. 현행 법제 중에서 노동감시에 대한 가장 구체적인 규정을 담고 있는 것이 개인정보보호법이기 때문에, 이를 3장에서 다시 설명할 것이다.

3. 위치정보의 보호 및 이용 등에 관한 법률(약칭: 위치정보법)

개인의 위치정보와 관련해서는 개인정보보호법 이전에 위치정보법이 적용된다. '위치정보'란 "이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보"이다. 특정한 개인의 위치정보를 '개인 위치정보'라고 하며, 이 역시 개인정보가 된다. 휴대전화, 자동차와 같은 사물의 위치정보가 수집되는 경우에도 이 사물의 위치정보가 특정한 개인과 연결되어 있을 경우 개인 위치정보가 될 수 있다. 예를 들어 설치기사가 들고 다니는 단말기의 GPS를 통해 설치기사의 위치를 파악할 수 있다면 위치정보법이 적용되는 것이다.

위치정보를 이용한 다양한 서비스를 제공하는 사업자를 '위치기반서비스사업자'라고 하고, 위치정보를 수집해서 서비스사업자에게 제공하는 사업자를 '위치정보사업자'라고 한다. 기지국을 통해 내 위치정보를 수집하는 SKT, KT, LGU+ 등 이동통신사나 휴대전화의 GPS를 통해 내 위치정보를 수집하는 구글이나 애플과 같은 모바일 운영체제 업체들이 위치정보사업자라고 할 수 있다. 위치기반서비스사업자는 위치정보에 기반하여 다양한 서비스를 제공하는 앱 사업자들인데, 예를 들어 GPS 정보를 기반으로 길찾기 서비스를 제공하는 네이버, 내 위치를 기반으로 지역 정보를 제공하는 앱 등이 이에 해당한다.

위치정보사업자가 내 위치정보를 수집하고자 하는 경우나 위치기반서비스사업자가 내 위치정보를 제3자에게 제공하려고 하는 경우 정보주체인 내 동의를 받아야 한다. 여기서

제3자는 사용자가 될 수 있는데, 즉 사용자가 어떤 앱(위치기반서비스사업자)을 통해 노동자 차량의 위치정보, 곧 노동자의 위치정보를 파악하는 경우 해당 노동자의 동의를 받아야 하는 것이다.

만일 위치기반서비스사업자가 정보주체가 지정하는 제3자에게 개인의 위치정보를 제공하는 경우, 매회 정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보해야 한다. 예를 들어 노동자의 위치정보가 사용자에게 일정 간격으로 제공되는 경우, 위치기반서비스사업자는 위치정보가 제공되는 매 경우마다 노동자에게 이 사실을 통보해야 하는 것이다. 다만 정보주체의 동의를 받아 최대 30일의 범위에서 일정한 횟수 또는 기간 등의 기준에 따라 모아서 통보할 수 있다. 노사관계 내에서 위치정보 수집이 이루어질 경우 매번 통보하는 것이 번거로울 수 있기 때문에 대부분 모아서 통보하는 방식을 취하게 된다.

위치정보사업자 혹은 위치기반서비스사업자가 정보주체의 동의를 얻지 않거나 동의 범위를 넘어 개인위치정보를 수집·이용 또는 제공한 경우 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처해진다. 이를 "알고 영리 또는 부정한 목적으로 개인위치정보를 제공받은 자" 역시 마찬가지의 처벌에 처해지게 되는데, 사용자가 동의를 받지 않고 부정한 목적, 예를 들어 노동자를 감시하려는 목적으로 노동자의 위치정보를 위치정보사업자 등으로부터 제공받는 경우가 이에 해당한다.

한편 사용자가 직접 제작한 앱이나 블랙박스 등의 설비를 이용해 노동자의 위치를 직접 수집하는 경우도 있을 수 있다. 그럴 경우에도 정보주체인 노동자의 동의를 받아야 하며, 동의 없이 수집·이용 또는 제공할 경우 3년 이하의 징역 또는 3천만 원 이하의 벌금에 처하게 된다.

> **위치정보법**
>
> 제15조(위치정보의 수집 등의 금지) ①누구든지 개인위치정보주체의 동의를 받지 아니하고 해당 개인위치정보를 수집·이용 또는 제공하여서는 아니 된다.

따라서 사업장 내에서 노동자의 위치정보를 수집하는 경우 노동자의 동의를 받아야 하며, 동의를 받지 않았다면 위치정보법 위반이 된다. 물론 사용자가 동의를 요구할 경우 현실적으로 노동자가 동의를 거부하기는 힘들 것이다. 이와 관련한 문제는 3장에서 보다 상세하게 설명할 것이다.

한편 위치정보법은 정보주체(노동자)가 언제든지 동의를 철회하거나 위치정보의 수집·이용·제공의 일시적인 중지를 요구할 권리, 그리고 개인위치정보 자료에 대한 열람 혹은 고지, 정정을 요구할 권리를 보장하고 있다.

4. 통신비밀보호법

노동감시로 인해 노동자의 통신의 비밀과 자유가 침해될 수도 있다. 당사자 몰래 인터넷 통신 내용을 모니터링하거나 전화 혹은 대화 내용을 녹음하는 경우가 이에 해당한다. 통신비밀보호법은 누구든지 우편물의 검열, 전기통신의 감청, 통신내역의 제공, 공개되지 않은 타인 간의 대화를 녹음하거나 청취하지 못하도록 금지하고 있다. 그러나 여기서 검열이나 감청이란 '당사자의 동의 없이' 하는 것을 의미하므로, 사업장 내에서 노동자의 사전 동의를 받는다면 통신비밀보호법 위반이 되지 않을 수 있다. 이를 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인 간의 대화를 녹음 또는 청취한 자는 1년 이상 10년 이하의 징역과 5년 이하의 자격정지의 처벌을 받는다.

통신비밀보호법 제3조의 통신사실확인자료란 통화 내역(통화일시·시간, 통화상대방 등)이나 인터넷 로그기록 등 통신의 내용이 아닌 통신을 한 기록(메타정보)을 의미한다. 제3조에 따르면 당사자 동의 없이 통신사실확인자료를 제공하는 것도 금지되지만, 이에 대한 처벌 규정은 없다. 그러나 위법성이 인정되기 때문에 손해배상을 요구할 수는 있다.

한편 통신비밀보호법이 규율하는 '감청'은 실시간으로 통신 내용을 가로채거나 방해하는 것을 의미한다. 이미 통신이 완료되어 서버에 저장되어 있는 자료에 대해서는 통신비밀보호법이 적용되지 않는다. 예를 들어 서버에 저장된 이메일이나 컴퓨터 하드디스크에 저장된 내용에는 통신비밀보호법이 적용되지 않으며 아래에서 설명할 정보통신망법이 적용된다.

> **통신비밀보호법**
>
> 제2조(정의)
> 7. "감청"이라 함은 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다.
> 제3조(통신 및 대화비밀의 보호) ①누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다.

5. 정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)

전자적 감시를 통하여 수집된 정보가 회사의 정보통신망을 통하여 처리되고 있는 정보라고 한다면 정보통신망법이 적용된다. 정보통신망법 제49조는 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다고 정하고 있다. 따라서 정당한 권한이 없이 회사 내 정보통신망에

저장된 이메일이나 자료의 내용을 확인하고 이를 제3자에게 누설한 경우 정보통신망법이 적용된다. 그런데 이는 타인의 비밀 침해라는 맥락에서 적용되며, 타인의 개인정보를 본인의 동의 없이 유출했다면 개인정보보호법 역시 위반한 것이 된다. 만일 본인의 동의하에 해당 정보에 접근했다면 적법한 접근으로 인정될 수 있을 것이다.

> **정보통신망법**
>
> 제49조(비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.

6. 근로자참여 및 협력증진에 관한 법률(약칭: 근로자참여법)

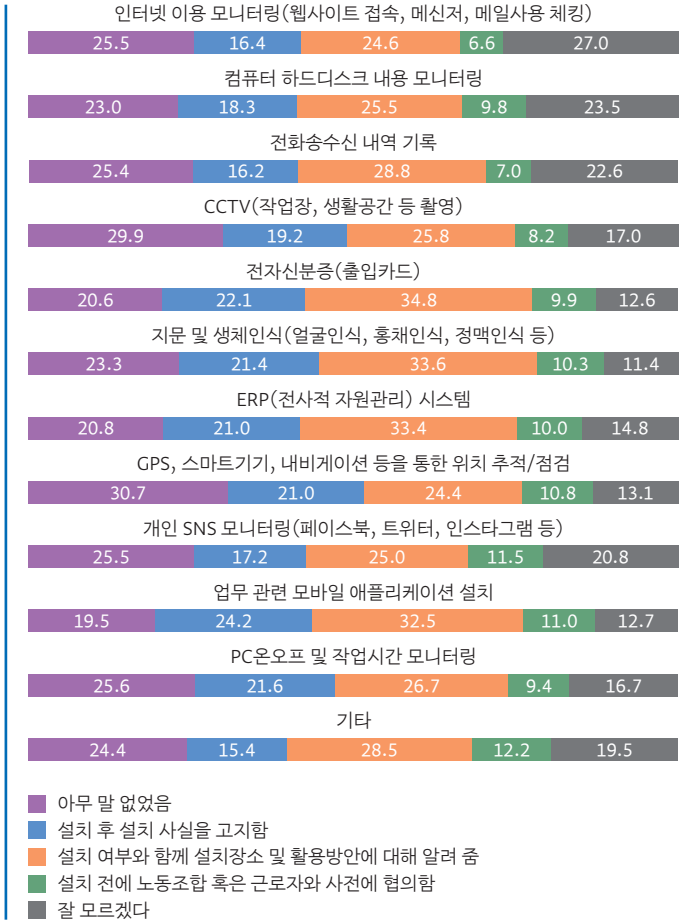
앞서 설명한 개인정보보호법, 위치정보법, 통신비밀보호법, 정보통신망법 등은 일반적으로 적용되는 규정들이며, 사용자와 노동자 사이의 특수한 관계를 고려한 규정을 두고 있지는 않다.

근로자참여법은 제20조는 현행 노동 관련 법률에서 '근로자 감시설비'를 규율하고 있는 유일한 규정이다. 근로자참여법은 30인 이상 근로자를 사용하는 사업장에 노사협의회를 설치하여야 한다고 정하고 있고, 그 노사협의회의 협의 사항으로 "사업장 내 근로자 감시설비의 설치" 정하고 있다.

> **근로자참여법**
>
> 제20조(협의 사항)
>
> ① 협의회가 협의하여야 할 사항은 다음 각 호와 같다.
>
> 1~12. (생략)
>
> 14. 사업장 내 근로자 감시설비의 설치
>
> 15~17. (생략)
>
> ② 협의회는 제1항 각 호의 사항에 대하여 제15조의 정족수에 따라 의결할 수 있다.

그러나 근로자참여법 제20조 위반 시 벌칙이나 과태료 규정이 없어서 노사협의회에서 협의하지 않았다고 하더라도 이를 제재할 방법이 없다. 근로자참여법은 협의회에서 의결된 사항을 이행하지 않는 경우에만 1천만 원 이하의 벌금에 처한다고 정하고 있을 뿐이다. 따라서 근로자참여법이 현실적인 효력을 갖기 위해서는 이에 대한 처벌 규정을 둘 필요가 있다.

> **디지털 전자기술 설치 시 사전 고지 및 협의 미흡**
>
> 2021년 수행된 실태조사[3]에 따르면, 사업장 내에 디지털 전자기술을 설치할 때 고지 없이 설치하는 비율이 20~30% , 설치 후에 고지를 하는 비율이 15~25% 정도로 전반적으로 35~50% 정도 사업장에서 근로자에 대한 사전고지가 미흡한 것으로 나타났다. 노동조합 혹은 근로자와 사전에 협의한다는 비율은 10% 내외에 불과하였다. 50% 이상의 응답자들이 30인 이상 사업장에서 근무하고 있음을 고려할 때, 근로자참여법이 거의 지켜지고 있지 않음을 알 수 있다.



7. 근로기준법

근로기준법은 근로자의 사생활 보호와 관련하여, 제98조 제1항에서 "사용자는 사업 또는 사업장의 부속 기숙사에 기숙하는 근로자의 사생활의 자유를 침해하지 못 한다"라는 일반규정을 두고 있을 뿐이다. 다만 감시설비를 통한 노동자 감시가 해당 노동자에 대한 직장 내 괴롭힘과 연결되는 경우가 많은데, 이 경우 근로기준법이 적용될 수 있다.

사업장 내에서 감시설비의 설치와 관련된 문제가 발생했을 때, 부당한 감시설비의 설치를 감독하거나 노동자 권리의 구제를 요청할 기관으로 고용노동부가 가장 먼저 떠오를 수 있지만, 근로기준법에는 관련 조항이 없고 개인정보보호법의 주무부처도 아니어서 고용노동부는 노동감시와 관련한 감독할 권한이 미흡한 상황이다. 이 문제를 해결하기 위해서는 근로기준법을 개정하여 근로자 감시설비의 설치 요건 및 절차 등을 규율하도록 할 필요가 있다.

8. 노동조합 및 노동관계조정법(약칭: 노동조합법)

노동조합법과 관련해서는 노동자의 개인정보 처리에 관한 사항이 단체교섭의 대상이 되는지가 문제된다. 노동조합법은 단체협약의 구체적인 내용을 명시하지 않고 있는데, 일반적으로 "개별근로자의 근로계약상의 지위를 정하는 협의의 근로조건 사항과 노동조합에 관한 사항"을 단체교섭의 대상으로 삼고 있다. 노동자 개인정보의 처리에 관한 사항은 근로조건에 해당하며, 따라서 노동조합이 근로자들을 대리하여 사용자와 이와 관련한 사항을 교섭할 수 있을 것이다.

3장

노동감시와 개인정보

감시설비를 통해서 수집된 노동자의 정보 역시 개인정보이며, 따라서 개인정보보호법의 적용을 받는다. 3장에서는 감시설비 설치 및 활용에 대한 대응의 맥락에서 중요하게 고려해야 할 개인정보보호법 규정에 대해 다룬다.

다만 일반적인 근로자 개인정보 수집·처리에 대해서는 본 가이드에서 상세하게 다루지는 않을 것이다. 이와 관련해서는 행정안전부와 고용노동부가 함께 발간한 「개인정보보호 가이드라인[인사·노무 편]」을 참조할 수 있다.

> **개인정보보호 가이드라인〔인사·노무 편〕**
>
> 「개인정보보호 가이드라인〔인사·노무 편〕」은 2012년에 초판이 발간되었고 2015년에 개정되었다. 이 가이드라인은 근로자 등 개인정보 처리 기본원칙을 소개하고 채용준비, 채용결정, 고용유지, 고용종료 등 인사·노무 업무 단계별 개인정보 처리요령을 설명하고 있다. 그러나 사업장 내 감시설비를 통한 개인정보 처리와 관련한 사항은 다루고 있지 않으며, 2016년 이후 개인정보보호법의 개정 사항도 반영하고 있지 않다. 특히 2020년 개인정보보호법 개정으로 통합 개인정보보호위원회가 설립되었고, 기존 행정안전부의 감독권한도 보호위원회로 이관되었다.
>
> 2017년 국가인권위원회는 「개인정보보호 가이드라인〔인사·노무 편〕」에 사업장 전자감시의 주요 유형별 개인정보 처리의 요건·절차 및 근로자의 권리 보호 등에 관한 사항을 구체적으로 정할 것을 권고하였지만, 고용노동부는 권고를 이행하지 않고 있다.
>
> ※「개인정보보호 가이드라인〔인사·노무 편〕」은 아래 홈페이지에서 다운받을 수 있다.
>
> : 개인정보보호위원회 홈페이지 > 정책·법령 > 지침·가이드라인

1. 개인정보의 개념

개인정보는 "살아 있는 개인에 관한 정보"로서 이름, 주민등록번호, 영상 등을 통해 개인을 알아볼 수 있는 정보뿐만 아니라, "해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보"도 포함한다. 예를 들어 차량번호 자체만으로는 누구의 차량인지 모를 수 있지만 경찰 등은 차량 소유주를 추적 가능하다. 보험회사나 사용자도 차량번호를 개인정보의 하나로 보유하고 있을 수 있다. 회사 내 컴퓨터에 고정 IP 주소가 부여되어 있다면 이 역시 개인정보라고 볼 수 있다. 이를 통해 회사 내에서는 로그 기록에 남은 특정 IP 주소로 접속한 사람이 누구인지 알 수 있기 때문이다. 감시설비를 통해 기록된 정보를 통해 특정 개인을 식별하거나 추적할 수 있다면 개인정보로 볼 수 있다.

아래는 「개인정보보호 가이드라인[인사·노무 편]」에서 설명하고 있는 개인정보의 예시이다.

개인정보의 예시

유형구분	개인정보항목
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련 정보	학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
그 밖의 수익정보	보험(건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격테스트 결과 직무태도, 취업일˙퇴직일 등 근속기간, 휴가˙휴직기록, 근무시간 기록 등
법적 정보	전과기록, 자동차 교통 위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(E-mail), 전화통화내용, 로그파일(Log file), 쿠키(Cookies)
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

2. 개인정보 처리원칙

개인정보보호법 제3조는 개인정보 보호 원칙을 규정하고 있다. 통상 원칙 규정이 다소 진부하고 뻔한, 그러나 실질적인 의미는 별로 없는 것처럼 보일 수 있으나, 그렇지 않다. 개인정보 보호 원칙에 비추어 구체적인 사안을 판단하면 문제점을 쉽게 인식할 수 있는 경우가 많다. 실제로 사업장에서 이 원칙을 벗어나 개인정보를 수집하는 경우가 많다.

제3조(개인정보 보호 원칙)

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

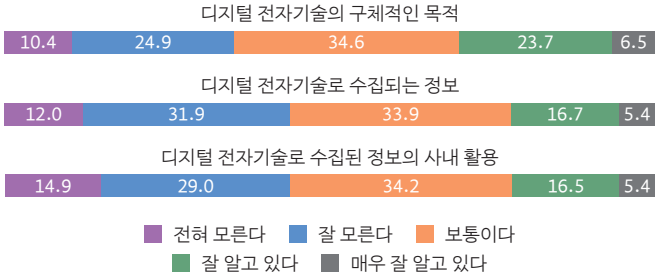
⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인

> 정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.
> ⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

예를 들어 모든 개인정보의 수집과 처리는 그 목적을 명확하게 할 필요가 있다(1항). 개인정보를 수집 목적 외로 활용하는 것은 제한되는데(3항), 목적이 명확하지 않으면 수집 목적 외의 활용인지 모호해지기 때문이다. 그런데 사업장 내에서 감시설비를 설치할 때, 그 설치 사실과 목적을 명확하게 고지하지 않는 경우가 많다. 만일 목적이 명확하다면, 예컨데 사업장에 설치된 CCTV가 시설 안전을 목적으로 한 것이라면, CCTV를 통해 수집된 정보를 징계 목적으로 활용하는 것은 목적 외 활용이 됨을 쉽게 알 수 있다. 또한 감시설비를 통해 어떠한 개인정보가 수집, 처리되는지 명확하게 고지하지 않는 것은 그 자체로 5항의 원칙을 위반한 것이다. 개인정보보호법은 이러한 원칙의 구현을 위한 구체적인 조항을 가지고 있으므로, 이처럼 원칙을 이해하고 있으면 사업장에서 위법한 개인정보 활용이나 감시설비 설치에 대해 문제점을 인식하기 용이할 것이다.

감시설비로 수집된 개인정보의 처리에 대한 인지 여부

2021년 실태조사에 따르면, 사업장 내에 설치된 감시설비의 설치 목적이 무엇인지, 이를 통해 어떠한 개인정보가 수집되는지, 수집된 개인정보가 회사 내에서 어떻게 활용되는지 근로자가 제대로 인지하지 못하는 경우가 30~40%에 달했다. 이는 감시설비 설치시 그 사실과 목적 등이 제대로 고지되지 않고 있기 때문이다. 이는 개인정보 처리원칙이 제대로 준수되고 있지 않음을 보여 준다.



3. 개인정보 수집·이용의 법적 근거

모든 개인정보의 수집·이용은 적법한 근거가 있어야 하는데, 개인정보보호법 제15조 1항에서 규정한 여섯 가지 중의 하나에 해당해야 한다.

> 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
> 1. 정보주체의 동의를 받은 경우
> 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피

한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

우선 사업장 내에서 노동자 개인정보를 수집하는 법적 근거로는 제2호와 제4호를 들 수 있다. 근로계약의 체결 및 이행을 위하여, 사용자는 제4호에 따라 노동자의 개인정보를 수집할 수 있다. 이름, 연락처, 계좌번호 등 업무상 소통이나 급여 지급에 필요한 정보들이 이에 해당한다. 동의를 받을 필요는 없지만 근로계약 체결 및 이행 과정에서 노동자들이 충분히 인지할 수 있다. 제2호는 법령에서 개인정보 수집을 규정하고 있는 경우이다. 근로기준법에 따라 근로자 명부, 임금대장 등을 작성하기 위해 근로자 개인정보를 수집하는 경우가 이에 해당한다.

노동감시와 관련하여 문제가 될 수 있는 것은 제1호와 제6호이다. 사용자는 감시설비를 도입할 때 노동자의 동의를 받을 수 있는데, 이때 다음 네 가지 사항을 정보주체(노동자)에게 알려야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

이때 동의의 진정성이 문제가 될 수 있다. 사업장 내에서 노동자는 사용자에 비해 취약한 지위에 있을 수밖에 없으므로, 사용자가 동의를 요구할 때 노동자가 이를 거부하는 것은 쉽지 않다. 해고되거나 인사상의 불이익을 받을 수 있기 때문이다. 동의는 정보주체가 자신의 권리를 행사하는 중요한 수단이지만, 그것이 의미가 있기 위해서는 진정한 동의여야 한다. 동의가 형식적인 절차에 그친다면 오히려 정보주체의 개인정보를 남용하는 빌미가 될 수 있다. 진정한 동의가 되기 위해서는 정보주체가 동의하는 내용에 대해 충분히 인지한 상태에서 아무런 외부적인 압력 없이 자유롭게 동의의 의사표현을 할 수 있어야 한다. 그런데 사업장 내에서, 더구나 노동자를 감시할 수 있는 설비를 설치하는 것에 대해 노동자가 한 동의가 진정한 동의가 될 수 있을지 의문이다. 노동자의 동의가 자유롭게 주어졌다는 것에 대한 입증 책임은 결국 개인정보처리자인 사용자에게 있다. 노동자들은 설사 형식적

인 동의를 했더라도 부당한 감시설비 도입과 개인정보 수집에 대해서는 언제든지 동의의 진정성을 문제 삼을 수 있다.

물론 사업장 내에서 동의의 진정성이 항상 문제가 되는 것은 아니다. 노동자의 안전을 위한 설비의 도입이나 사원 복지를 위한 가족 개인정보의 수집과 같이 노동자에게 이익이 되는 경우, 또는 거부해도 별다른 불이익을 당할 염려가 없는 경우에는 동의의 진정성이 인정될 수 있다. 이는 구체적인 맥락에 따라 다르며, 결국 사용자가 동의의 진정성을 입증해야 한다.

사용자가 노동자에게 고지와 동의 없이 감시설비를 도입하는 경우도 있다. 이때 사용자는 제15조 제1항 제6호, 즉 "개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우"를 근거로 들 수 있다. 시설 보호나 영업비밀 보호 등 사용자의 "정당한 이익"을 위해 감시설비를 도입하고 개인정보를 수집할 수 있다는 얘기다. 그러나 사용자의 정당한 이익을 명분으로 모든 형태의 개인정보 수집이 정당화될 수 있는 것은 아니다. 제6호에 규정되어 있는 바와 같이 사용자의 정당한 이익이 노동자(정보주체)의 권리보다 "명백하게 우선"하는 경우여야 하며, 이를 위해 감시설비를 통한 개인정보 수집이 사용자의 "정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 않"아야 한다. 예를 들어 시설 보호를 목적으로 CCTV를 설치한다면, CCTV의 촬영 범위는 보호하고자 하는 시설에 한정되어야 하며, 불필요하게 노동자의 활동까지 모니터링할 수 있다면 이는 합리적인 범위라고 보기 힘들다.

물론 사용자의 정당한 이익이 정보주체로서 노동자의 권리보다 우선하는지 아닌지, 수집되는 개인정보가 합리적인 범위인지 아닌지는 명확하지 않으며 관점에 따라 달라질 수 있다. 이 때문에 정부(개인정보보호위원회와 고용노동부)는 감시설비의 도입과 노동자 개인정보 수집의 맥락에서 제15조 제1항 제6호가 구체적으로 어떻게 해석될 수 있는지에 대한 지침을 제공할 필요가 있다. 나아가 근로기준법 등 법 개정을 통해 감시설비 도입시 업무 관련성과 비례성의 원칙을 명문화할 필요가 있다.

사용자가 정당한 이익 조항에 근거하여 감시설비를 동의 없이 도입했을 경우, 노동자 혹은 노동조합은 이것이 노동자의 권리를 과도하게 침해하지 않는지, 합리적인 범위에서 개인정보를 수집하는지 문제제기할 필요가 있다. 설사 감시설비가 도입되더라도 그 활용 범위와 조건은 다양할 수 있기 때문이다. 예를 들어 작업 현장에 CCTV를 도입할 것인가 여부도 중요하지만, 설사 CCTV를 도입하더라도 촬영의 범위는 어떻게 할 것인지, 카메라의 성능은 어느 정도가 적절할지, 영상은 얼마나 오래 보관할지, 촬영된 영상을 누가 어떤 목적으로 열람할 수 있도록 할지 등에 따라 노동자에게 미치는 영향이 달라질 수 있다. 4장에서 노동감시의 유형별로 노동자 권리에 미치는 부정적 영향을 최소화하기 위한 고려 사항을

자세히 설명한다.

> **사업장 개인정보 처리에 대한 유럽연합의 해석**
>
> 유럽연합의 개인정보보호법인 GDPR은 '동의'consent에 대한 정의 규정을 두고 있는데, 이에 따르면 "동의는 (…) 정보주체가 개인정보의 처리에 대해 자유롭게 제공하여야 하는데, 구체적으로, 고지된 명확한 합의를 나타내주는 적극적인 행위any freely given, specific, informed and unambiguous indication of the data subject's wishes로써 제공되어야 한다"고 규정하고 있다. 유럽연합 회원국의 개인정보 감독기구 대표로 구성되고 개인정보 보호규정 해석의 지침을 제공하는 WP29는 2017년 발간한 의견서[4]에서 노사관계의 성격을 고려할 때 사업장 내에서 대부분의 개인정보 처리는 근로자의 동의를 적법 근거로 삼을 수는 없다고 보고 있다. 노동자들이 자유롭게 동의할 수 있는 위치가 아니기 때문이다.
> 또한 사용자가 정당한 이익legitimate interest을 적법 근거로 삼을 경우 개인정보 처리가 처리 목적에 비례적이어야 하고, 가장 덜 침해적인 방식으로 이루어져야 하고, 특정한 위험만을 대상으로 해야 한다. 사용자의 정당한 이익과 근로자의 기본권과 자유 사이의 균형을 위해서는 '완화 조치'mitigating measures가 반드시 취해질 필요가 있는데, 이는 (감시의 형태에 따라) 근로자 프라이버시권을 침해하지 않을 수 있도록 모니터링을 제한하는 것을 포함한다.
> 국내 개인정보보호법은 "개인정보처리자의 정당한 이익"이 "**명백하게** 정보주체의 권리보다 우선하는 경우"로 제한하고 있어 적어도 형식적으로는 유럽연합보다 정보주체의 권리를 강하게 보호하고 있다.

개인정보 수집이 동의, 법령, 계약, 사용자의 정당한 이익 등 어떠한 근거에 따른 것이든 상관없이 그 목적에 필요한 최소한의 개인정보만을 수집해야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자(즉 사용자)가 부담한다(개인정보보호법 제16조 제1항).

앞서 살펴본 바와 같이 노동자의 취약한 지위를 고려할 때, 개별 노동자의 동의는 진정한 동의가 되기 힘들다. 사용자가 정당한 이익을 근거로 감시설비를 도입할 경우에도, 노동자의 권리 침해를 최소화하는 방식으로 도입될 필요가 있는데 이를 전적으로 사용자의 결정에만 의존하는 것은 한계가 있다. 따라서 감시설비의 도입이나 개인정보 처리와 관련하여 사업장 내에서는 노동조합 혹은 노동자 대표와 협의하도록 할 필요가 있다. 근로자 참여법에서 노사협의회의 협의사항 중 하나로 "사업장 내 근로자 감시설비의 설치"를 두고 있는 이유도 이 때문이지만, 벌칙 조항이 없어 사실상 유명무실한 상황일 뿐 아니라 세부적인 규정도 두지 않고 있다. 따라서 근로기준법을 개정하여 감시설비 도입시 노동조합(혹은 노동자 대표)과의 협의를 의무화하고 고용노동부가 이에 대해 감독할 수 있도록 규정할 필요가 있다.

4. 민감정보 및 고유식별정보

개인정보 중에서도 건강정보와 같이 사생활을 현저하게 침해할 우려가 있는 개인정보는 '민감정보'로서 특별한 보호를 필요로 한다. 현재 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄

경력자료에 해당하는 정보, 생체인식정보, 인종이나 민족에 관한 정보 등이 민감정보로 규정되어 있다.

> **제23조(민감정보의 처리 제한)** ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
> 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
> 2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우
>
> **시행령**
>
> **제18조(민감정보의 범위)** 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016. 9. 29., 2020. 8. 4.>
> 1. 유전자검사 등의 결과로 얻어진 유전정보
> 2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
> 3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
> 4. 인종이나 민족에 관한 정보

민감정보의 수집은 다른 개인정보와 별도의 동의를 받거나 법령에서 허용한 경우로 제한되는데 이는 사용자가 노동자의 민감정보를 수집할 때에도 마찬가지다. 즉 사용자가 노동자의 노동조합 가입 여부에 대한 정보를 수집하거나 질병정보를 수집하고자 할 경우, 해당 정보의 수집을 허용하는 법령이 있거나 혹은 노동자의 별도의 동의를 받아야 한다. 그런데 앞서 설명한 바와 같이 동의가 진정한 것으로 인정받기 위해서는 수집되는 민감정보가 업무와 필수적으로 관련된 매우 제한적인 범위로 한정되어야 할 것이다.

감시설비를 통해 민감정보가 수집될 수도 있다. 대표적인 사례가 지문, 홍채, 정맥, 얼굴 등 생체인식을 활용한 출입통제장치이다. 생체인식정보를 통한 스마트폰 잠금해제를 통해 생체인식정보 활용에 대한 거부감이 줄어들고 있지만, 생체인식정보는 개인에게 치명적인 악영향을 미칠 수 있는 민감한 개인정보다. 생체인식기술을 활용한 감시설비에 대한 대응 방안은 4장에서 다룰 것이다.

고유식별정보도 민감정보와 마찬가지로 엄격하게 보호된다. 이 역시 법령에서 구체적으로 처리를 요구하거나 정보주체로부터 별도의 동의를 받은 경우에만 처리할 수 있다. 이러한 고유식별정보에는 여권번호, 운전면허번호, 외국인등록번호가 포함된다. 그러나 주민등록번호의 경우에는 법령에서 허용한 경우에만 수집할 수 있다. 즉 단지 노동자의 동의를 받았다고 수집할 수 있는 것이 아니다.

5. CCTV 등 영상정보처리기기

가장 보편적으로 활용되고 있는 감시설비 중 하나가 CCTV이다. 개인정보보호법 제25조는 CCTV와 같은 영상정보처리기기에 대한 특별한 규정을 두고 있다. 일반적인 개인정보 수집과 다르게 CCTV를 통한 개인정보 수집은 불특정 다수를 대상으로 할 가능성이 크기 때문에 전통적인 동의 방식에 기반해서 개인정보를 수집하기 힘들기 때문이다.

주의할 점은 개인정보보호법 제25조는 '공개된 장소'에 설치된 CCTV에만 적용된다는 점이다. 사무실 안과 같이 특정 직원들만 출입하는 장소의 경우에는 제15조 제1항이 적용되므로, 직원들의 동의를 받거나 사용자의 정당한 이익에 근거하여 설치해야 한다. 공개된 장소가 단지 거리나 공원만을 의미하는 것은 아니다. 관공서의 민원실, 기업 건물의 로비와 같이 불특정 다수가 출입하는 공간은 '공개된 장소'로서 제25조의 적용을 받는다. 불특정 다수의 승객이 탑승하는 버스나 택시에 설치된 CCTV 역시 제25조의 적용을 받는다. 제25조 2항에서 규정하고 있는 바와 같이 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소에는 누구든지 CCTV를 설치·운영해서는 안 된다.

제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자 성명 및 연락처
4. 그 밖에 대통령령으로 정하는 사항

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는

아니 되며, 녹음기능은 사용할 수 없다.

공개된 장소에 설치된 CCTV가 노동감시 목적으로 이용될 가능성을 배제할 수 없다. 그러나 제25조는 공개된 장소에 설치된 CCTV의 설치 목적을 몇 가지로 제한하고 있다. 즉 법령에서 구체적으로 허용하고 있는 경우, 범죄의 예방 및 수사, 시설안전 및 화재 예방, 교통단속, 교통정보의 수집·분석 및 제공을 위하여 필요한 경우 등이다. 따라서 공개된 장소에 설치된 CCTV를 노동감시 목적으로 활용하는 것은 목적 외 이용으로서 불법이 된다.

또한 제25조 4항에서 규정하고 있는 바와 같이, 공개된 장소에 CCTV를 설치할 때에는 설치 목적 및 장소, 촬영 범위 및 시간, 관리책임자 성명 및 연락처 등을 포함한 안내판을 설치해야 한다. CCTV를 설치 목적과 다른 목적으로 임의로 조작하거나 다른 곳을 비춰서는 안 된다. 녹음 기능을 사용하지 못한다는 점도 주의할 필요가 있다.

앞서 CCTV라고 표현했지만, 제25조의 영상정보처리기기에는 CCTV 뿐만 아니라 유무선 인터넷을 통해 수집·저장할 수 있는 네트워크 카메라도 포함된다. 그러나 네트워크 카메라로 촬영된 영상을 임의의 이용자가 인터넷을 통해 접근할 수 있도록 해서는 안 된다. 네트워크 카메라 역시 설치된 목적 범위 내에서 운영되어야 한다.

회사 내의 공개되지 않은 장소에 설치된 CCTV의 경우에는 제25조가 아니라 일반적인 개인정보와 마찬가지로 제15조 제1항이 적용된다. 즉 정보주체의 동의 혹은 사용자의 정당한 이익에 근거하여 설치될 것이다. 앞서 (3장 3절에서) 설명한 바와 같이, 정보주체의 동의에 기반할 경우에는 그것이 진정한 동의인지, 정당한 이익에 기반할 경우에는 사용자의 정당한 이익이 노동자의 권리보다 명백하게 우선하는지, 그리고 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 범위 내에서 운영되는지 따져볼 필요가 있다. 이러한 판단은 CCTV의 성능, 촬영 범위, 안전조치 등에 따라 달라질 수 있다. 이에 대해서는 4장에서 다시 설명하기로 한다.

만일 CCTV에 얼굴인식 기능이 향후 도입된다면 생체인식정보는 민감정보이므로 제23조가 적용된다. 즉 (앞서 4절에서 설명한 바와 같이) 정보주체의 별도의 동의가 있는 경우, 혹은 법령에서 요구하거나 허용한 경우에만 민감정보인 생체인식정보를 수집할 수 있다.

6. 개인정보 처리방침의 수립

회사 홈페이지는 보통 화면 하단에 해당 기업의 개인정보 정책을 보여주는 '개인정보 처리방침'에 접근할 수 있는 링크를 제공한다. 대다수는 소비자들의 어떠한 개인정보를 어떤 목적으로 처리하는지, 어떻게 관리하는지에 대한 내용을 담

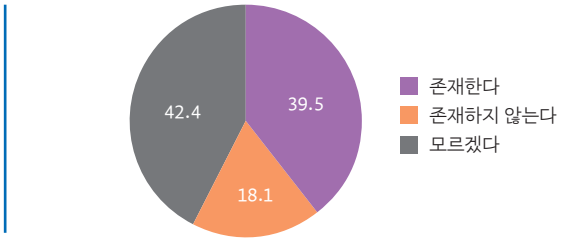
고 있다. 개인정보보호법 제30조는 개인정보처리자로 하여금 개인정보처리방침을 수립하고 공개하도록 하고 있다.

> 제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.
> 1. 개인정보의 처리 목적
> 2. 개인정보의 처리 및 보유 기간
> 3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
> 3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
> 4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
> 5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
> 6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
> 7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
> 8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항
> ② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

그런데 개인정보보호법의 규율 대상은 소비자, 국민의 개인정보뿐만 아니라 노동자의 개인정보 역시 포함한다. 따라서 노동자 개인정보의 처리자인 사용자는 노동자 개인정보를 어떻게 처리하는지를 담은 개인정보 처리방침을 수립하고 이를 공개해야 한다. 물론 이 경우 내부 게시판 등을 통해 공개해도 되지만, 입사 지원자는 이에 접근할 수 없으므로 개별적으로 제공할 필요가 있다.

노동자로부터 직접 수집하는 개인정보뿐만 아니라 노동자의 업무 과정에서 생성되는 정보, 감시설비를 통해 생성되는 정보 역시 개인정보이다. 예를 들어 CCTV로 촬영된 영상, 업무용 단말기를 통해 수집된 노동자의 위치정보, 인터넷 모니터링을 통해 수집한 노동자의 인터넷 접속기록 등 역시 해당 노동자의 개인정보다. 따라서 이 역시 개인정보 처리방침에 포함되어야 한다. 노동자들은 사내에서 수집되는 노동자의 개인정보에 대해 개인정보 처리방침이 모두 포괄하고 있는지 확인할 필요가 있다.

> **과반수 사업장, 근로자 개인정보 처리방침이 존재하는지 미지수**
> 2021년 실태조사에 따르면, 과반 이상의 회사에서 근로자 개인정보 처리방침이 없거나 당사자들이 존재 여부를 알지 못하는 것으로 드러났다. 근로자 개인정보 처리방침이 존재하는지 여부에 대한 답변으로 '모르겠다'가 499명(42.4%)로 가장 많았으며, '존재한다' 465명(39.5%), '존재하지 않는다' 213명(18.1%)으로 나타났다.
> 이를 보면 과반수의 직장에 근로자 개인정보 처리방침이 없을 것으로 추측할 수 있으며, 소비자 개인정보에 비해 노동자 개인정보 보호에 대한 관심은 극히 미약하다는 점을 알 수 있다.



7. 개인정보 권리 침해에 대한 대응

노동자의 개인정보에 대해서도 개인정보보호법이 적용되며, 따라서 개인정보보호법을 위반한 노동자 개인정보의 처리는 개인정보보호법에 따라 처벌된다. 예를 들어 정보주체(노동자)의 동의를 받지 않고 개인정보를 제3자에게 제공하는 경우, 또는 수집된 개인정보를 수집 목적 외로 이용하거나 제3자에게 제공하는 경우, 개인정보처리자(사용자)는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처하게 된다. 감시설비를 통해서 수집된 개인정보를 목적 외로 이용하거나 제3자에게 제공한 경우 역시 마찬가지다. 사용자가 형사처벌 조항을 위반한 경우 수사기관에 고소하거나 고발할 수 있다.

동의를 받지 않고 개인정보를 수집한 경우, 제25조를 위반하여 CCTV를 설치한 경우, 보유기간이 경과했음에도 개인정보를 파기하지 않은 경우, 열람권 등 정보주체의 권리를 보장하지 않은 경우 등은 과태료 대상이 된다. 이 경우 개인정보보호위원회에 이 사실을 신고하여 과태료 부과나 시정명령 등의 조치를 요구할 수 있다.

개인정보에 관한 권리를 침해받은 경우 정보주체는 개인정보침해 신고센터에 이를 신고할 수 있다. 현재 한국인터넷진흥원이 운영하는 개인정보침해 신고센터 홈페이지에서 신고 및 상담 신청이 가능하다.

개인정보 권리 침해자를 상대로 손해배상을 청구하는 등 민사적인 대응도 가능하다. 그러나 침해의 정도가 심하지 않은 경우, 대부분의 사람들에게 소송을 제기하는 것은 부담스러울 수 있다. 이 경우 개인정보 분쟁조정위원회에 분쟁조정을 신청할 수 있다. 개인정보 분쟁조정위원회는 개인정보 침해와 관련한 분쟁을 소송보다 신속하게 해결하는 역할을 한다. 다만 한쪽 당사자가 분쟁조정에 응하지 않을 경우에는 조정이 이루어지지 않는다. 분쟁조정 역시 홈페이지를 통해 온라인으로, 혹은 우편을 통해서도 신청할 수 있다.

> 개인정보보호위원회 : https://www.pipc.go.kr
> 한국인터넷진흥원 개인정보침해 신고센터 : https://privacy.kisa.or.kr
> 개인정보 분쟁조정위원회 : https://www.kopico.go.kr

개인정보 침해 문제이기는 하지만 노사관계 내에서 발생한 문제이니 고용노동부나 노동위원회에서 침해를 구제할 수 있으면 좋을 것이다. 그러나 노동감시가 직장 내 괴롭힘이나 부당노동행위와 연결되지 않는 이상(물론 노동감시는 개

인정보 침해 문제로 그치지 않고 종종 직장 내 괴롭힘이나 부당 노동행위로 이어진다), 감시설비의 도입이나 개인정보 침해 문제에 대해 고용노동부가 개입할 법적 권한이 모호하다. 이 문제를 해결하기 위해서는 근로기준법에 사업장 내에서 감시설비의 설치 및 개인정보 수집을 근로조건의 하나로 규정하고 감시설비 도입 요건에 대한 상세한 규정을 둘 필요가 있다.

4장

감시설비 도입에 대한 대응 방안

1. 공통 대응 방안

본 절에서는 감시설비의 유형별 대응 방안에 앞서서 공통적인 대응 방안을 설명한다. 아래에 설명하는 내용은 감시설비의 유형과 상관없이 적용할 수 있는 것들이다.

① 우선 노동자의 인격권, 개인정보자기결정권, 사생활의 권리 등 기본권은 사업장 내에서도, 그리고 근무 시간 내에서도 침해될 수 없는 기본권임을 인식할 필요가 있다. 물론 사용자가 회사 재산에 대한 시설관리권이나 노동자에 대한 일정한 노무지휘권을 가지고 있는 것이 사실이지만, 그것이 근무 시간 중에는 사생활이 존재할 수 없음을 의미하는 것은 아니다. 현실적으로 업무와 사생활을 완벽하게 분리하는 것은 불가능하며, 사업장 내에서도 노동자의 기본권이 본질적으로 침해되어서는 안 된다. 따라서 모든 감시설비는 노동자의 기본권을 침해하는 것이고, 감시설비의 도입은 원칙적으로 금지되어야 한다.

> 유럽인권재판소 역시 근무시간 중 회사 인터넷을 사적 용도로 사용한 것에 대해 사용자가 사칙 위반으로 근로자를 해고한 사안에서, 회사 내 근로자의 사적인 생활을 '0'으로 줄이는 것은 불가능하다고 지적하며 근로자의 사생활에 대한 권리가 부당하게 침해되었다고 결정하였다(ECtHR, Bărbulescu v. Romania [GC], No. 61496/08, 5 September 2017, para 121).[5]

② 감시설비는 그 설치 목적이 정당하고 노동자의 기본권 제한을 최소화할 수 있는 한도에서 예외적으로 도입될 수 있고, 이 경우 정당하고 적법한 절차를 거쳐야 한다. 어떠한 감시설비도 비밀리에 도입돼서는 안 되며, 고지나 동의 없이 개인정보를 수집하는 것은 개인정보보호법 위반이다. 비밀리에 전송 중인 이메일이나 SNS 대화 내용을 모니터링하는 것은 통신비밀보호법 위반이 될 수 있다. 은밀한 감시 및 개인정보 수집은 기본권 침해일 뿐만 아니라 현행법 위반이므로, 형사 고발을 포함하여 강력한 문제제기가 필요하다.

③ 어떠한 감시설비를 도입했는지 포괄적으로 고지하는 것으로는 충분하지 않다. ▲ 해당 감시설비의 설치목적 ▲ 감시설비의 구체적인 사양과 기능 ▲ 감시설비의 운영 범위, 기간, 방법 ▲ 감시설비를 통해 수집되는 개인정보의 종류, 보유 및 이용기간 등에 대한 상세한 정보를 투명하게 공개할 것을 사용자에게 요구해야 한다.

④ 특히 감시설비의 설치 목적, 감시설비를 통해 수집되는 개인정보의 처리 목적을 명확히 할 필요가 있다. 목적이 명확해야 해당 시스템이 목적 달성을 위한 최적의 수단인지, 덜 침해적인 대체 수단은 없는지, 목적 달성과 무관하게 작동하는 기능은 없는지 등을 판단할 수 있다. 감시설비, 그리고 감시설비를 통해 수집되는 개인정보는 애초 설정된 목적 외로 활용되어서는 안 된다. 이는 개인정보보호법 위반이 될 수 있다.

⑤ 노동자 개인정보 처리방침이 존재하는지 확인해야 한다. 대부분의 기업들이 소비자의 개인정보 처리방침을 홈페이지를 통해 공개하고 있지만, 노동자 개인정보 처리방침은 두고 있지 않은 경우가 많다. 노동자 개인정보 처리방침을 두지 않는 것도 개인정보보호법 위반이며, 1천만 원 이하의 과태료 부과 대상이 된다. 감시설비를 통해 수집되는 개인정보에 대해서도 ▲ 처리 목적 ▲ 처리 및 보유기간 ▲ 제3자 제공 및 위탁에 관한 사항 ▲ 정보주체의 권리 ▲ 개인정보보호책임자의 성명과 연락처 ▲ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항 등이 개인정보 처리방침에 포함되어야 하며 그 내용이 변경될 경우에도 마찬가지이다.

⑥ 감시설비의 도입을 정당화할 수 있는 법적인 근거가 무엇인지 확인할 필요가 있다. (2021년 현재) 근로기준법에는 감시설비와 관련된 규정이 없다. 근로자 참여법에서는 30인 이상 근로자를 사용하는 사업장에 노사협의회를 설치하여야 한다고 정하고 있고, 노사협의회의 협의 사항으로 '사업

장 내 근로자 감시설비의 설치'를 정하고 있다. 따라서 감시설비 도입에 대해 노사협의회에서 협의했다면, 근로자 참여법에 따른 것으로 볼 수 있다.

⑦ 감시설비를 통한 개인정보의 수집과 관련해서는 개인정보보호법 제15조 제1항 어디에 해당하는지 확인해야 한다. 즉 정보주체(노동자)의 동의를 받은 것인지(1호), 아니면 법률에서 감시설비를 설치할 수 있도록 허용하고 있는지(2호), 근로계약의 이행을 위한 것인지(4호), 혹은 개인정보처리자(사용자)의 정당한 이익 달성(6호)을 명분으로 설치하는 것인지 등을 확인한다. 어떤 경우든 최소한의 개인정보를 적법하고 정당하게 수집해야 하는 등 개인정보 보호 원칙을 준수해야 한다. 만일 감시설비 설치와 관련한 명확한 법적 근거가 없다면 불법적인 것이므로 철거를 요구해야 한다.

⑧ 근로자 참여법에 따른 협의와 개인정보보호법에 따른 정보주체의 동의가 어떠한 관계에 있는지(예를 들어, 근로자 참여법에 따라 노사협의회에서의 협의를 통해 감시설비를 도입했지만, 노동자는 동의하지 않는 경우 어떻게 할 것인지) 모호하지만, 개인정보보호위원회는 근로자 참여법에 따른 노사협의회에서의 협의가 우선하는 것으로 해석하고 있다. 만일 근로자 참여법에 따라 노사협의회에서 감시설비 도입과 관련한 협의한 바가 없었다면 개인정보보호법에 근거를 둘 수밖에 없다.

⑨ 사용자가 감시설비 설치에 대해 노동자의 동의를 요구할 경우, 그 동의가 진정으로 자유로운 동의가 되기 위해서는 노동자가 이를 거부할 수 있어야 한다(또한 언제든지 철회할 수 있어야 한다). 현실적으로 대부분의 경우 노동자가 동의를 거부하는 것은 쉽지 않을 것이다. 국내 여건에서 법원이 노동자의 의사를 반영하지 않은 형식적인 동의서가 진정한 '동의'가 아니라고 판단해 줄 것인지는 모호하다. 그러나 강압적이고 형식적인 동의를 통해 감시설비를 도입했다면, 설사 동의를 했더라도 그것이 진정한 동의가 아니었음에 대해 언제라도 문제제기할 필요가 있다. 또한 상당수의 사용자들은 포괄적 동의서를 징구하고 있는데 이는 처리 목적을 명확하게 해야 한다든가, 목적에 필요한 최소한의 정보만을 수집해야 한다는 등의 개인정보 보호원칙에 반한다. 원칙적으로 포괄 동의는 인정되지 않는다. 여기서 포괄적 동의란 다수의 목적에 대해 일괄해서 한 장의 문서로 동의를 받는다든가, 구체적이지 않은 목적에 대해 막연하게 동의받는 것을 의미한다.

⑩ 감시설비를 통해 민감정보가 수집될 경우, 반드시 노동자의 '별도의 동의'를 받아야 한다. 즉 동의 없이 민감정보를 수집하거나 다른 개인정보에 대한 동의에 통합하여 동의를 받는 것은 개인정보보호법 위반이다. 예를 들어 노동자의 건강정보, 노동조합·정당의 가입·탈퇴, 지문·홍채·정맥·얼굴 등 생체인식정보, 유전정보, 범죄경력자료에 해당하는 정보, 인종이나 민족에 관한 정보 등을 사용자가 수집하고자 할 경우 노동자의 별도 동의를 받아야 한다. 그러나 노사관계 내

에서 동의가 노동자의 자유로운 동의가 되기 힘들다는 점을 고려하면, 법령에 수집 근거가 있거나 민감정보 수집을 정당화할 수 있는 강력한 이유가 없는 한 적법한 민감정보 수집이 되기 힘들다. 노동자는 민감정보 수집을 요구받을 때 이러한 점을 고려하여 가능한 민감정보를 제공하지 않도록 해야 한다.

⑪ 법률에서 특정한 감시설비의 설치를 규정하거나 혹은 법령상 의무를 준수하기 위하여 불가피하게 감시설비를 도입할 수도 있다. 예를 들어, 어린이집 CCTV의 경우, 보육교사에 대한 노동감시가 될 수 있지만 CCTV의 설치를 의무화하였기 때문에 설치할 수밖에 없다. 혹은 개인정보보호법은 개인정보의 안전한 보호를 위한 조치의 하나로 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하도록 하고 있는데, 이 경우 개인정보 취급 업무를 담당하는 노동자의 활동이 자동으로 기록될 수 있다. 이처럼 법령에 따라 감시설비를 설치한 경우에도 법령에서 정하고 있는 안전조치를 제대로 취하도록 해야 하며, 수집된 개인정보가 설치 목적 외로 활용되지 않도록 해야 한다. 예를 들어 '아동학대 방지 등 영유아의 안전과 어린이집의 보안을 위하여' 설치된 어린이집 CCTV 영상자료를 보육교사의 근태관리 목적으로 활용해서는 안 된다.

⑫ 사용자가 노동자의 동의 혹은 법률적 근거 없이 감시설비를 도입하고, 개인정보보호법 제15조 제1항 제6호에 따른 '개인정보처리자의 정당한 이익'을 주장할 수도 있다. 예를 들면 시설 보호나 영업비밀 보호 등을 위해 필요하다는 것이다. 그러나 사용자의 정당한 이익이 있다고 감시설비 도입이 무조건 정당화되는 것은 아니다. 사용자의 정당한 이익이 정보주체인 노동자의 권리보다 "명백하게 우선"해야 하고, 감시설비를 통한 개인정보 수집이 사용자의 "정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 않"음을 사용자가 입증해야 한다. 반대로 노동자는 수집되는 개인정보가 해당 목적을 위해 필수적이지 않거나 다른 대체수단이 존재함을 주장할 수 있다. 혹은 감시설비 도입으로 인해 침해되는 노동자의 권리가 정당한 이익에 비해 지나치게 클 경우도 문제제기할 수 있다. 노동자의 동의도 받지 않고 침해되는 노동자의 권리에 비해 사용자의 정당한 이익이 크지 않다면, 감시설비 도입의 적법성을 부정할 수 있다.

⑬ 노동자 역시 정보주체이며 개인정보보호법이 보장하는 정보주체의 권리, 즉 자기정보에 대한 열람권, 정정·삭제권, 처리정지권 등을 보장받아야 한다. 사용자가 자신의 개인정보를 실제로 어떻게 보유하고 있는지 궁금하다면 개인정보 열람요구를 할 수 있다. 이때 단지 개인정보의 항목이 아니라, 보유하고 있는 개인정보 자체를 제공받을 수 있다. 그래야 잘못된 정보가 있을 경우 정정 요청을 할 수 있기 때문이다(기업들은 소비자의 개인정보 열람신청에 대해서도 항목만을 제공하는 경우가 많다) 만일 보유기간이 지난 개인정보

가 있다면 삭제 요청을 할 필요가 있다.

⑭ 감시설비 도입시 노동조합 혹은 노동자 대표와 협의할 것을 요구해야 한다. 노동관계법에서 감시설비 도입과 관련한 사항을 단체협상의 대상으로 구체적으로 규정하고 있는 것은 아니다. 그러나 감시설비의 도입은 근로조건에 관한 사항이라고 볼 수 있다. 근로자 참여법에서도 노사협의회의 협의 사항으로 규정하고 있다. 노사 간의 권력이 불균형한 특수성을 고려할 때 노동자 개인 차원에서 대응하는 것보다는 집단적인 대응이 필요하다. 특히 사용자의 정당한 이익과 노동자의 권리 사이의 균형을 고려할 때, 사용자 관점에서만 판단하는 것은 공정하지 못하기에 노동자의 집단적인 의사가 반영되기 위해서라도 노동조합과의 협의가 필요하다. 더불어 감시설비의 도입이 노동자 개인에게도 인권침해와 스트레스를 유발할 수 있지만, 노동조합의 설립이나 운영을 위축시킴으로써 노동자의 단결권, 단체행동권, 단체교섭권을 위협할 수 있기 때문에, 이러한 측면에서도 노동조합 차원에서 개입할 당위성이 존재한다.

또한 감시설비를 도입할 때 단지 도입 여부를 다투거나, 감시설비를 도입하게 되더라도 그 운영의 범위나 방법, 수집되는 개인정보의 종류 및 보관기간, 개인정보 보호를 위한 안전조치의 방법 등 구체적인 이행방법은 매우 다양할 수 있으므로, 노사 간의 협의를 통해 구체적인 방안을 도출해 내는 것이 합리적이다.

⑮ 감시설비 도입과 관련하여 노동조합 혹은 노동자 대표와 협의한다고 하더라도, 협의의 결과가 개별 노동자의 의사와 다를 수 있다. 이 경우 가능하다면 개별 노동자가 다른 선택을 할 수 있는 권리를 보장해야 한다. 예를 들어 노동조합과의 협의를 통해 출퇴근 확인 목적의 지문인식기를 도입하기로 결정했더라도, 지문인식을 원하지 않는 노동자에게는 대체 수단을 제공할 수 있을 것이다. 물론 CCTV처럼 개별적인 선택권을 부여하기 힘든 경우도 있지만, 가능할 경우 개별 노동자의 선택권을 존중해야 할 것이다.

⑯ 노동자의 권리를 심각하게 침해할 우려가 있거나 그 영향력을 판단하기 힘든, 인공지능과 같은 새로운 기술의 경우 개인정보 영향평가를 수행할 것을 요구해야 한다. 개인정보 영향평가는 개인정보 침해의 위험성이 큰 개인정보 처리와 관련하여 사전에 그 위험요인을 평가하고 위험성을 최소화하는 조치를 마련하도록 하기 위한 제도이다. 국내 개인정보보호법은 공공기관에 대해서는 영향평가를 의무화하고 있고, 민간의 개인정보처리자에게도 개인정보 침해가 우려되는 경우 영향평가를 하도록 권장하고 있다.

> **제33조(개인정보 영향평가)** ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 보호위원회가 지

> 정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.
> ⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

⑰ 노동자와 노동조합은 노동감시와 관련한 법과 제도 마련을 위한 투쟁에 적극 나서야 한다. 노동감시는 개별 노동자에게는 인권을 침해할 우려가 있고, 노동조합에게는 노동조합 활동을 위축시킬 수 있기 때문이다. 현행 법제를 통해서도 과도한 개인정보 수집과 감시설비 도입에 문제제기할 수 있지만, 보다 명확하게 감시설비 도입의 원칙과 노동조합과의 협의를 의무화할 필요가 있다. 또한 개인정보 감독기구인 개인정보보호위원회뿐만 아니라, 노동현장에서의 문제를 관할하는 고용노동부에 부당한 감시설비의 도입을 감독할 수 있는 권한을 명확하게 부여할 수 있도록 법률 개정을 요구해야 한다.

2. 컴퓨터 및 인터넷 이용 모니터링

1) 개요

요즘에는 어느 산업 분야든 컴퓨터와 인터넷을 사용하지 않는 것을 상상하기 힘들다. 따라서 노동자의 업무에 대한 관찰, 평가, 감시는 노동자의 컴퓨터 및 인터넷 이용에 대한 모니터링을 포함할 수밖에 없다. 과거 오프라인 작업 공간에서 사용자가 노동자를 감시하려면 많은 비용이 들었고 은밀하게 할 수 없었기 때문에 사용자의 감시활동은 제한적일 수밖에 없었다. 그러나 감시 프로그램을 통한 컴퓨터와 인터넷 이용에 대한 자동화된 감시는 아주 적은 비용으로 손쉽게, 대상 노동자가 알지 못하는 사이에 원격에서도 은밀히 이루어질 수 있다.

게다가 감시는 상상을 초월할 정도로 정밀하게 이루어질 수 있다. 컴퓨터와 인터넷 이용을 모니터링하는 통상의 감시 프로그램들은 다음과 같은 기능을 포함하고 있다.

- 컴퓨터를 통해 이루어지는 채팅이나 대화의 캡쳐
- 이메일, 웹브라우징 등 인터넷 사용 모니터링, 특정한 트래픽 저장
- 모든 키보드 입력의 기록(키로깅)
- 방문한 웹사이트의 추적 및 특정 사이트 차단
- 원격으로 컴퓨터 스크린샷 보기, 기록
- USB 등 외부 저장 매체에의 저장 탐지 및 차단
- 직원들의 생산성 수준 평가
- 직원들의 세부 활동 기록 및 광범위한 보고서 작성

최근에는 노동자의 컴퓨터를 감시할 수 있는 프로그램을 통틀어 보스웨어bossware라는 명칭으로 부르기도 한다. 2019년 말부터 전 세계적으로 확산된 코로나19로 인해 재택 근무

가 많아지면서 보스웨어 시장도 확대되고 있다. 게다가 기존에 보스웨어가 회사에서 제공하는 PC에만 설치되어 있었다면, 재택 근무에 따라 기업들은 개인의 PC에도 보스웨어를 설치할 것을 요구하고 있다. 보스웨어를 통해 재택 근무 중인 직원들의 모니터를 정기적으로 캡쳐하거나 키보드로 무엇을 타이핑하는지 들여다보는 식으로 노동자를 감시할 수 있다. 이러한 보스웨어의 감시에 대응하기 위해 '안티 보스웨어'가 등장하기도 했는데, 일정 시간 자리를 비운 것을 감추기 위해 키보드나 마우스 움직임을 자동으로 보내는 소프트웨어를 의미한다.

기업들이 컴퓨터나 인터넷을 모니터링하는 시스템을 도입하는 명분은 정보보안, 영업비밀 유출 방지, 근태 및 업무성과 관리 등 다양할 수 있다. 그러나 직원의 컴퓨터 및 인터넷 이용에 대한 모니터링은 과도한 사생활 침해와 노동통제를 야기할 수 있다. 이메일이나 SNS를 통해 사적인 내용이 전달될 수도 있으며, 어떠한 사이트에 접속하는지, 인터넷에서 어떠한 콘텐츠를 열람하는지 역시 개인의 민감한 취향이나 성향을 드러낼 수 있다. 또한 자신이 항상 모니터링되고 있다는 인식은 노동자를 위축시키고 정신적인 압박을 야기할 수 있다. 모니터링 시스템의 도입 목적이 정당하다고 할지라도 목적 달성에 필요한 범위에서, 프라이버시권 침해를 최소화하는 방식으로 도입될 필요가 있다.

한편 이러한 모바일 환경이 보편화되면서 모바일 앱을 통해 모바일 기기 및 인터넷 활용에 대한 모니터링이 이루어질 수 있다. 이에 대해서는 이 장의 5절에서 다룬다.

2) 동의 없이 전송 중인 통신 내용 접근은 불법 감청

당사자 동의 없이 전송 중에 있는 이메일, 메신저 등 인터넷 통신 내용을 들여다보는 것은 불법이다. 통신비밀보호법 제3조는 누구든지 적법한 근거 없이 전기통신을 감청하거나 타인 간의 비공개 대화를 녹음 또는 청취하는 것을 금지하고 있다. 여기서 감청이란 "당사자의 동의 없이" 통신의 내용을 지득하거나 전기통신을 방해하는 것을 의미한다. 따라서 사용자가 인터넷 모니터링 프로그램을 통해 노동자의 이메일이나 메신저 내용을 동의 없이 취득하는 것은 통신비밀보호법 위반에 해당한다. 사용자가 노동자의 통신 내용을 엿볼 수 있는 프로그램을 노동자의 동의 없이 설치할 경우, 이에 대해 고발할 수 있다.

그러나 컴퓨터와 인터넷 모니터링이 모두 통신비밀보호법 위반인 것은 아니다. 우선 감청은 "당사자의 동의 없이" 통신 내용을 지득하는 것을 의미한다. 따라서 사용자가 사전에 인터넷 모니터링에 대해 노동자의 동의를 받았다면, 통신비밀보호법 위반은 아닐 수 있다.

또한 통신비밀보호법은 "전송 중에 있는" 통신 내용에 적용된다. 따라서 이미 전송이 완료되어 서버나 PC에 저장되어 있는 이메일이나 메신저 대화 내용 등에 접근하는 경우에는

통신비밀보호법이 적용되지 않는다. 즉 같은 이메일이라고 할지라도 전송 과정 중에 가로챌 경우에는 통신비밀보호법이 적용되지만, 이미 수신 완료된 이메일에 접근할 때에는 통신비밀보호법이 적용되지 않는다. 하지만 정당한 권한이 없이 타인의 이메일을 해킹하여 열람하는 것은 정보통신망법 위반이 될 수 있다.

> **정보통신망법**
> 제49조(비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.

또한 적법한 근거 없이 다른 사람의 개인정보를 수집하거나 제3자에게 제공하는 것은 개인정보보호법 위반이 될 수 있다. 이는 사용자가 노동자의 이메일 계정에 정당한 권한 없이 접근하거나 노동자의 개인정보를 수집할 경우에도 마찬가지로 적용된다. 다만 회사가 정보보안이나 영업비밀 유출 방지 등 정당한 목적으로 설치한 프로그램을 통해 노동자의 이메일이나 개인정보에 접근하는 경우, 이를 정당한 권한 혹은 적법한 근거가 있는 것으로 볼 수 있을지 논란이 될 수 있다. 이에 대해서는 아래에서 다시 살펴본다.

3) 모니터링과 개인정보보호법의 적용

모니터링을 통해 수집되는 이메일이나 접속 내역 등도 특정 노동자와 연결되어 있을 경우 개인정보에 해당한다. 사용자가 인터넷 모니터링 프로그램을 통해 노동자의 개인정보를 수집할 경우에도 개인정보보호법이 적용된다. 아래 사례는 사용자가 고지나 동의 없이 개인정보를 수집, 열람한 것은 노동자의 개인정보자기결정권을 침해하는 것임을 확인하고 손해배상을 인정한 사건이다.

> **〔사례〕 MBC 트로이컷 프로그램을 이용한 노동조합 사찰 사건[6]**
> 2012년 MBC는 노조 파업 중 김재철 전 MBC 사장의 법인카드 사용내역서 유출 사건이 발생하자 'IT보안강화 방안'을 명분으로 트로이컷 TrojanCut 프로그램을 직원들이 사용하는 컴퓨터에 설치하도록 하였다. 이 프로그램은 기본적으로 '사용자 입력행위 `기반 기술'을 근거로 하여 컴퓨터에서 사용자가 직접 조작하여 정보나 파일 등을 외부(자료의 외부전송 또는 이동 저장장치에의 저장)로 내보는 것은 허용하고 사용자의 조작 없이 해커가 전산망에 침입하여 정보나 파일을 빼내려 하는 경우 이를 막는 역할을 하는 '해킹 방지 솔루션' 프로그램이다. 추가로 'DLPData Loss Prevention, 내부자료의 유출방지' 기능, 즉 컴퓨터 사용자가 웹메일 또는 메신저 등을 통하여 메일이나 자료를 주고받거나, 이동저장장치USB 등에 자료를 저장하는 경우 그 웹메일과 메신저의 대화내용 및 첨부 파일, 그리고 이동저장장치에 저장된 파일 등이 중앙관제서버에 저장되도록 하는 이른바 '로깅'logging 기능도 포함되어 있었다. MBC 구성원들이 사내에서 또는 가정에서 컴퓨터를 이용하여 'MBC 포털'(MBC 인트라넷)에 접속하는 순간 컴퓨터에 자동으로 설치되었다. 그러나 일반적인 탐색기 설정으로는 프로그램의 설치 폴더를 확인할 수 없고, '숨겨진 프로세스'로 작동하여 작업관리창에서 위 프로그램이 실행되는지를 확인할 수 없었다.
> MBC는 프로그램 설치 과정에서 프로그램의 도입 및 설치 경위, 자료나

파일의 사내 서버 저장 등 위 프로그램의 각종 특성, 설치방법 등에 관한 내용을 소속 직원들에게 사전에 알리지 아니하였고, 직원으로부터 정보보호 서약서나 동의서를 받지도 않았다. MBC 간부는 이 프로그램을 이용하여 전·현직 노동조합 집행부의 파일을 열람하였으며, 이에 노동조합과 일부 조합원은 회사와 행위자를 상대로 조합원의 쟁의행위와 일상적인 조합 활동을 침해하였고, 피해를 입은 조합원들이 경험한 정신적 고통에 대한 손해배상 청구하였다.

이 사건의 항소심 법원은 트로이컷 관제 서버에 저장되어 정보가 열람된 사실을 인정할 수 있는 원고들에 대해서는 "트로이컷 관제 서버에 저장된 정보들은 개인정보자기결정권의 보호 대상이 되는 개인정보에 해당하므로, 이를 관제 서버에 일괄하여 저장함으로써 수집·보관한 행위 및 나아가 이를 열람까지 한 행위는 정보주체에 해당하는 원고 6인의 개인정보자기결정권을 침해하는 것"이라고 판단하고 각 50만 원의 손해배상을 인정하였다. 나아가 이러한 행위는 노동조합의 집단적 단결권 및 단체행동권을 침해하는 것으로 보아 원고 노동조합과 소속 본부에 각 1500만 원의 손해배상을 인정하였다. 다만 법원은 원고들의 개인정보나 자료들이 트로이컷 관제 서버에 저장 또는 열람되었다는 사실을 인정할 만한 증거가 없는 나머지 원고 4인에 대한 청구는 기각하였다. 대법원은 피고들의 상고를 기각하였다.

개인정보보호위원회는 "회사가 업무효율성 및 영업비밀 보호 등을 이유로 직원의 업무처리 내역 및 인터넷 접속 내역 등을 모니터링하는 시스템을 설치하는 것은 정보주체의 권리보다 명백히 우선한다고 보기 어려우므로, 노사 협의에 따라 처리하거나 직원에 대한 고지 또는 동의 절차를 거치는 것이 바람직하다"고 해석하고 있다.[7] 다만 고지 또는 동의 절차를 거치는 것만으로 모든 모니터링 시스템이 정당하다는 의미는 아니다.

4) 컴퓨터 및 인터넷 모니터링에 대한 노동자의 대응 방안

① 현대 사회에서 어떤 직종에서 일하든 컴퓨터 및 인터넷의 사용은 필수에 가깝다. 컴퓨터와 인터넷의 사용이라고 표현했지만, 이를 통해서 수행하는 작업은 무수히 다양하다. 워드나 엑셀과 같은 특정한 애플리케이션을 실행하고, 뉴스를 보거나 자료를 검색하는 등 다양한 목적으로 인터넷을 탐색하며, 이메일과 메신저를 통해 업무적이거나 혹은 사적인 소통을 하게 된다. 이를 모니터링하는 것은 개인의 하루 일상을 투명하게 들여다보는 빅브라더나 다름없다. 이에 따른 노동자 프라이버시 침해는 매우 심각하며, 컴퓨터와 인터넷 사용에 대한 전면적인 모니터링은 어떠한 명분으로도 정당화되기 힘들다.

② 비밀리에 컴퓨터 및 인터넷을 모니터링하는 것은 불법이다. 고지나 동의 없이 비밀리에 개인정보를 수집하는 것은 개인정보보호법 위반이며, 비밀리에 전송 중인 이메일이나 SNS 대화 내용을 모니터링하는 것은 통신비밀보호법 위반도 될 수 있다.

③ 상업적으로 판매되고 있는 모니터링 프로그램들은 다양한 기능들을 제공하고 있다. 각 기능마다 수행하고자 하는 목적과 노동자에게 미치는 영향이 다르다. 따라서 사업장에 설치되는 프로그램이 구체적으로 어떠한 기능을 포함하고

있는지, 사용자가 활용하고자 하는 기능은 무엇인지, 해당 프로그램을 통해 어떠한 개인정보가 수집되고, 어떻게 처리되며, 얼마나 오래동안 보관되는지 등을 알 필요가 있다. 사용자에게 이에 대한 상세한 정보를 투명하게 공개하도록 요구해야 한다. 이해하기 어려운 전문적인 내용의 경우 가능한 쉽게 설명할 것을 요구할 수 있다.

④ 모니터링의 특정 기능은 지나치게 프라이버시 침해적이다. 키보드 입력을 기록하는 것이나 노동자가 일하는 모습을 정기적으로 촬영하여 서버에 전송하는 기능 등은 정당화하기 어렵다. 노동자와 노동조합은 모니터링 프로그램에서 제공하는 여러 기능들이 설치 목적 달성과 관련된 합리적인 범위 내에 있는지, 노동자의 권리를 과도하게 침해하지 않는지 따져 보아야 한다. 설사 특정 기능이 설치 목적과 관련되어 있을지라도 노동자의 권리를 과도하게 침해한다면, 덜 침해적인 대체적인 수단이 없는지, 혹은 권리 침해를 최소화하는 방향으로 제한적으로 적용할 수 없는지 검토할 필요가 있다. 예를 들어 영업비밀 유출 방지라는 목적이 정당하다고 할지라도 이메일을 관리자가 언제든지 열람하도록 하는 것은 노동자의 권리를 과도하게 침해할 수 있다.

⑤ 수집되는 개인정보가 합리적인 범위 내인지, 정보주체의 권리를 과도하게 침해하지 않는지는 구체적인 맥락에 따라 다를 수 있다. 예를 들어 모니터링 프로그램의 목적이 근무시간 내에 업무와 관계없는 사이트에 접속하는 것을 방지

하는 것이라면, 굳이 노동자의 인터넷 접속 기록 일체를 수집할 필요는 없으며 특정 사이트에의 접속을 차단하는 것으로 충분할 것이다. 물론 여기서 특정 사이트에 대한 차단이 정당한가는 별개의 문제이며, 사전에 노동자 대표 혹은 노동조합과의 협의를 통해 차단 목록이 합의될 필요가 있다.

⑥ 이메일이나 SNS 모니터링의 경우 회사에서 부여한 업무용 계정인지, 혹은 개인 계정인지에 따라 권리 침해의 정도가 다르다. 개인 계정을 통해서는 업무 목적의 통신뿐만 아니라 사적인 소통도 많이 이루어질 것이므로, 모니터링 프로그램을 통해서 개인 계정을 모니터링하는 것은 정당화되기 힘들다. 회사에서 부여한 업무용 계정일 경우에도 이를 통해 사적인 소통이 이루어질 수 있으므로 항상적인 모니터링을 허용해서는 안 된다. 그보다는 의심스러운 트래픽이 발생했을 경우에만 특정 조치를 취하도록 요구할 수 있다. 예를 들어 업무용 계정일지라도 시스템 관리자나 사용자가 언제든지 개인 계정에 접근해서 열람할 수 있도록 허용되는 것이 아니라, 보안 위협이 발생했을 경우 조치에 필요한 최소한의 한도 내에서 시스템 관리자 등 정당한 권한을 가진 담당자만 접근하도록 한다든가, 기밀 유출의 의심이 있을 경우 해당 이메일 발송자에게 우선 이에 대한 고지를 하고 동의하에 열람하는 방안 등이 있을 수 있다.

⑦ BYOD Bring Your Own Device는 노동자가 노트북이나 스마트폰 등 자신의 기기를 직접 회사에 가지고 와서 업무에 활

용하는 것을 말한다. 코로나19 이전부터 이러한 경향이 있었는데, 특히 재택근무가 확대되면서 강화되고 있다. 그런데 BYOD는 사적인 영역과 업무 영역의 구분을 더욱 모호하게 만들 수 있다. 따라서 컴퓨터 및 네트워크 모니터링으로 인한 프라이버시 침해를 최소화하기 위해서는 회사에 업무용 기기를 제공할 것을 요구해야 한다. 만일 자신의 기기를 사용해야 한다면 모니터링 프로그램이 사적인 통신을 침해하지 않도록 요구해야 한다.

⑧ 재택근무하는 노동자를 모니터링하기 위한 프로그램 설치도 정당한 목적 달성을 위해 필요한 최소한의 경우로 제한되어야 하겠지만, 특히 노동자가 개인 PC를 사용할 경우에는 모니터링 프로그램의 설치를 더욱 제한할 필요가 있다. 개인 PC는 가정에서 사적인 목적으로도 활용될 수 있으므로, 모니터링 프로그램을 통해 과도하게 사생활이 노출될 위험이 있기 때문이다. 따라서 사용자가 별도의 업무용 PC를 지급하던가, 개인 PC에 설치하더라도 제한된 영역에서만 작동하도록 하는 등 사생활 침해를 최소화할 수 있는 방안을 모색해야 한다. 또한 만일 모니터링 프로그램을 통해 사적인 통신이 기록되었음을 확인할 경우 이를 즉시 삭제하고 이러한 문제가 재발하지 않도록 대책 마련을 요구해야 한다.

⑨ 회사 내에서 인터넷을 사용할 경우, 자신도 모르게 인터넷 활용이 모니터링될 위험성을 배제하기 힘들다. 이러한 위험을 방지하기 위해서 노동자 개인 수준에서 취할 수 있는 조치는 이메일이든 웹 브라우징이든 전송되는 모든 트래픽을 암호화하는 것이다. 즉 종단간 암호화 기능을 제공하는 애플리케이션을 사용하도록 한다. 보통 통신 내용은 여러 지점을 거치게 되는데(예를 들어 철수 → 철수의 메일 서버 → 통신사 → 영희의 메일 서버 → 영희), 발신자인 철수부터 수신자인 영희까지 통신 내용을 암호화하는 것을 종단간 암호화라고 한다. 통신 보안과 관련한 자세한 내용은 진보네트워크센터가 제작한 「디지털 보안 가이드」를 참고할 수 있다(디지털 보안 가이드 홈페이지: https://guide.jinbo.net/digital-security/).

3. CCTV 등 영상정보처리기기

1) 개요

2021년 디지털 노동감시 실태조사에 따르면, 여전히 CCTV는 사업장에 가장 많이 도입되어 있는 감시설비다. 설치 비용이 크지 않아 편의점이나 식당 등 소규모 사업장에서도 쉽게 CCTV를 설치할 수 있다. 사용자들이 CCTV를 설치하는 주요 이유는 범죄 예방이나 시설 안전 등이다. 문제는 이렇게 설치된 CCTV가 노동자의 근태 관리 목적으로도 활용될 수 있다는 점이다. 많은 사례에서 노동자를 근무태만 등으로 징계하기 위한 근거자료로 CCTV 영상정보가 활용되고 있다. 나아가 노동조합 활동을 감시하기 위한 목적으로 노

동조합 사무실 앞이나 근처에 CCTV를 설치하여 노동조합 사무실을 드나드는 사람들을 촬영하거나, 집회 등 노동조합 활동이 벌어지는 장소를 집중적으로 촬영해서 노동조합 활동에 참여한 사람들을 색출해 내는 근거자료로 활용하기도 한다.

> 〔사례〕 CCTV 감시를 통한 직장 내 괴롭힘
>
> 사단법인 직장갑질119가 2020년 상반기에 이메일로 받은 제보를 분석한 결과에 따르면, 총 1,588건(월평균 265건)의 제보 중 직장 내 괴롭힘이 700건 44.1%로 가장 많았고, 노동법 위반이 619건(39.1%), 코로나 갑질이 269건(16.9%) 순이었다. 직장 내 괴롭힘 유형은 모욕·명예훼손(27.3%), 폭언 폭행(16.1%), 따돌림·차별(15.9%), CCTV 감시·부당지시(11.4%)로 CCTV 감시에 따른 부당지시가 11.4%에 달하였다.
>
> 구체적인 사례로는 ① 대표자가 직원들의 동의를 구하지 않고 CCTV를 설치한 뒤 '보안및 안전을 위하여 24시간 사무실 CCTV 녹화' 안내표지를 부착한 뒤 "CCTV로 보니까 화장실 갈 거 다 가고 인터넷하고 그러더라"라며 직원들에게 똑바로 일할 것을 지시하였고, ② 병원에서 환자 탈의실을 제외한 모든 구역에 CCTV를 설치한 뒤 점심시간에 쉬는 직원에게 "쳐 자빠져 잔다"라고 카카오톡 메시지를 보내고, 환자가 없는 시간에 핸드폰 한다고 시말서를 쓰라고 지시한 사건이 있었다. 또한 ③ 대표자와 대표자 가족 중심으로 운용되는 가족회사에서 갑자기 근로자에게 해고 통보를 하였는데, 이에 반발하자 '일을 안 한다'의 근거라며 대표자가 CCTV 영상을 캡처해 카카오톡 메시지를 보낸 사례가 있었다.[8]

기술 발전으로 영상정보처리장치 역시 고도화되고 있다. 화질도 고도화되고 있고 회전 및 줌 기능은 기본이며, 외부자의 침입과 같은 특정 상황이 발생하면 실시간으로 알려주는 지능형 CCTV로 발전하고 있다. 스마트폰을 통해서 원격으로 모니터링 및 조정할 수 있음을 물론이다. 사용자가 언제 어디서나 노동자를 감시할 수 있는 환경이 조성된 것이다.

인공지능 기술에 힘입어 CCTV는 계속 고도화되고 있다. 세계 최대 전자상거래업체인 아마존Amazon은 인공지능 관리 시스템을 갖춘 감시 카메라를 배달 차량에 탑재하였다. 해당 카메라는 운전자의 행동을 관찰하면서 교통안전 수칙을 잘 지키는지, 운전자가 졸거나 운전 중 딴 짓을 하지는 않는지 등을 지속적으로 관찰하고 안전운전에 위반되는 행위가 포착되면 점수를 측정한다. 아마존은 이렇게 지속적으로 노동자들을 관찰하고 그들을 평가하고 있다.[9]

CCTV는 촬영 대상자의 기본권을 심각하게 침해할 수 있는 여러가지 특성을 가지고 있다. 우선 촬영 대상자를 사전에 특정하기 곤란한 경우가 많고 다수를 대상으로 한 대량 감시가 가능하다. 또한 촬영된 영상을 통해 대상자가 누구인지 뿐만 아니라, 개인의 특징, 행동, 음성, 사람들 사이의 관계 등 다양한 개인정보의 수집이 가능하다. 원거리 촬영을 통해 정보주체가 알지 못하는 사이에 영상정보가 수집될 수도 있다. 만일 여러 CCTV의 영상이 연계되고 개인식별 기능까지 추가된다면 자동화된 개인 추적도 가능해질 것이다. CCTV는 지속적으로 고도화되면서 앞으로도 주요 감시설비의 하나로 활용될 가능성이 크다. 따라서 CCTV를 정당한 목적으로 도입할 필요가 있다고 할지라도 그에 따른 피해를 최소화하기

위한 조치가 함께 고려되어야 한다.

2) 주요 사례 및 개인정보보호법의 적용

CCTV를 통해 촬영되는 영상정보 역시, 영상정보 안에 있는 개인을 '식별'할 수 있다면 '개인정보'이며, 개인정보보호법의 적용을 받는다. 다만 CCTV를 통해 촬영되는 대상이 불특정 다수일 경우 사전에 동의를 받는 것이 불가능하기 때문에, 개인정보보호법은 제25조에서 CCTV 혹은 인터넷에 연결된 IPTV와 같은 영상정보처리기기의 설치·운영에 대한 특별한 규정을 두고 있다. 다만 제25조는 불특정 다수가 출입할 수 있는 '공개된 장소'에 설치된 CCTV에 대해 적용된다. 예를 들어 회사 건물의 로비에 설치된 CCTV, 영업용 버스에 설치된 CCTV 등에는 제25조가 적용될 것이다. 자세한 내용은 3장 5절을 참고한다.

만일 공개된 장소에 설치된 CCTV가 아니라 직원만이 출입할 수 있는 사업장 내에 설치된 것이라면 개인정보보호법 제15조의 적용을 받는다. 우선 법령에서 CCTV의 설치를 규정한 경우가 있다(제15조 제1항 제2호). 영유아 보육법에 따른 어린이집 CCTV, 초·중등교육법에 따른 학교 CCTV, 주차장법에 따른 주차장 CCTV, 의료법에 따른 수술실 CCTV 등이 그것이다. 혹은 촬영 대상이 될 수 있는 특정 노동자들의 동의를 받아 설치할 수도 있다(제15조 제1항 제 1호).

법령상의 규정도 노동자의 동의도 없었을 경우, 사용자는 제15조 제1항 제6호에 따른 사용자의 "정당한 이익을 달성하기 위해 필요한 경우"로 주장할 수 있다. 그러나 이 경우 사용자의 정당한 이익이 정보주체의 노동자의 권리보다 우선해야 하며, 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 범위 내에서 개인정보를 수집해야 한다. 물론 그 기준이 객관적으로 명확한 것은 아니기 때문에, 노동자 입장에서도 사업장 내에 설치되는 CCTV가 합당한 범위를 벗어나서 노동자를 감시할 목적으로 사용될 우려가 없는지 주목할 필요가 있다. KT 업무지원팀 노동자에 대한 CCTV 감시는 이와 관련한 사례이다.

> **〔사례〕 KT의 업무지원팀 노동자에 대한 CCTV 감시[10]**
>
> KT는 2014년 9천여 명을 명예퇴직시킨 후, 명예퇴직을 거부한 노동자 290명을 대상으로 업무지원단CFT을 만들어 배치하였다. CFT가 만들어지고 팀장이 노동자를 대상으로 노동조합 가입여부, 노조 활동 가담 정도 등을 분석한 자료가 발각되기도 했다. KT는 전국 41개팀 업무지원단 사무실 안팎에 CCTV를 설치했는데, 이 CCTV는 사무실 출입 근로자를 비추도록 고정되어 있었다. CCTV 설치 과정에서 직원들의 동의를 구하는 절차는 없었다.
>
> CFT 소속 노동자들은 CCTV가 찍은 영상의 내용과 그 활용 여부에 대한 정보공개를 요청하였으나 KT는 거부하였고, 이에 노동자들은 2017년 업무지원단 사무실 안팎에 설치된 CCTV가 직원 감시용으로 설치됐다며 위법사항 점검을 요청했다. 이에 한국인터넷진흥원에서 현장 조사를 진행하였는데, 의정부 지사의 경우 다른 부서들이 있는 층의 CCTV는 엘리베이터·계단 등 청사 시설물을 폭넓게 비추는 반면 CFT 사무실 앞 CCTV는 직원들이 오가는 출입문만 비추고 있었다. 그러나 개인정보침해 신

고의 접수·상담, 침해 사실의 조사를 담당하고 있는 한국인터넷진흥원은 CCTV 설치행위의 적법성 여부를 판단하지 않고 조사를 종결하였다. 이 사례에서 KT가 설치한 CCTV의 경우 공개된 장소에 설치된 것이 아니기 때문에 개인정보보호법 제15조의 적용을 받는다. 이에 따라 개인정보처리자인 KT는 촬영 대상이 되는 노동자의 동의를 받던가 혹은 사업자의 '정당한 이익'이 명백하게 정보주체의 권리보다 우선하며, 목적 달성에 필요한 합리적인 범위를 벗어나지 않은 것임을 입증할 필요가 있다. CFT 소속 노동자들이 CCTV 설치에 반발하고 있다는 점에서 정보주체의 동의를 받지 않았음은 명백하다. 또한 기사[11]에 따르면, KT는 "시설안전과 보안, 사고예방 등 일반적인 목적으로 설치된 CCTV"라고 주장하는 것으로 보이는데, 다른 부서의 CCTV와 달리 직원들이 오가는 출입문만 비추고 있었다는 점에서 사업자의 정당한 이익을 위한 합리적인 범위 내라고 보기 힘들다.

CCTV를 애초 설치 목적 외로 이용하거나 제3자에게 제공하는 것은 개인정보보호법 위반이다. 예를 들어, 범죄예방 목적으로 설치한 CCTV의 영상자료를 직원 징계 목적으로 활용하는 것은 불법이다. 이런 측면에서 앞서 직장갑질 119에 신고된 사례들(CCTV 영상자료를 징계의 근거로 사용한 사례들)의 경우 개인정보의 목적 외 활용으로 될 가능성이 크다. 한편 아래와 같이 개인정보보호위원회 역시 영상정보처리기기의 설치한 목적 외로 영상자료를 활용한 것에 대해 개인정보보호법 위반이라고 보았다.

영상정보처리기기를 이용한 동의없는 개인정보 처리에 대한 개인정보보호위원회의 법령 해석

○○기관은 버스회사가 버스 내 영상정보처리기기 녹화물을 운전기사들의 징계나 근무평정 자료로 사용하는 행위가 「개인정보 보호법」을 위반하는지에 대한 법령해석을 요청하였다. 버스 안에 영상정보처리기기를 설치한 목적은 '교통사고 증거수집 및 범죄예방'으로 영상정보를 설치목적과 관계없는 운전기사의 징계 또는 근무평정의 자료로 사용하는 것은 허용되지 않으나, 「개인정보 보호법」 제18조제2항의 예외 사유에 해당하는 경우에는 그 범위 내에서 허용될 수 있다고 해석하였다. (2013. 5.)[12]

CCTV의 설치는 그 장소나 촬영 각도 등에 따라 노동조합의 활동을 감시하는 부당노동행위로 간주될 수도 있다. 고용노동부는 CCTV 설치가 부당노동행위에 해당하는지 여부에 대하여 ▲CCTV 설치 목적 내지 동기 ▲CCTV 설치장소·규모·방법 ▲설치장소와 설치목적·필요성의 부합성 ▲보호·관찰의 대상 및 그 방법 ▲녹화화면의 관리 등 운영실태 ▲CCTV 설치 전후의 노사관계 ▲조합활동에 미치는 영향 등 설치를 필요로 하는 현실적이고 상당한 이유가 있는지를 종합하여 판단한다고 밝힌 바 있다.[13] 이러한 판단 근거들은 제15조 제1항 제6호에 따른, 사용자의 정당한 이익과 노동자의 권리 사이의 균형을 판단하는 데에도 사용될 수 있을 것으로 보인다.

얼굴인식 기술의 도입 등 CCTV의 성능이 발전할수록 노동자의 권리에 미치는 부정적 영향은 커질 수 있다. 이와 관

련하여 유럽연합의 개인정보 감독기구는 이러한 사용은 대체적으로 불법일 수 있고, 사용자는 얼굴인식 기술의 사용을 자제할 것을 권고하고 있다.

> **첨단 영상정보처리기기에 대한 유럽연합 개인정보 감독기구의 해석**
>
> 유럽연합의 「사업장에서의 개인정보처리에 대한 의견서」는 비디오 분석 기술의 발전으로 인해 자동화된 방법으로 노동자의 얼굴 표정을 감시하거나, (공장에서) 이동 패턴을 관찰하는 등이 가능해졌는데, 이는 비례성의 원칙을 위반하여 노동자의 권리와 자유를 침해할 수 있으며 대체적으로 불법일 수 있다고 지적하고 있다. 또한 이러한 개인정보의 처리는 프로파일링 및 노동자에 대한 자동화된 의사결정을 포함할 수 있기 때문에, 사용자는 가능한 얼굴인식 기술의 사용을 자제해야 한다고 권고하였다.[14]

얼굴인식과 같은 생체인식정보는 개인정보보호법 제23조에 따른 민감정보에 해당한다. 따라서 법령에 근거가 있거나 정보주체의 별도의 동의가 없는 한 처리할 수 없다. 사업장 내 얼굴인식 설비의 설치를 요구하는 법령은 현재 없으며, 노사관계의 특수성을 고려할 때 노동자의 자유로운 동의가 인정받기 어렵다는 점을 고려하면, 사실상 국내에서도 사업장 내에서 얼굴인식 기술의 사용은 불법이 될 가능성이 크다.

3) CCTV 등 영상정보처리장치의 설치에 대한 노동자의 대응 방안

① 넓은 범위를 대상으로, 정보주체도 모르는 사이에 은밀하게, 체계적인 감시가 가능하다는 점에서 CCTV 등 영상정보처리장치(편의상 CCTV로 지칭하지만 폐쇄회로 텔레비전을 포함한 모든 종류의 영상장치를 포함한다)는 노동자 및 노동조합에 대한 감시 목적으로 활용될 위험성이 크다. 따라서 원칙적으로 노동자를 대상으로 한 CCTV의 활용은 금지해야 한다. 시설이나 사물에 대한 모니터링을 위해 CCTV를 설치했더라도, 이를 통해 노동자나 다른 사람이 촬영될 수 있으므로 적절한 안전조치를 취해야 한다.

② 최근 CCTV가 소형화되어 사람의 눈에 띄지 않는 몰래카메라가 설치될 수 있으니 주의해야 한다. 이는 개인정보보호법을 위반하는 명백한 불법행위다. 동의 없는 개인정보 수집(개인정보보호법 제15조 위반)이나 개인정보보호법 제25조에서 규정한 목적 외로 CCTV를 설치하는 것은 과태료 대상일 뿐이지만, "거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득"한 것으로 인정될 경우에는 3년 이하의 징역 또는 3천만 원 이하의 벌금에 해당하는 형사처벌을 받을 수 있다. 만일 이를 통해 "성적 욕망 또는 수치심을 유발할 수 있는 다른 사람의 신체를 그 의사에 반하여" 촬영했을 경우에는 '성폭력범죄의 처벌 등에 관한 특례법'으로 처벌(5년 이하의 징역 또는 1천만 원 이하의 벌금)이 가능하다.

은밀한 노동감시는 노동자의 기본권을 심각하게 침해하는 행위이므로 강력한 대응이 필요하다.

③ 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는

장소의 내부를 촬영할 수 있는 CCTV의 설치는 개인정보보호법 위반이다. 이에 근거하여 설치를 반대해야 하고, 사용자가 설치를 강행할 경우 개인정보보호위원회에 신고한다.

④ CCTV가 설치된 경우, ▲설치 목적 및 장소 ▲촬영 범위 및 시간 ▲관리책임자 성명 및 연락처 등을 포함한 안내판을 설치하도록 해야 한다. 이는 공개된 장소에 설치된 CCTV의 경우에는 의무이며, 공개되지 않은 사업장 내 장소에 설치될 경우에도 안내판을 설치하도록 요구할 필요가 있다. 그래야 노동자들이 CCTV에 의해 모니터링될 수 있음을 항상 인지할 수 있기 때문이다.

⑤ 설치 목적과 다른 목적으로 CCTV를 임의로 조작하거나 다른 곳을 비추도록 해서는 안 된다. 이는 공개된 장소에 설치된 CCTV의 경우에는 의무이며, 공개되지 않은 사업장 내 장소에 설치될 경우에도 설치 목적 외 임의 조작은 동의받은 목적 외 개인정보 수집이나 사용자의 '정당한 이익'을 벗어난 활용 등 개인정보보호법 위반이 될 수 있다. CCTV를 임의로 조작하여 노동조합 활동이나 집회 등을 감시한 사례가 종종 발생한 바 있다.

⑥ CCTV의 녹음 기능은 사용하지 않도록 요구한다. 공개된 장소에 설치된 CCTV의 경우 이는 개인정보보호법 위반이 되며, 정보주체의 동의 없는 음성 녹음은 통신비밀보호법 위반이 될 수 있다.

⑦ 법률에서 CCTV 설치를 요구한 경우에는 법령에서 요구하는 안전조치를 취하고 있는지 확인할 필요가 있다. 예를 들어 영유아 보육법의 경우 어린이집에 CCTV 설치를 의무화하면서 ▲아동학대 방지 등 영유아의 안전과 어린이집의 보안을 위하여 최소한의 영상정보만을 적법하고 정당하게 수집하고, 목적 외의 용도로 활용하지 아니하도록 할 것 ▲영유아 및 보육교직원 등 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 영상정보를 안전하게 관리할 것 ▲영유아 및 보육교직원 등 정보주체의 사생활 침해를 최소화하는 방법으로 영상정보를 처리할 것 등의 의무를 준수하도록 하고 있다.

⑧ 노동조합과 CCTV의 설치 여부에서부터 CCTV 설치 방법과 수집된 영상정보의 처리 방법에 대해 구체적으로 협의할 것을 요구한다. 이러한 협의에는 다음과 같은 내용이 포함될 수 있다. ▲설치 목적 ▲해상도 등 세부 사양 ▲네트워크와의 연결 여부 ▲설치 장소 ▲촬영 범위·시간·방법 ▲줌이나 회전 등 조작 가능 여부 ▲원격조작 가능 여부 ▲음성 녹음 여부 ▲모니터링 권한을 가진 자 혹은 부서 ▲영상정보 보관기간 ▲영상정보 열람 권한을 가진 자 혹은 부서 ▲안전조치 ▲정보주체의 열람권 보장 방법 등. 단체협약을 통해 CCTV 설치에 대해 합의한 경우, 단체협약에 위배되는 CCTV의 철거를 요구할 수 있다.

〔사례〕 단체협약을 위반하여 설치된 CCTV에 대해 철거할 것을 판결

이 사건 단체협약 제71조 제1항은 조합 또는 조합원을 감시할 목적으로 CCTV 등의 감시장비를 설치하는 행위를 전면적으로 금지하면서, 그 단서에서 노동안전, 도난 등 위험·사고방지를 위해 감시장비를 설치하는 경우에는 사전 합의를 거친 경우에 한하여 감시장비를 설치할 수 있도록 규정하고 있다. 피고가 위 규정을 위반하여 이 사건 CCTV를 설치한 행위는 원고 지부의 자유로운 활동이나 그 조합원들의 인격권을 침해할 여지가 있고, 피고가 이 사건 CCTV를 조합원들을 감시하려는 목적이 아니라 방범 및 보안 목적으로 설치하는 경우에도 위 단체협약에서 정한 바에 따라 이 사건 CCTV를 설치하기 전에 미리 원고 지부와 합의를 하여야 한다. 그런데 피고는 이 사건 CCTV를 설치하면서 원고 지부와 아무런 사전 합의를 하지 않았다. 피고가 원고와 아무런 사전 합의 없이 이 사건 CCTV를 설치한 것은 이 사건 단체협약에 위배되므로, 피고는 이 사건 CCTV를 철거할 의무가 있다. **(의정부지방법원 고양지원 2012.2.3 선고 2011가합3374 판결)**

⑨ 지능형 CCTV 혹은 얼굴인식 기능을 포함한 CCTV는 극히 예외적인 경우 외에는 도입되어서는 안 된다.

4. 노동자 위치정보의 수집 및 추적

1) 개요

회사는 다양한 목적으로 노동자의 위치를 파악한다. 예를 들어 고객 방문 서비스의 원활한 조정이나 화물의 운송 현황 파악 등을 명분으로 위치추적이 이루어진다. 실제로 수집되는 것은 단말기(스마트폰이나 PDA)나 차량 등 기기의 위치정보이지만, 이를 통해 해당 기기를 보유·사용하고 있는 정보주체, 즉 노동자의 위치를 파악할 수 있으므로, 이 역시 '개인위치정보'의 수집이 될 수 있다.

정보통신기술의 발전으로 인해 우리의 위치는 더욱 쉽게 파악되고 기록되고 있다. 스마트폰을 가지고 있기만 해도 통신사는 24시간 내 위치를 기록하고 있다. 스마트폰의 GPS를 통해 지도앱이나 페이스북 등 서비스 제공자들은 내 위치를 기록하고, 그에 기반한 서비스를 제공한다. IP 주소, Wifi 공유기, RFID 카드, 생체인식 출입통제 시스템 등을 통해서도 내 위치가 파악될 수 있다. 교통카드나 신용카드 기록은 단지 물품과 서비스의 내역만이 아니라 내 위치를 보여준다. 업무 과정에서 이러한 각종 장치들을 통해 위치정보가 수집될 수 있다.

사업장 내에서 여러 경영상의 이유로 사물 혹은 노동자의 위치를 파악할 필요가 있다고 해도, 노동자의 위치정보가 상시적으로 파악·기록됨에 따라 원래의 수집 목적을 벗어나 노동감시의 목적으로 활용될 가능성을 배제할 수 없다. 예를 들어 화물 운송 현황 파악 목적으로 수집되는 차량의 위치정보가 해당 노동자의 근태 관리나 징계 목적으로 활용될 가능성이 있는 것이다. 코로나19 이후 재택근무가 일상화되면서 재택근무 중인 노동자들의 관리를 위해 위치추적 기능이 활용되고 있기도 하다.

개인위치정보는 해당 개인에 대해 여러 가지를 얘기해줄

수 있다. 예를 들어, 현재 제 위치에서 근무하고 있는지, 근무지를 이탈했는지, 사적인 업무를 보고 있는지, 카페에서 누군가와 만나고 있는지, 해당 정보주체의 통상적인 이동 패턴은 어떠한지 등을 파악할 수 있다. 차량을 지속적으로 모니터링 한다면 운전자의 운전습관을 알 수도 있다. 따라서 개인의 위치정보는 매우 민감한 개인정보이며 엄격한 보호가 필요하다. 업무과정에서 수집되는 노동자의 위치정보 역시 마찬가지다.

노동자의 위치정보는 PC 및 인터넷 모니터링 프로그램이나 모바일 앱, CCTV, 스마트카드나 생체인식 출입통제장치 등을 통해서도 수집될 수 있다. 각 감시설비에 대한 대응 방안은 해당하는 절을 참고한다.

2) 노동자 위치정보 수집에 대한 법적 규율

개인위치정보 역시 개인정보의 하나이지만, 개인정보보호법에 우선하여 '위치정보의 보호 및 이용 등에 관한 법률'(위치정보법)이 적용된다(위치정보법에 대한 설명은 2장 3절을 참고). 그런데 위치정보법은 주로 위치정보사업자와 위치기반서비스사업자가 개인위치정보 수집·처리하는 문제를 규율하고 있다. 하지만 사용자가 위치정보사업자나 위치기반서비스사업자로부터 노동자의 위치정보를 제공받을 수는 있지만, 스스로 위치정보사업자나 위치기반서비스사업자로서 수집하는 것은 아니다. 위치정보법에서 위치정보사업자나 위치기반서비스사업자가 아닌 자가 위치정보를 수집·이용할 때 적용되는 규정은 제15조밖에 없다. 이에 따라 사용자를 포함하여 누구든 타인의 위치정보를 수집하기 위해서는 정보주체의 동의를 받아야 한다. 그러나 위치정보법 제15조는 정보주체의 동의 없이 위치정보를 수집·이용하지 못하도록 할 뿐, 동의를 받을 때 고지해야 할 내용이라든가 수집한 위치정보를 어떠한 원칙에 따라 처리해야 하는지 등은 별도로 규정하고 있지 않다. 사용자가 위치정보사업자로부터 노동자의 위치정보를 제공받든 직접 수집하든 상관없이 노동자의 위치정보를 수집할 경우 개인정보보호법의 적용을 받게 된다. 따라서 사용자가 처리하는 개인위치정보와 관련해서는 본 가이드의 개인정보보호법의 적용에 대한 내용을 참고하면 된다.

다시 정리하자면, 사용자가 노동자의 개인위치정보를 수집하는 방법은 몇 가지로 구분된다.

① 위치정보사업자나 위치기반서비스사업자가 노동자의 위치를 수집하고 이들로부터 위치정보를 제공받을 수 있다. 예를 들어 스마트폰의 기지국 위치정보를 통신사업자가 수집하고, 통신사업자로부터 위치정보를 제공받아 위치기반서비스사업자가 위치추적시스템을 구축하면, 사용자는 위치추적시스템을 통해 노동자의 위치를 파악할 수 있다. 이 경우 위치정보법에 따라 위치정보사업자, 위치기반서비스사업자, 사용자는 모두 노동자의 동의를 받아야 한다.

② 위치정보사업자나 위치기반서비스사업자의 개입 없이, 사용자가 다양한 방법으로 노동자 혹은 노동자가 보유한 기기로부터 위치정보를 직접 수집할 수 있다. 예를 들어 노동자의 기기에 설치된 특정 앱을 통해 수집된 GPS 위치정보를 직접 수집할 수 있을 것이다. 스마트카드 기록을 통해 특정 노동자가 회사 건물 내에 어디를 출입했는지를 파악할 수도 있다. 이 경우에도 해당 노동자의 동의를 받아야 한다. 다만 위치정보법은 단지 동의 없이 수집·이용 또는 제공하지 못하도록 할 뿐 다른 구체적인 규정이 없으므로, 위치정보를 포함한 노동자 개인정보의 처리는 개인정보보호법이 적용된다.

한편 국가인권위원회는 산불감시원의 위치정보활용 사건에서 개인정보자기결정권 침해를 인정하며, 위치정보 사업자 등이 목적을 벗어나 개인위치정보를 사용하지 않도록 조치하고 정보주체인 산불감시원에게 개인위치정보가 어떻게 사용·관리되는지, 정보주체의 권리 제한 및 보장내용이 무엇인지 등을 충분히 인지할 수 있도록 조치할 것을 권고했다. 산불감시원에게 개인위치정보 조회에 대한 동의를 받기는 했지만, 위치정보법 제15조, 제18조, 제19조에서 규정하는 동의를 포괄한다고 보기는 어렵다고 보았다. 국가인권위원회의 판단은 인권적 관점에서 정보주체에 대한 충분한 고지의 필요성과 목적 외 활용을 통제하기 위한 조치를 요구했다는 점에서 의미가 있다.

〔사례〕 국가인권위 2010진정0040200 등 산불감시원 위치정보활용 사건

산림청과 관할 구청 등 시행기관은 산불 발생 시 진화의 효율성을 위해 '산불 상황 관제 시스템'을 도입하여 실제 이동하며 산불감시 및 예방 활동을 하는 산불감시원에게 위치조회 단말기를 지급하였다. 위치 기반서비스사업자는 산불감시원에게 지급된 단말기의 위치를 이동통신사의 통신망을 통해 확인하여 '산불 상황 관제 시스템'을 운용하였고, 산림청과 시행기관은 위치기반서비스업자가 운용하는 이 시스템에 접속하여 산불감시원의 위치를 파악하였다. 단말기는 24시간 계속 작동되는 것이 아니라 실제 근무시간인 09:00~18:00 동안에만 작동하며, 단말기의 ON/OFF는 산불감시원이 직접 버튼을 누르도록 되어 있다. 시행기관은 단말기를 통해 산불감시원의 출퇴근, 근무지 이탈 등을 확인할 수 있고 산불감시원의 이동사항 및 위치 등을 관리하여 담당구역 및 순찰경로 등을 조정함으로써 효율적인 산불예방활동을 강화할 수 있다. 또한 실제 산불발생 시 단말기의 응급버튼을 누르면 시스템에 표시되어 정확한 산불발생 위치와 위성사진을 이용하여 신속하게 진화할 수 있다. 시행기관은 산불감시원으로부터 개인위치정보 조회에 대한 동의서를 받았지만, 위치정보사업자와 위치기반서비스사업자는 개인위치정보 수집 이용 제공에 대한 어떠한 동의도 받지 않았다

이에 대해 국가인권위원회는 산림청이 산불감시원에게 위치조회 단말기를 착용하도록 한 것은 법령상의 동의를 받았고 산불 예방과 신속한 산불 진화라는 공익적 목적에 부합하기 때문에 인권침해라고 단정하기 어렵지만, 위치정보를 누구에게 제공하여 어떤 방식으로 사용되는지, 그리고 개인 위치정보가 보호되는 방식과 산불감시원에게 법적으로 보장되는 권한 등에 대해서 충분히 설명하지 않았다는 점과 위치정보사업자 및 위치기반서비스 사업자에게 산불감시원의 개인 위치정보가 남용되지 않도록 구체적인 보호조치를 하지 않았다는 점을 들어 헌법 제10조 및 제17조에 기반을 둔 개인정보자기결정권을 침해한 것으로 판단하였다.

한편 고용노동부는 2020년에 발행한「재택근무 종합 매뉴얼」에서 "재택근무자의 근태관리를 위해 GPS 등을 통해 위치추적을 해도 되는지"에 대한 질의에 대한 답변에서 "재택근무자로부터 위치정보(GPS 등)를 수집하기 위해서는, 사전에 ▲수집·이용 목적, ▲수집항목, ▲정보 보유·이용 기간, ▲동의 거부 가능 사실 등을 고지한 후 근로자의 동의를 받아야 "한다고 설명하고, 그러나 동의를 강요해서는 안 된다고 덧붙였다. 또한 근태관리를 위해 GPS 위치정보의 수집 필요성이 있다고 하더라도 "정보수집을 강제하거나 그 거부를 이유로 한 징계는 정당하다고 보기 어렵다"고 하였다.

그러나 이에 대해 노동자들은 반발을 했는데,[15] 현실적으로 노동자가 사용자의 위치정보 수집 요구를 거부하기 힘들기 때문에, 형식적인 동의를 받고 재택근무 노동자를 위치추적하는 데 악용될 수 있다는 것이다. 이는 비단 위치정보 수집뿐만이 아니라 모든 형태의 감시설비 도입과 개인정보 수집에 관련된 문제일 것이다. 특히 위치정보법의 경우 정보주체의 동의 없이 위치정보를 수집하지 못하도록 했기 때문에, 진정한 동의가 보장된다면 위치정보의 수집을 거부할 수 있는 근거도 될 수 있지만 형식적인 동의가 관행이 된다면 사실상 위치정보의 남용을 허용할 수 있는 양면성을 가지고 있다.

3) 노동자 위치정보 수집 및 추적에 대한 노동자의 대응 방안

① 노동자의 위치정보를 직접적으로 수집하기 보다는 차량이나 단말기와 같은 사물의 위치정보 수집을 통해 개인위치정보를 수집할 수 있다. 그러나 이동성이 있는 사물의 위치정보라도 이를 통해 그것을 소지하고 있는 개인을 식별할 수 있고, 해당 개인의 위치를 파악할 수 있다면 '개인위치정보'임을 인식해야 한다. 사물의 위치정보라는 이유로 동의 없이 수집되어서는 안 된다.

② 해당 업무수행에 반드시 필요한 경우가 아니라면 위치정보 수집에 동의를 해서는 안 된다. 노동자는 위치정보 수집에 대한 동의를 요구받을 때, 해당 목적 달성을 위해 자신의 위치정보가 필요한지 따져보아야 할 것이다. 노동조합이 개인위치정보의 수집 여부 및 범위에 대해 협의를 할 경우에도 특정 목적 달성을 위해 위치정보의 수집이 필요한지, 또는 필요한 범위는 어디까지인지 따져보아야 한다.

③ 위치정보는 정보주체의 동의가 있어야 수집할 수 있으며, 이는 자유로운 동의여야 한다. 따라서 동의를 거부했다는 이유로 징계를 받아서는 안 된다.

④ 업무수행을 위해 위치정보를 수집할 수밖에 없는 경우, 해당 업무 목적 외로 수집된 개인위치정보를 활용하도록 허용해서는 안 된다. 예를 들어 화물 운송 현황 파악 목적으로 수집한 위치정보가 노동자 징계 목적으로 활용되어서는 안 된다.

⑤ 근무 시간 중에 사적인 이용이 허용될 경우, 혹은 업무를 목적으로 활용한 기기를 퇴근 시간 후에 계속 소지하는 경

우 등과 같이 업무 목적으로 위치정보를 수집할 수밖에 없지만 업무 외적인 개인의 위치도 수집될 우려가 있는 경우, 정보주체가 위치추적 기능을 끌 수 있는 권한을 부여받을 필요가 있다.

5. 업무 관련 모바일 앱 설치

1) 개요

점차 스마트폰, 태블릿, PDA 등 모바일 기기가 데스크탑 PC를 대체하고 있다. 이동성이 있어 언제 어디서나 활용 가능할 뿐만 아니라, 기기의 성능도 데스크탑에 맞먹을 정도로 고도화되고 있고 카메라, GPS 등 데스크탑에는 없는 기능들도 보유하고 있다.

회사 내에서도 스마트폰 등을 활용한 업무가 증가함에 따라 기기에 업무에 필요하다는 명분으로 특정 앱의 설치를 요구하는 기업이 증가하고 있다. 특히 사무실 밖에서 근무하는 노동자의 경우 더욱 그렇다. 그러나 일반 노동자들이 자신의 스마트폰에 설치된 앱이 어떻게 작동하는지 자세히 알기는 힘들며 그럴수록 노동감시에 대한 불안이 커질 수밖에 없다.

나아가 노동자의 개인 스마트폰이든, 회사에서 지급한 기기이든 상관없이 업무용으로 사용되는 다양한 모바일 기기를 통합적으로 관리하고 있는 솔루션도 활용되고 있다. 이를 MDMMobile Device Management이라고 하는데, 직원들의 스마트폰, 태블릿 등 모바일 기기를 등록하고 통합 관리할 수 있는 솔루션을 의미한다. 아동·청소년의 스마트폰 사용을 감시·통제하는 감시 앱도 널리 활용되고 있는데, 사실상 기능적 측면에서는 다를 바 없다. MDM은 다음과 같이 원격으로 모바일 기기를 통제할 수 있는 다양한 기능들을 포함하고 있다.

- 모바일 기기의 기능 관리: 카메라 및 마이크의 기능 제어
- 네트워크 제어: GPS/와이파이/블루투스 등 네트워크 제어, 위치추적, 화면캡쳐 및 화면유출방지 등
- 애플리케이션 관리: 업무용 앱 설치 및 앱 데이터 관리, 앱 사용 모니터링 등
- 모바일 기기 보안: 화면 잠금, 단말기 위치 찾기, 데이터 백업 및 삭제, 공장 초기화 등
- 관리 및 보고: 등록된 모바일 기기 현황, 사용 통계, 로그 관리 등

유사하지만 조금씩 다른 솔루션으로, 기기가 아니라 애플리케이션과 관련 데이터만을 통제하는 MAMMobile Application Management, 스마트폰, 태블릿뿐만 아니라 노트북, 데스크탑, 사물인터넷 기기 등 모든 하드웨어를 제어하는 UEMUnified Endpoint Management, 다양한 소프트웨어 관리 툴을 통합적으로 관리할 수 있는 EMMEnterprise Mobility

Management 등이 있다.[16]

원격으로 컴퓨터와 인터넷 사용을 모니터링하는 솔루션과 마찬가지로, MDM는 노동자의 모바일 기기 사용을 전면적으로 감시·통제할 수 있다. 노동자가 모바일 기기로 무엇을 하고 있는지 모니터링하는 것을 넘어 원격으로 앱을 설치하거나 화면 잠금을 하는 등 직접 통제도 가능하기 때문이다. 또한 통상적으로 데스크탑 컴퓨터의 경우 회사에서 지급하는 것을 사용하지만, 모바일 기기의 경우 노동자 개인의 스마트폰을 사용하는 경우도 많아 노동자의 기본권에 미치는 영향이 더욱 크다.

2) 업무용 앱을 통한 노동감시의 규율

모바일 기기 역시 컴퓨터라는 점에서 사업장 내에서 설치되어 모바일 기기 자체 및 모바일 기기를 통한 인터넷 사용을 모니터링하는 앱의 설치에는 제2절 '컴퓨터 및 인터넷 이용 모니터링'에서 설명한 내용들이 기본적으로 적용된다. 기술적으로는 일반 컴퓨터와 다른 모바일 기기의 특성이 고려되어야 하며, 데스크탑 컴퓨터에 비해 특정 개인과의 연결성이 강하다고 할 수 있다. 업무용 앱은 특정 업무를 위한 애플리케이션에서부터 MDM 솔루션과 같은 전면적인 감시·통제가 가능한 솔루션까지 다양할 수 있는데, 기능에 따라 노동자의 기본권에 미치는 영향이 달라질 것이다. 또한 이러한 모바일 앱의 설치가 정당화될 수 있는지는 설치 목적의 정당성, 정보주체의 권리에 미치는 부정적인 영향의 정도, 개인정보 처리의 투명성 정도, 대체 수단의 존재 여부 등에 따라 달라질 것이다. 특히 모바일 앱의 경우 노동자의 개인 스마트폰에도 설치될 수 있는데, 이 경우 노동자의 개인적 활용까지 모니터링될 가능성이 크다.

아래 사례는 업무용 앱 설치 요구를 거부한 노동자에 대해 징계를 한 것에 대해, 사용자의 업무 지시의 필요성보다 노동자의 개인정보자기결정권의 침해가 더 크다고 판단하며 징계 무효를 확인한 사건이다. 해당 앱의 기능이 투명하게 노동자에게 고지되지 않았고, 별도 단말기의 지급과 같은 대체수단이 있었던 점 등이 중요하게 고려된 것으로 보여진다.

> **〔사례〕 KT의 업무지원팀 근로자에 대한 업무용 앱 설치 강요**
>
> 2015년 KT는 업무지원단 소속 노동자들에게 무선서비스 품질 측정 앱을 개인 단말기에 설치할 것을 지시하였다. 이 앱은 개인 휴대폰의 ▲카메라 ▲현재 위치 ▲통화 ▲연락처 ▲캘린더 일정 ▲저장소 ▲문자메시지 ▲계정정보 등 12개 항목에 접근권한을 부여하도록 하고 있다. 마지막까지 해당 업무지시를 거부한 한 노동자는 '(사규에 정해져 있는) 별도 단말기의 지급' 혹은 '해당 부서 내의 다른 업무로의 이전'을 요구했으나 사측은 이를 무시하였고, 당사자가 황창규 당시 대표이사에게 고충 이메일을 보내자 업무지시 불이행 및 조직질서 위반을 사유로 정직 및 전보의 징계 조치를 하였다. 이에 당사자는 사측을 상대로 징계무효확인 소송을 제기했고, 2017년 1심 판결(수원지방법원 성남지원 2017. 4. 4. 선고 2015가합206504 판결)에 이어 2018년 6월 항소심(서울고등법원 2018. 6. 26. 선고 2017나2024180 판결)에서도 '징계가 무효임을 확인하며, 회사는 이에 따른 임금 손해액을 지급하라'는 판결을 받아 승소 확정

되었다.

사측은 노동자들의 우려가 근거가 없고, 설치 시 '동의' 여부를 묻기 때문에 개인정보를 침해하지 않는다며 해당 업무지시의 정당함을 주장하였다. 그러나 법원은 ▲해당 앱이 위와 같은 접근권한들을 요구하는 것은 기본권인 개인정보자기결정권에 대한 제한에 해당한다는 점, ▲과학기술의 진보에 따라 기업의 근로감시활동이 전자장비와 결합, 확대됨에 따라 노동자의 인격권 내지 사생활 침해 우려가 고조되는 상황 및 앱 이용자들이 본인의 정보가 어떻게 수집, 활용되는지 알 수 없는 상황을 고려해야 한다는 점, ▲따라서 노동자는 가능한 한 개인정보자기결정권의 침해 방지를 위하여 업무수행과 관련하여 보호받아야 할 자신의 개인정보자기결정권을 존중해줄 것을 사용자에게 요구할 수 있다는 점을 명확히 판시하였다. ▲결론적으로 이 사건에서 존중되어야 하는 노동자의 개인정보자기결정권에 비해 사용자의 업무지시의 필요성이 더 크다고 볼 수 없으므로, 해당 노동자에 대한 징계는 그 사유가 부존재하여 위법, 무효라고 보았다.

위 판결은 노동자의 개인정보자기결정권과 사용자의 업무지시권 사이의 이익형량을 통해 개인정보자기결정권 제한의 불이익을 중요하게 평가하였다. 이에는 개인정보 침해 우려가 없음을 노동자들에게 입증하고 설득하려는 노력이 미흡했던 점, 개인정보 침해 우려가 없는 대안이 존재했다는 점 등이 영향을 미쳤다. 그러나 앱을 설치하도록 강요한 사용자의 업무지시가 개인정보보호법상 '실질적 동의절차'를 확보한 것이 아니라는 측면에서 법률 위반의 소지가 있음에도, '형식적 동의절차'가 있다는 이유로 개인정보보호법 위반이 아니라고 판단한 것은 문제가 있다. 진정으로 자유로운 의사표시가 아닌 '형식적 동의절차'만으로 동의요건을 충족한 것으로 보는 것에 대해서는 지속적으로 문제제기할 필요가 있다.[17]

특히 MDM 기능을 하는 앱의 경우 노동자에 대한 전면적인 모니터링과 통제가 가능하기 때문에 앱의 도입을 정당화하기 힘들다. MDM 앱이 제공하는 기능 중 일부 기능만 사용한다고 해도 운영 과정이 노동자에게 투명하지 않다면, 사용하지 않을 것이라 믿었던 기능들이 사용될 가능성을 우려할 수밖에 없다. MDM 앱을 사용하기보다는 목적 달성을 위한 특정 기능만을 가지고 있는 앱을 사용하는 것이 바람직하다.

유럽연합 회원국의 개인정보 감독기구 대표로 구성되고 개인정보 보호규정 해석의 지침을 제공하는 WP29는 2017년 발간한 의견서에서 MDM을 처음 도입할 때 개인정보처리자(사용자)는 개인정보 영향평가를 시행해야 한다고 권고하였다. 그리고 영향평가의 결과 특정 환경에서 MDM 기술을 사용할 필요가 있다고 하더라도, 그 결과인 개인정보 처리가 비례성과 보충성의 원칙을 준수하고 있는지 평가가 필요하다고 하였다. 사용자는 이 기술이 특정 목적으로만 사용되고 더 폭넓은 노동 감시의 일환이 되지 않도록 보장해야 한다. 비록 특정 목적이라고 하더라도 추적 기능은 완화되어야 하는데, 예를 들어 사용자가 기록된 위치정보에 접근할 수 없도록 하고 모바일 기기의 위치를 파악하거나 분실되었을 경우에만 접근할 수 있도록 설정될 수 있을 것이다. 또한 노동자들은 MDM의 추적 기능과 그 영향에 대해 충분한 정보를 제공받아야 한다고 권고하였다.[18]

그러나 국내 유수의 대기업들은 보안 등을 명분으로 MDM 타입의 모바일 앱의 설치를 강요하여 노동자와 노동조합의 반발을 야기하고 있다. 문제가 되는 사례를 보면 공통

적으로 앱이 어떠한 기능을 하고 개인정보가 어떻게 처리되는지에 대해 노동자에게 투명하게 설명하지 않고 있으며, 정보주체인 노동자 및 노동조합과의 협의 없이 일방적으로 도입되고 있다는 문제점을 가지고 있다.

〔사례〕 국내 기업의 MDM 도입 논란 사례

2014년 포스코는 광양제철소에서 일하는 사내하청 직원들에게 MDM 앱 '포스코 소프트맨'의 설치를 요구하고 설치하지 않을 경우 출입을 통제하겠다고 하여 노동자들이 반발하였다. 금속노조 포스코사내하청지회는 개인정보 유출 및 사생활 침해를 우려하며 앱 설치를 거부하였다. 이미 포스코 광양제철소에서 일하는 정규직은 해당 앱을 설치한 상태였다. 이 앱은 스마트폰 카메라 통제, 모바일 앱 실행 및 통제, 스마트폰 업무시스템 장애 발생시 원격 지원 기능, 스마트폰 모니터링 기능 등을 가지고 있는 것으로 알려졌다. 포스코 측은 광양제철소가 국가보안목표 '가'급 시설이기 때문에 보안을 위해 MDM 앱 설치를 요구한 것이라고 하지만, 문제는 이 앱을 통한 감시의 범위가 어디까지인지 명확히 밝히지 않았다.[19]

2020년 현대자동차는 공장 보안을 명분으로 울산공장 하청직원들을 대상으로 모바일출입시스템 도입을 결정하였고, 이에 노동조합은 불법파견을 합리화하기 위한 것이라며 반발하였다. 이 시스템은 MDM 타입의 앱이었으며, 울산공장의 협조전에서 "신청과정 중 모바일 본인인증 및 삼성/LG폰의 경우 카메라촬영 통제(MDM) 기능 적용"이라고 명기되어 있었다. 현대자동차는 보안을 위한 것이며 감시 사찰은 없다는 입장이지만, 이 앱의 도입과 관련해서 노동조합과 협의하거나 앱의 기능 및 수집되는 개인정보에 대해 투명하게 공개하지 않은 것으로 보인다.[20]

삼성물산은 평택시 삼성전자 반도체공장 건설현장에 삼성의 보안 앱을 도입하였다. 이 앱을 통해 로그인해야 건설현장의 출입이 가능하며, 이 앱을 사용하는 동안 위치서비스와 알림. 블루투스 기능이 활성화된다. 건설노조 경기도건설지부는 노동자들에게 앱의 통제 범위를 알려 주지 않는 것을 비판하며 문자메시지, 카카오톡, 실시간 통화까지 감청되는 것은 아닌지 우려하였다.[21]

현대중공업은 2021년 8월, 보안을 이유로 노동자에게 MDM 설치를 권고했다. 사측은 MDM이 다양한 기능이 있음에도 "촬영기능만 제한하겠다"고 하지만, 노조는 보안스티커 부착으로 충분하다는 입장이다. 촬영 방지가 목적이라면 다른 대체수단이 있음에도 불구하고 MDM 앱을 도입한다면, 향후 앱 기능의 활용이 확대될 가능성도 있다.[22]

3) 업무용 앱 설치에 대한 노동자의 대응 방안

① 모바일 기기에 설치되는 앱의 기능, 앱이 접근·처리할 수 있는 데이터의 범위 등에 대해 투명하게 공개할 것을 요구해야 한다. 필요하다면 노동조합이 해당 분야의 기술 전문가에게 자문을 요청할 수 있어야 한다. 해당 앱의 기능과 작동 범위를 모르는 상황에서 앱 설치에 동의해서는 안 된다.

② 모바일 기기에 설치되는 앱의 특정 기능이 필요한 이유를 명확히 해야 한다. 특정한 업무 목적 달성을 위해 반드시 필요한 것이 아닐 경우, 해당 기능을 활성화하지 않도록 요구한다. 가능하다면 목적 달성에 필요한 기능만 있는 앱을 설치하는 것이 바람직하다.

③ 통상적으로 스마트폰 등 모바일 기기는 개인과의 결합이 강하고 24시간 갖고 다니는 경우가 많기 때문에, 모바일 기기에 대한 감시는 해당 개인의 프라이버시를 크게 침해할 수 있다. 따라서 가능한 개인 소유의 모바일 기기를 업무용으

로 사용하는 것은 자제할 필요가 있고, 업무용 앱을 설치할 모바일 기기를 회사에서 제공하도록 요구하는 것이 바람직하다. 만일 불가피하게 업무에 필요한 앱을 개인용 스마트폰에 설치해야 한다면, 해당 앱의 기능은 특정 목적 달성을 위한 것으로 제한되어야 하며, 스마트폰의 여타 기능이나 데이터에 접근하도록 해서는 안 된다.

④ MDM 앱은 개인의 프라이버시를 심각하게 침해할 우려가 있기 때문에, MDM 설치는 거부할 필요가 있다. 예외적으로 MDM를 설치할 필요가 있다면 여러 안전장치가 마련되어야 한다. 우선 해당 앱에 대한 개인정보 영향평가를 수행할 필요가 있다. 국내 개인정보보호법은 공공기관의 경우 일정한 요건을 갖춘 개인정보 처리에 대해 영향평가를 의무화하고 있으며, 민간기업 등 공공기관 외의 경우에도 개인정보 처리의 위험성이 높을 경우 영향평가를 수행할 것을 권고하고 있다. 또한 MDM 설치 목적이 명확해야 하고 해당 목적 달성에 필요한 최소한의 기능만 활성화되어야 한다. MDM을 통해 수집된 개인정보에 대한 접근 권한 및 요건도 반드시 필요한 경우로 제한되어야 한다. MDM은 개인정보 침해 위험성이 큰 만큼, 반드시 노동조합 혹은 노동자 대표와의 협의를 통해 도입되어야 하며, 적절한 감사 등 남용을 최소화할 방안이 마련되어야 한다.

⑤ 이 장의 2절 '컴퓨터 및 인터넷 이용 모니터링'의 관련 내용을 참조한다.

6. 지문 등 생체인식정보의 수집

1) 개요

스마트폰 잠금해제 기능에서부터 출입국 관리, 근태관리 시스템까지 지문, 정맥, 홍채 등 생체인식기술의 활용이 증가하고 있다. 코로나19로 비대면 및 비접촉이 중요해지자 얼굴인식을 통한 출퇴근 관리 기기를 도입하는 경우도 늘어나고 있다. 해외에서는 인공지능과 얼굴인식 기술을 활용해 용의자 추적 목적으로 일반 시민의 얼굴을 스캔하고 운전면허 데이터베이스의 사진과 대조하는 등 범죄수사 목적으로 활용하고 있어 논란이 커지고 있다. 이러한 생체인식정보는 암호와 같이 외울 필요도 없고 스마트카드와 같이 분실할 우려도 없기 때문에 일상생활에서 보안 목적으로 많이 도입되고 있지만, 우리 몸의 특징을 활용한다는 점에서 인권 침해의 우려를 불러일으킨다.

생체인식정보는 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적·생리적·행동적 특징에 관한 정보로서 특정 개인을 인증·식별하기 위해 일정한 기술적 수단을 통해 처리되는 정보를 의미한다.[23] 이러한 생체인식정보는 몇 가지 특성을 가지고 있는데, 우선 대부분의 사람들이 가지고 있는 특징이라는 점이다(보편성). 대다수 사람들이 가지고 있는 특징이 아니라면 식별이나 인증을 목적으로 활용되기 힘들 것이다. 둘째는 다른 사람과 구별되는, 특정 개인에게 고유한

정보이다(고유성). 셋째 평생 변하지 않는 속성을 가지고 있다(영구성). 지문이 지워지는 것과 같은 예외적인 경우가 있지만, 대체적으로는 영구적인 속성을 가지고 있다.

이러한 특성 때문에 생체인식정보가 개인의 프라이버시에 미치는 영향은 치명적일 수 있다. 비밀번호나 신용카드는 유출이 되면 바꿀 수 있지만 생체인식정보는 유출이 되어도 바꿀 수 없다. 한번 유출되면 그 피해를 복구하는 것이 거의 불가능할 수 있다. 나아가 생체인식정보는 나도 모르게 수집될 수 있는 위험도 증가한다. 예를 들어 먼 거리에서 정보주체가 인식하지 못하는 사이에 영상장치로 촬영하고 홍채나 얼굴인식정보를 추출할 수도 있고, 컵과 같은 물건에서 지문과 유전자 정보를 채취할 수도 있다. 생체인식정보를 통해 나의 일거수일투족이 감시, 추적될 위험성이 있는 것이다.

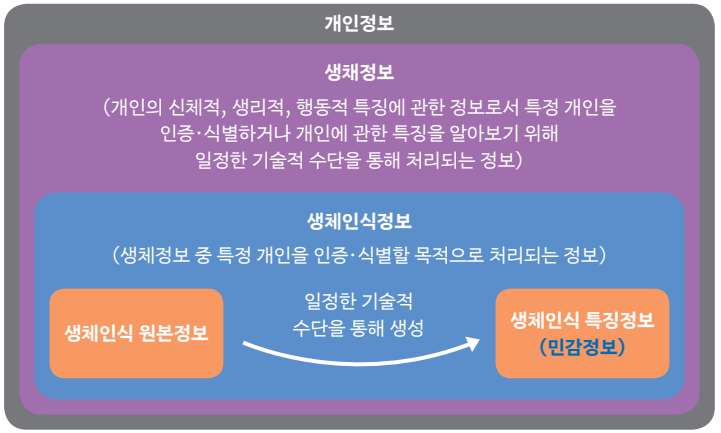
2) 생체인식정보 처리 관련 규율

생체인식정보는 전 세계적으로 민감정보로서 특별한 보호를 받는다. 우리나라는 2020년 개인정보보호법 시행령 개정을 통해 생체인식정보를 민감정보로 인정하였다. 민감정보를 처리하기 위해서는 법령에서 민감정보의 처리를 허용하거나, 정보주체로부터 별도의 동의를 받아야 한다.

개인정보보호위원회는 2021년 9월, 생체인식정보의 안전한 활용기반의 조성을 목적으로 「생체정보 보호 가이드라인」을 발간하였다. 이 가이드라인은 생체정보 중 특정 개인을 인증·식별하기 위한 것, 즉 지문,홍채, 얼굴 등에서 추출한 특징점 등을 이용하여 특정 개인임을 확인하려는 목적의 정보를 생체인식정보로 규정하고 있다. 여기서 인증이란 "이용권한이 있는 특정 개인임을 확인하기 위하여 이용자가 입력한 생체정보를 기기 등에 저장된 정보와 대조하여 본인 여부를 확인"하는 것을 의미하며, 식별이란 "개인의 생체정보를 데이터베이스에 저장된 다수의 생체정보와 대조하여 여러 사람 중 특정 개인을 구분하여 확인"하는 것을 의미한다. 예를 들어 생체인식 출입통제 시스템에서 특정 방문자의 지문과 등록된 지문을 비교하여 정당한 출입 권한이 있음을 확인하는 것이 인증이라면, 길거리 CCTV에 찍힌 특정인을 운전면허 데이터베이스와 비교하여 누구인지 확인하는 것이 식별이라고 할 수 있다.

사람의 연령.성별.감정 등의 상태를 확인 또는 분류하기 위한 용도로 활용하기 위한 생체정보는 생체인식정보가 아니다. 예를 들어 어떤 앱이 안면인식을 통해 특정 연령이나 성별을 분류하는 기능을 한다면 이는 생체정보를 활용하는 것이기는 하지만 생체인식정보의 활용은 아니다. 블로그에 올린 인물 사진 역시 개인정보이기는 하지만 생체인식정보는 아니다. 여기서 생체인식정보인지 여부가 중요한 것은 이에 따라 개인정보보호법의 적용이 달라지기 때문이다. 기업 내에서는 주로 출입통제나 권한 확인 등 인증 목적으로 활용하기 때문에 생체인식정보로 간주할 수 있고 개인정보보호

개인정보, 생체정보, 생체인식정보의 관계

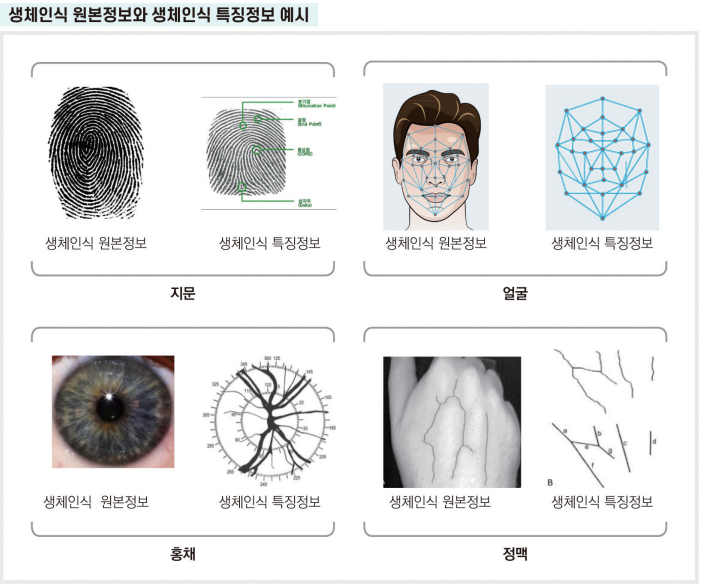


출처: 「생체정보 보호 가이드라인」

법상 민감정보로 규율된다.

생체인식정보는 '원본정보'와 '특징정보'로 구분된다. 원본정보는 인증 또는 목적으로 입력장치 등을 통해 수집·입력되는 정보이고 이로부터 특징점을 추출하는 등의 일정한 기술적 수단을 통해 생성되는 정보를 특징정보라고 한다. 가이드라인은 원본정보는 생체인식정보를 전자적으로 처리하는 과정에서 유출되거나 오·남용되는 경우 개인정보 침해 위험성이 크므로, 원본정보의 안전한 보관을 위해 저장시 암호화, 원본정보를 특징정보 생성 후에도 보관하는 경우 다른 개인정보와 분리 보관 등 별도의 보호조치를 할 것을 권고하고 있다. 물론 일반적으로 특징정보가 생성되면 원본정보의 수집.이용 목적이 달성된 것이므로, 특징정보 생성 후 원본정보

생체인식 원본정보와 특징정보의 예시



※ 출처 : scienceDirect.com

출처: 「생체정보 보호 가이드라인」에서 재인용

를 지체없이 파기하는 것이 원칙이다. 원본정보가 남아 있을 경우 또 다른 목적으로 남용될 가능성이 있기 때문이다.

기업 내에서 출입통제 목적으로 생체인식정보 시스템을 도입한다면, 우선 전 직원을 대상으로 생체정보를 수집한 후 특징정보를 추출하여 데이터베이스를 구축할 것이다. 이후 직원들이 자신의 지문, 얼굴 등을 인식시키면 이로부터 특징점을 찾아내 데이터베이스에 기록된 정보와 비교하여 정당한 권한을 가진 사람인지 판단하게 된다. 이때 특징정보를 추출할 때 사용한 원본정보는 삭제하도록 할 필요가 있다.

개인정보보호위원회가 중앙행정기관으로서 권한이 확대된 것과 생체인식정보가 민감정보로 인정된 것은 모두 2020년에 들어서이다. 그 이전에 생체인식 기술의 도입이나 노동감시와 관련한 민원은 국가인권위원회에 주로 제기되었다. 국가인권위원회에 접수된 생체인식 관련 진정은 대부분 지문인식과 관련된 사건이다. 이러한 진정 사건에 대해 국가인권위원회는 생체인식정보의 인권침해성을 고려하여 대체수단을 마련할 것과 정보주체의 개별 동의를 얻을 것 등의 조치를 마련할 것을 권고하고 있다.

> 〔사례〕 출퇴근 지문인식기 관련 국가인권위원회의 결정
>
> **– 국가인권위원회 침해구제 제2위원회 결정 – 19진정0262600 사건**
>
> A시에서 운영하는 한 도서관에서 지문인식을 이용한 출퇴근 관리를 시행했다. 해당 시는 초과근무수당 부당운영 등의 문제를 겪고 있었고 이를 해결하기 위한 한 방편으로 기존 수기대장에서 복무관리시스템을 활용하는 것으로 변경하였고 이와 함께 지문인식기를 설치하여 운영하고 있었다. 지문인식기 외에 대체수단은 없는 상황이었고, 물리적으로 지문인식이 불가능한 경우에만 아이디와 패스워드를 이용한 근태관리를 진행했다. 이에 국가인권위원회는 개인의 권리에 대해 제대로 고지하지도 않았고, 대체방안도 마련하지 않은 채 지문인식기를 활용하여 직원들의 지문정보를 수집, 활용한 것은 사실상 지문등록을 강요한 것이라 할 수 있으며 개인정보자기결정권을 침해한 것으로 판단된다고 결정했다.

3) 생체인식정보의 수집에 대한 노동자의 대응 방안

①「생체정보 보호 가이드라인」에서도 권고하고 있다시피, 생체인식정보는 개인정보 침해 위험성이 크기 때문에 처리 목적을 달성할 수 있는 다른 수단이 있는지 사전에 검토할 필요가 있다. 생체인식 시스템을 도입할 경우에도, 생체인식정보마다 특성과 위험성이 다르기 때문에, 활용 목적을 달성하면서도 침해 위험성을 최소화할 수 있는 생체인식정보를 선택한다. 예를 들어 단지 출퇴근 시간을 확인하려는 목적으로 생체인식 시스템을 도입하는 것은 생체인식정보의 위험성 및 다른 대체수단이 많이 있음을 고려할 때, 도입하지 않는 것이 바람직하다.

② 생체인식정보 시스템의 도입 단계부터 개인정보보호 중심 설계 원칙을 적용하여 생체인식정보 처리의 모든 과정에서 예상되는 개인정보 침해위험 요인을 사전에 분석하고 예방 조치를 취하도록 요구해야 한다. 개인정보보호 중심 설계Privacy by Design, PbD란 제품·서비스 개발 시 기획 단계부터 개인정보 처리의 전체 생애주기에 걸쳐 이용자의 프라이버시를 고려한 정책을 적용하여 설계에 반영하는 것을 의미한다. 직장 내에서 생체인식정보 시스템을 도입할 경우, 자체적으로 시스템을 개발하기보다는 시장에 출시된 제품을 구매하는 경우가 많을 것이다. 그러나 실제 생체인식정보를 수집·운영하는 곳은 그것을 구매한 기업이기 때문에, 목적 달성을 위해 생체인식정보 시스템이 필요한지, 필요하다면 어떠한 생체인식정보를 수집할 것인지, 생체인식정보 수집의 법적 근거는 무엇인지, 위험성을 최소화하기 위한 안전조치는

어떻게 취할 것인지 등에 대해 사전 분석이 필요하다.

③ 생체인식정보 시스템을 도입하더라도 다른 불가피한 목적이 있는 것이 아니라면, 특징정보 추출 후 원본정보는 삭제하도록 해야 한다.

④ 생체인식정보 시스템을 도입하더라도 출입카드나 수기명부와 같은 대체수단이 반드시 마련되어야 한다. 설사 노동조합 차원에서 생체인식정보 시스템 도입에 동의했다고 하더라도, 생체인식정보의 제공을 원하지 않는 노동자에게 최소한의 선택권을 제공할 필요가 있다. 또한 때로는 지문이 손상되는 등 생체인식을 사용할 수 없는 경우도 있기 때문에 대체수단의 마련이 필요하다.

⑤ 생체인식정보는 매우 민감한 정보이기 때문에, 생체인식정보 시스템의 도입 전에 개인정보 영향평가를 수행할 필요가 있다. 수집되는 개인정보의 양이 많은 경우, 인공지능 등 신기술과 결합할 경우에는 더욱 필요하다. 또한 생체인식정보를 단말기 내에서 처리하는 것보다 중앙 서버에 전송하여 처리하는 경우 위험성이 더욱 커지기 때문에, 개인정보 영향평가를 통해 침해 요인을 분석하고 안전조치를 마련할 필요가 있다. 국내 개인정보보호법은 공공기관의 경우 일정한 요건을 갖춘 개인정보 처리에 대해 영향평가를 의무화하고 있으며, 민간기업 등 공공기관 외의 경우에도 개인정보 처리의 위험성이 높을 경우 영향평가를 수행할 것을 권고하고 있다.

⑥ 생체인식정보는 민감정보이기 때문에, 다른 공공적 필요에 따라 법령에서 생체인식정보 수집을 허용하는 경우가 아니라면, 대부분 직장 내에서 생체인식정보를 수집하는 경우 정보주체의 '별도의 동의'를 받아야 한다. 즉, 시설 보안 등 개인정보처리자의 정당한 이익이 있다고 정보주체인 노동자의 동의 없이 도입할 수 없으며, 이는 개인정보보호법 위반이 된다. 노동자의 동의는 다른 개인정보에 대한 동의와 별도로 받아야 하며, 당연히 이 동의는 강제되어서는 안 된다.

7. 노동자 소셜 미디어 정보의 수집

1) 개요

소셜 미디어 활용이 기하급수적으로 늘어나면서 직장 내에서 소셜 미디어를 둘러싼 갈등도 증가하고 있다. 소셜 미디어는 그 특성상 완전히 사적인 공간이라고도, 혹은 공적인 공간이라고도 정의하기 힘들다. 이용자의 설정에 따라 상당히 많은 정보들이 공개적으로 접근 가능할 수도 있다. 기업이 노동자의 소셜 미디어 활용을 모니터링하는 명분은 기업 이미지 훼손, 기밀 정보의 유출, 직원의 생산성 등이다. 이에 일부 기업들은 회사 내규에 소셜 미디어 가이드라인을 만들어 직원에게 이를 지킬 것을 요구하기도 한다. 최근 몇년 간 기업이 직원의 소셜 미디어를 확인하고 소셜 미디어 게시물을 근거로 징계나 해고를 하는 등의 사건이 발생하기도 했다. 입사

지원자들의 소셜 미디어를 미리 살펴보고 이를 채용 결정에 참고하기도 하는데, 2018년 한 기사에 따르면 대다수의 인사 담당자가 "지원자의 SNS 내용 및 SNS 활용 능력을 검토"한다고 밝혔다.[24]

그러나 업무 목적으로 소셜 미디어를 활용하는 것이 아니라면 이는 업무 외의 개인적인 활동에 속한 것이므로, 소셜 미디어 활동을 모니터링하는 것은 노동자의 프라이버시를 심각하게 침해할 수 있다. 소셜 미디어에는 해당 개인의 기본적인 개인정보뿐만 아니라, 다른 사람과의 관계, 취향, 정치적 견해, 건강 상태, 이동 기록 등 매우 다양하고 민감한 정보들이 포함될 수 있기 때문이다. 또한 기업이 개인의 소셜 미디어를 검열한다는 사실을 안 노동자들은 소셜 미디어 활용이 위축되거나 급기야 계정을 삭제하는 경우도 종종 발생하는데, 이는 노동자의 표현의 자유를 침해하는 것이다.

2) 소셜 미디어 정보 수집에 대한 규율

노동자의 소셜 미디어 프로파일이나 내용 역시 개인정보이며, 따라서 개인정보보호법에 따라 처리되어야 한다. 소셜 미디어를 업무 상 활용하는 것이 아니라면, 사용자가 노동자의 소셜 미디어를 모니터링하고 관련 정보를 수집해야 할 정당한 이유는 없다. 다만, 소셜 미디어를 통해 공개한 내용과 관련하여 향후에 명예훼손이나 영업비밀 유출 등 법적 분쟁이 발생하는 것은 별개의 문제이다.

채용 단계에서 지원자의 소셜 미디어 정보를 살펴보는 것은 일정하게 허용될 수도 있다. 이와 관련하여 「개인정보보호 가이드라인(인사·노무편)」은 소셜 미디어를 직접적으로 언급하고 있는 것은 아니지만, 해킹 등 부정한 방법을 사용하는 것이 아닌 이상, 인터넷을 통해 지원자의 공개된 개인정보를 당사자의 동의 없이 수집할 수 있다고 하고 있다.

> **Q. 1-6 입사지원자의 논문, 저서 등의 정보를 인터넷을 통해 수집하려고 하는데 동의가 필요한가요?**
>
> 답변) 불특정 다수가 열람할 수 있는 사이트 등에 공개된 개인정보의 수집·이용에 대해서는 동의를 받을 필요 없습니다.
>
> - 언론, 온라인 도서관, 인물DB 등 정당한 절차에 따라 개인정보를 공개하는 웹사이트에서 개인정보를 수집·이용하는 것은 동의가 필요하지 않습니다.
> - 그 경우에도 해킹 등 부당한 방법으로 수집하여 공개한 개인정보임이 확실시되는 경우에는 수집·이용할 수 없습니다.
>
> ※ 관련규정 : 표준 개인정보보호 지침 제6조(개인정보의 수집) 제4항
> 개인정보 보호법 제59조(금지행위) 제2호, 제3호, 위반 시 5년 이하 징역 또는 5천만원 이하 벌금

그러나 채용 과정에서 소셜 미디어 정보를 수집한다는 사실은 지원자에게 공개되어야 한다. 「개인정보보호 가이드라인(인사·노무편)」에서도 "본인으로부터 직접 개인정보를 수집하는 것이 원칙이며, 제3자로부터 제공받는 것이 불가피한 경우 관련 정보주체로부터 내용(출처, 수집 내용 등)을 알려주어야 함"이라고 하고 있다. 그리고 채용 여부가 결정된

즉시 관련 내용을 삭제해야 한다.

채용 후에 노동자의 소셜 미디어 정보를 항상적으로 모니터링하는 것은 정당화될 수 없다. 이와 관련하여 유럽연합의 의견서에서도 "일반적으로 고용 중에는 노동자의 소셜 미디어 정보의 모니터링이 발생해서는 안" 되며, 또한 사용자가 소셜 미디어에 접근하게 해달라고 요청해서도 안 된다고 하고 있다. 다만 사용자가 사직한 근로자의 '경업금지(Non-compee clause) 조항'(일정기간동안 경쟁관계에 있는 동일계열 회사에 취업하지 않겠다는 약속) 기간 동안, 계약 준수 여부를 확인하기 위해 당사자의 링크드인을 모니터링하는 것은 인정하고 있다. 물론 이에 대해 당사자는 모니터링의 범위에 대해 적절하게 고지를 받아야 한다.

3) 소셜 미디어 정보 수집에 대한 노동자의 대응 방안

① 지원자의 소셜 미디어 정보는 업무 역량 평가에 필요한 최소한의 한도 내에서 수집되어야 하며, 이와 관련한 사실이 당사자에게 고지되어야 한다. 노동자와 노동조합은 회사가 입사 지원자의 개인정보까지 보호하는 원칙을 수립하도록 노력해야 한다.

② 노동자의 소셜 미디어 내용을 일상적으로 모니터링하는 것은 허용되어서는 안 된다. 노동자와 노동조합은 회사가 이러한 정책을 가지고 있다면 즉시 이 정책을 폐기할 것을 요구해야 한다. 이러한 맥락에서 노동자에게 소셜 미디어 계정 정보를 요구하는 것도 허용해서는 안 되며, 이를 거부해야 한다.

③ 명백하게 불법적인 행위가 아니라면, 노동자의 소셜 미디어 내용이 징계에 대한 근거로 사용되어서는 안 된다.

> **〔사례〕 인터넷 게시글을 근거로 한 MBC PD의 해고와 무효판결**
>
> MBC에 재직중인 권성민 PD는 지난 2014년 MBC의 '세월호 보도 참사'와 관련해 개인적 사과를 인터넷 사이트 '오늘의 유머' 게시판에 올렸다는 이유로 정직 6개월의 정직 처분을 당했다. 이후 소송을 통해 일부 복권되었지만 정직 기간이 끝난후 권성민 PD를 경인지사 수원총국으로 발령냈다. 권성민 PD는 이와 관련한 이야기들을 웹툰으로 만들어 자신의 SNS에 게시했다. MBC는 이를 이유로 권성민 PD를 해고하기에 이르렀다. 당시 MBC는 권성민 PD가 "자신의 주장만이 옳고 정당하다는 미성숙함과 오만에 빠져 상대가 누구든 닥치는 대로 비난하고 모욕을 줬다"며 "기형적으로 난 떡잎은 잘라내야 잡초로 자라지 않고, 피를 뽑아 줘야 벼가 잘 자라듯 자성의 기회를 줬음에도 반복적인 해사 행위를 좌시할 수 없다"고 판단했다며 해고 사유를 설명했다.
>
> 권성민 PD가 자신의 이야기를 SNS에 웹툰으로 그려 발행한 것에 대해 '해사 행위'로 규정하고 해고 절차를 감행한 것이다. 이후 이어진 복직 소송에서 각 1, 2, 3심 재판부는 모두 권성민 PD의 손을 들어줬다. 사측은 "사내 '소셜미디어 가이드라인'을 위반했다"며 "충분한 해고 사유"라고 주장했지만, 법원은 "해당 웹툰이 MBC(피고)의 명예를 훼손시켰다고 인정하기에 부족"한 것은 물론 "전보발령과 해고는 모두 무효임을 확인한다"고 판결했다.[25]

8. 기타 감시설비에 대한 대응

앞서 설명한 감시설비 외에도 다양한 감시설비가 있고 앞으로도 기술 발전에 따라 새로운 기기가 도입될 것이다. 예를 들어 스마트카드 역시 직장 내에 많이 도입되어 있고, 스마트카드의 형태와 기능 역시 다양하다. 사원증이나 신용카드와 결합되는 경우도 있고, 물리적인 카드에서 모바일 형태로 진화하고 있기도 하다. 그러나 노동감시 측면에서는 스마트카드의 형태가 어떠한지 상관없이 어떠한 개인정보가 어떠한 방식으로 처리되는지에 주목할 필요가 있다. 그리고 앞서 살펴 본 개인정보, 위치정보, 생체정보 등의 처리에 대한 대응 방안을 참고하여 대응할 수 있다.

전사적 자원관리Enterprise Resource Planning, ERP 시스템 역시 마찬가지다. ERP는 경영, 인사, 재무, 생산 등 기업 내의 모든 인적, 물적 자원과 관련된 정보의 흐름을 통합적으로 관리하는 시스템을 의미한다. 아마도 대다수의 기업들이 다양한 형태의 ERP 시스템을 보유하고 있을 것이다. 이는 경영 정보 시스템의 하나이고 노동감시 자체를 목적으로 하는 것은 아니지만, 업무 효율성을 위해 노동자의 개인정보 역시 처리하기 때문에 노동감시의 목적으로도 활용될 수 있다. ERP 시스템 자체가 제품에 따라 다양한 구성과 기능을 가지고 있으며, 앞서 설명한 기능들, 예를 들어 생체인식 근태관리 시스템이나 위치정보 수집, 인터넷 모니터링 등의 기능들을 포함하거나 혹은 연계되어 있을 수 있다. 따라서 ERP 시스템에 대한 대응 역시 노동자의 정보를 어떻게 수집, 처리하는지 주목할 필요가 있다. 특히 이렇게 노동 통제나 감시와 직접적인 관련이 없는 복합적인 시스템일수록 그 기능이 감추어져 있고, 노동자에 미치는 영향을 파악하기 힘들 수 있다. 따라서 어떠한 시스템이 도입되든 노동자 및 노동조합에 관련된 정보를 투명하게 공개할 것을 요구할 필요가 있다. 최소한 조금이라도 개인정보의 수집이 이루어지는 경우, 사용자는 개인정보의 처리에 대해 투명하게 공개할 의무가 있다.

5장

신기술과 노동감시

1. 플랫폼과 노동감시

1) 플랫폼 노동의 특성

음식 배달 플랫폼인 배달의민족, 운송 플랫폼인 우버와 타다, 전자상거래 플랫폼인 쿠팡, 영상 콘텐츠 플랫폼인 넷플릭스 등등…… 사람들 사이의 소통과 관계 형성에서부터 상품과 서비스의 거래에 이르기까지 플랫폼을 매개로 해서 이루어지고 있다. 물론 구글, 페이스북, 네이버, 카카오 등도 다양한 서비스를 제공하는 종합 플랫폼이다. 플랫폼은 사람과 사람, 물건과 물건을 매끄럽게 연결해주며 편리함을 제공한다. 하지만 플랫폼이 각 부문의 소통, 중개, 거래를 독과점하고 권력화하면서 다양한 사회 문제들이 제기되고 있다. 플랫폼의 독점력 남용으로 인한 중소업체의 붕괴와 공정경쟁의 훼손, 소비자 권리의 침해, 과도한 개인정보의 수집과 남용 등이 그것이다. 플랫폼 노동자의 정당한 권리 보장 문제도 새롭게 제기되고 있는 이슈 중의 하나다.

플랫폼을 통해 노동도 매개된다. 배달 노동, 유튜버의 창작 노동, 온라인으로 데이터 가공 작업을 하는 크라우드 워크와 같이 노동의 형태는 다양하다. 그러나 노동감시 측면에서 보았을 때 플랫폼 노동은 몇 가지 특성을 가지고 있다. 앞 장에서 다양한 감시설비별 대응 방안에 대해 설명하였지만, 플랫폼은 그 자체로 감시 시스템이다. 왜냐하면 플랫폼은 그 위에서 이루어지는 모든 소통과 거래의 데이터화를 전제하고 있기 때문이다. 데이터를 생산, 축적, 분석할 수 있는 역량이 플랫폼의 힘이다. 플랫폼 노동자이든 이용자이든, 아니면 플랫폼에 기대 사업을 하는 사업자이든, 이들의 모든 활동이 플랫폼에 기록되고 언제든 모니터링될 수 있다. 택시나 배달 서비스와 같이 모든 노동 과정 자체가 통제되는 경우도 있다. 전통적인 노동과 달리 플랫폼 노동은 특정한 작업장에 한정되지 않는다. 노동은 특정 업체 내에서뿐만 아니라, 거리와 카페에서, 혹은 노동자의 집에서 이루어질 수 있다. 플랫폼을 통한 노동감시 역시 특정 사업장에 국한되지 않으며, 언제 어디에서나 이루어질 수 있다.

플랫폼을 통해 수집된 데이터는 모종의 알고리즘을 통해 플랫폼 노동자에게 영향을 미칠 수 있는 여러 결정을 내리는 데 활용된다. 배달 노동자의 업무가 인공지능AI 알고리즘에 의해 배당되듯이, 누가 어떤 일을 할 것인지를 알고리즘이 결정한다. 해당 노동자가 과거에 성실하게 업무를 수행했는지, 작업 지시에 대한 거부는 없었는지, 업무 성과에 대한 소비자의 평가는 어떠했는지 등도 플랫폼 노동자에 대한 평가와 향후 업무 배당에 영향을 미친다. 그러나 정작 영향을 받는 노

동자들은 알고리즘이 어떻게 작동하는지 알 수 없다.

> **〔사례〕 인공지능 배차는 효율적인가**
>
> 2021년 6월 29일, 라이더유니온은 기자회견을 열어 배달의민족·요기요·쿠팡이츠 플랫폼 3사 AI 알고리즘 검증 실태조사 결과를 발표하였다. 이들은 3일 동안 11명의 라이더가 서울과 부산에서 AI 배차를 100% 수락했을 때, 평소대로 운행했을 때, 교통법규를 준수했을 때 어떠한 차이가 발생하는지 비교·분석하였다. 분석결과에 따르면, AI 배차 시스템에 따라 배달을 한 경우 업무효율이 떨어졌으며 오히려 주행거리가 늘어나 노동강도는 높아지고 수입은 줄어들었다고 한다.
>
> 그러나 라이더는 AI의 요구를 수락하지 않을 경우 불이익을 당할 수 있다. 검증에 참여한 쿠팡이츠 라이더는 둘째 날 자율적으로 거절하면서 배달했다가 계정정지를 당했고, 요기요 라이더는 95% 수락율을 유지하지 않으면 배달 한 건당 1,000원 마이너스, 등급하락 등 불이익을 받는다. 배민의 경우 과도한 거절시 다음에 배차가 지연될 수 있음을 경고한다고 한다. 라이더유니온은 AI 알고리즘이 효율적이지도 안정적이지 않은데도 불구하고, 이를 거절하는 것에 대해 불이익을 주는 것은 부당하다고 주장하였다. 또한 교통법규를 모두 지키면서 배달할 경우 한 건 당 약 30분이 소요되었고, 수익이 3분의 1 내지 2분의 1로 줄었다고 한다. 즉, 이는 교통단속만으로는 해결되지 않는 산업의 문제이자 산업안전보건의 문제라는 것이다.[26]

2) 플랫폼 노동감시에 대한 대응 방안

① 기업들은 플랫폼 노동을 원하는 시간에 원하는 만큼 할 수 있는 자유롭고 독립적인 노동으로 홍보한다. 이는 이전과 동일한 노동을 하면서도 노동자로서의 임금과 권리를 보장받지 못하는 현실을 은폐한다. 그래서 현재 플랫폼을 기반으로 일하는 사람들이 노동자로 인정받기 위한 싸움이 전 세계적으로 벌어지고 있고, 여러 국가에서 일정한 요건을 갖춘 경우 노동자로서의 권리를 인정하고 있다. 이는 노동감시의 맥락에서도 중요한데, 지금까지 살펴본 바와 같이 취약한 위치에 있는 노동자의 특성을 고려할 때 노동감시에 대응하기 위해서는 집단적으로 대응할 필요가 있기 때문이다. 현재 근로기준법에 노동감시와 관련한 명시적인 조항은 없지만, 노동조합을 통해 감시설비의 도입 여부 및 요건에 대한 단체협상을 진행할 수 있고, 많은 한계에도 불구하고 근로자참여법에서 감시설비의 도입을 노사협의회의 의제로 포함하고 있다. 그러나 노동자로 인정받지 못할 경우 노동조합 혹은 노사협의회 등을 통한 협의가 어려워지게 된다. 따라서 노동감시에 대한 대응의 맥락에서도 플랫폼 노동자들이 노동자로서의 지위를 인정받는 것이 중요하다.

> **플랫폼 노동자 보호를 위한 법적 규율**
>
> 정부는 플랫폼 노동자 보호를 명분으로 2021년 3월, 더불어민주당 장철민 의원의 대표발의로 '플랫폼 종사자 보호 및 지원 등에 관한 법률안(플랫폼 종사자 보호법)'을 발의하였다. 이 법은 플랫폼을 통해 중개 또는 알선 받은 노무를 제공하기 위하여 주로 자신의 노무를 제공하고 그 대가로 보수 등을 받는 사람을 '플랫폼 종사자'로 규정하고, 플랫폼을 운영하는 '플랫폼 운영자', 중간 관리업체인 '플랫폼 이용 사업자'가 플랫폼 종사자에 대해 갖는 책임과 의무를 규정하고 있다. 이에는 개인정보 보호나 분쟁해결 노력, 플랫폼과 관련한 정보제공의 의무 등이 포함된다.
>
> 그러나 노동계는 플랫폼 종사자 보호법에 반대하고 있다. 노동관계법에

따라 노동자로서 보호하는 것이 아니라 플랫폼 종사자라는 별도의 개념을 신설하는 것은 오히려 노동자로서의 권리를 박탈하는 것이기 때문이다. 노동계의 입장은 플랫폼 노동과 같은 다변화하는 고용형태를 반영할 수 있도록 기존 노동관계법을 적용 혹은 개정하라는 것이다. 또한, 플랫폼의 알고리즘 등 정보제공 의무와 관련해서도, 플랫폼 종사자 보호법은 플랫폼이 영업 비밀을 명분으로 공개하지 않을 경우 이를 제재할 방법이 없다는 한계가 있다.

② 노동자로서의 지위를 인정받든 아니든, 플랫폼의 개인정보 수집에 대해서는 여전히 개인정보보호법이 적용된다. 플랫폼을 통한 개인정보의 수집과 처리도 개인정보 보호원칙을 준수해야 하고 적법한 요건을 갖추어야 하며, 플랫폼 노동자 역시 정보주체로서의 권리를 보장받아야 한다. 3장과 4장에서 설명한 대응의 원칙과 방안이 플랫폼에 대해서도 거의 대부분 적용된다. 플랫폼 노동자의 개인정보 수집 문제 뿐만 아니라, 플랫폼을 통한 과도하고 불투명한 개인정보 처리 문제에 대해서도 사회적으로 대응할 필요가 있다.

③ 플랫폼 노동자에 대한 노동통제와 감시라는 맥락에서도 플랫폼 알고리즘의 투명성은 매우 중요하다. 자신의 노동과 그 대가가 어떠한 요소와 로직에 의해서 영향을 받는지 알아야 자신이 플랫폼과 공정한 관계를 맺고 있는지, 부당한 처우를 받고 있지는 않은지 판단할 수 있기 때문이다. 플랫폼에 노동자에게 영향을 미치는 관련 자료, 알고리즘 주요 요소와 로직에 대한 공개를 요구해야 한다. 또한 알고리즘 투명성을 의무화하는 법제 개선에 힘을 모을 필요가 있다.

알고리즘 투명성에 대한 요구

플랫폼 알고리즘에 대한 투명성 요구는 여러 측면에서 제기되고 있다. 네이버 뉴스 알고리즘 논란, 미국의 대선에 영향을 미쳤던 페이스북 – 케임브리지 애널리티카 사건과 같이, 플랫폼 알고리즘의 투명성과 공정성은 한 사회의 정치적 여론 형성이나 선거 등 민주주의 체제에 영향을 미칠 수 있다. 또한 빅테크 플랫폼의 자사 상품 선호 논란과 같이 공정한 경쟁을 위해 플랫폼의 알고리즘 투명성을 요구하기도 한다. 마지막으로 플랫폼의 알고리즘을 비롯한 인공지능 알고리즘은 다양한 개인정보를 기반으로 개인의 특성이나 행동을 분석·예측하는 프로파일링을 수행하고, 개인들에게 중대한 영향을 미치는 결정을 자동으로 수행하는 경우가 많아지고 있다. 인공지능 시스템을 통해 자동화된 채용, 대출 심사, 복지 혜택 등이 그러한 사례들이다. 인공지능 알고리즘이 야기할 수 있는 차별과 프라이버시 침해로부터 개인의 기본권을 보호할 필요성이 커지고 있다. 이에 대해서는 2절에서 좀 더 자세하게 설명하기로 한다.

2. 인공지능과 노동감시

1) 인공지능의 문제점

번역 서비스에서부터 뉴스 콘텐츠 추천까지, 인공지능 스피커에서 범죄수사 목적의 얼굴인식까지...알게 모르게 우리 사회 곳곳에 인공지능이 도입되고 있다. 인공지능을 통한 직원 채용, 플랫폼에서의 업무 할당 알고리즘, 시장 예측과 직장 내 의사결정 지원도구 등 고용과 노동 과정에서도 인공지능의 활용이 증가하고 있다.

인공지능은 여러 편의와 효율성을 제공할 수 있음에도 불구하고 인공지능의 개발 및 활용 과정에서 인권 침해의 우려가 제기되어 왔으며 노동자에 대해서도 예외가 아니다. 앞서 플랫폼 노동에서 언급했다시피, 알고리즘을 통한 업무 배분, 노동 과정에 대한 모니터링, 성과에 대한 평가와 관리 등은 노동자에게 상당한 스트레스를 유발할 수 있다. 인공지능과 알고리즘의 편향과 그에 따른 차별도 문제로 제기되고 있다. 이는 인공지능 학습에 이용된 데이터의 편향에 기인할 수도 있고 프로그램머의 개인적, 집단적 편견을 반영한 것일 수도 있다. 학습 데이터가 기존의 현실을 그대로 반영한 것일지라도 불평등하고 차별적인 현실을 고착시킨다는 비판을 면하기 힘들다. 인공지능과 알고리즘의 이러한 위험성은 채용 과정에서 성별, 연령, 지역 등에 따른 차별을 야기할 수 있고, 노동자의 성과 평가에 사용될 경우 그 공정성을 신뢰하기 힘들게 한다.

가장 큰 문제는 알고리즘의 작동방식이 투명하지 않다는 것이다. 알고리즘의 불투명성은 공공부문에서는 공공기관의 책임성 문제를 야기할 수 있다. 공공기관은 자신이 내린 어떠한 결정에 대해 국민들에게 그 근거를 설명할 의무가 있는데 이를 충족할 수 없는 것이다. 또한 인공지능 알고리즘의 결정에 따라 신체적, 재산적, 법적으로 커다란 부정적 영향을 받은 사람이 그 이유를 알 수 없다면, 자신이 부당하다고 생각하는 결정에 대해 이의제기를 하기 힘들어질 것이다. 인공지능 면접에서 탈락했거나 플랫폼으로부터 부정적인 평가를 받아도 그 이유도 모르고 받아들일 수밖에 없는 것이다.

> **〔사례〕 불투명한 인공지능 채용 절차**
>
> 2019년 한국경제연구원 조사에 따르면 인공지능을 활용한 채용을 이미 진행하고 있는 기업이 11.4%, 계획이 있는 기업이 10.7%였다.[27] 공공기관의 경우 2020년 최소 20여 곳 이상에서 채용 절차에 인공지능을 도입하였다. 그런데 시민사회단체들이 13개 공공기관에 정보공개를 청구한 바에 따르면, 대부분의 기관들이 관련 자료에 대해 비공개 하였는데, 일부 기관은 "AI면접 관련 자료관리 및 운영은 용역사에서 수행하므로 당사는 요청한 자료가 없다", "AI면접 관련 사항은 업체에 일임하고 있으니 업체로 문의하라" 고 답변하였다. 공공기관이 민간의 인공지능 시스템을 도입하면서도 인공지능 도입의 원칙과 절차조차 마련되어 있지 않음이 드러난 것이다.[28]
>
> 또한, 국회 국정감사 자료에 따르면 공공기관 인공지능 면접 평가와 사람 면접관의 평가가 판이하게 달랐던 것으로 드러났다. 또한, 민간 인공지능 제품이 불합격으로 결정한 사례에 대해서 해당 공공기관이 그 사유를 파악하지 못하고 있었다. 즉, 인공지능의 평가가 공정하고 효과적인지에 대한 검증없이 민간기업의 인공지능에 의존하고 있던 것이다. 이 인공지능 서류심사가 학력, 성별, 지역 등에 따라 지원자를 차별하지 않았는지, 인공지능 면접이 지원자의 외모, 사투리 등 발음, 표정 등에 대한 부정확하고 부당한 평가를 낳지는 않았는지 검증되거나 알려진 바가 전혀 없다.[29]

2) 인공지능과 알고리즘에 대한 노동자의 권리

국제노동기구ILO는 2019년에 발간한「일의 미래 보고서」에서 "일에 영향을 미치는 최종 선택이 알고리즘이 아니라

사람에 의해서 이뤄지도록 보장하는 '인간주도' 접근법을 지지한다"고 선언하였다. 더불어 노동자의 존엄성 보호를 위해 센서, 웨어러블 기기 및 기타 모니터링 기기를 통해 이루어지는 알고리즘 관리, 감시, 통제를 규제할 것을 촉구하였다.

2018년에 시행된 유럽연합의 개인정보보호법GDPR은 인공지능의 감시, 평가, 의사결정으로부터 노동자를 비롯한 정보주체의 권리를 보호하기 위해, 개인의 특성, 성과 등에 대한 예측이나 평가, 즉 프로파일링과 개인에게 중대한 영향을 미치는 자동화된 의사결정으로부터 정보주체를 보호하기 위한 규정을 포함하고 있다. 여기서 프로파일링이란 개인정보를 사용하여 개인의 특정 측면, 즉 업무 성과나 건강, 취향, 행태 등을 분석하거나 예측하는 것을 말한다. 예를 들어 온라인 서점에서 나의 구매 내역을 분석하여 내가 좋아할만한 신작을 추천해 주는 것, 나의 인터넷 사이트 방문 기록을 수집하여 맞춤 광고를 내보내는 것, 라이더의 이동경로와 배달건수, 평점 등을 기반으로 라이더의 성과를 측정하는 것, 이 모든 것들이 프로파일링이다.

유럽연합 개인정보보호법GDPR, 프로파일링 및 자동화된 의사결정에 대한 정보주체의 권리

유럽연합 개인정보보호법GDPR은 인공지능 등 자동화된 평가 및 의사결정에 대하여 두 가지 경우로 나누어 규율하고 있다. 첫째, GDPR은 노동자의 업무성과 등을 자동으로 평가하는 이른바 '프로파일링'에 대하여 규정하고 이를 규율하고 있다. 둘째, GDPR은 여기서 더 나아가 사람의 개입이 전혀 없는 완전 자동화 의사결정에 대하여 정보주체인 노동자가 그 대상이 되지 않을 권리를 규정하였다.

유럽연합의 프로파일링에 대한 가이드라인[30]은 프로파일링이 효율성을 증대시키고 자원을 절약하는 혜택이 있는 반면에, 개인이 프로파일링 대상이 되고 있는지 모르거나 정확히 무엇이 관여되어 있는지 이해하지 못할 수 있다는 점에서 불투명하다고 지적하였다. 또한 개인을 특정한 범주에 한정시켜 선택을 제한하고 기존의 고정관념과 사회적인 차별을 항구화할 우려도 있다. 예를 들어 편향된 현실 데이터로 학습한 검색 알고리즘이 구직자인 여성에게 남성보다 급여가 적은 직장을 추천할 수 있는 것이다.

프로파일링 역시 개인정보의 처리이므로 개인정보 보호원칙을 준수해야 한다. 더불어 정보주체인 노동자는 회사가 자신의 개인정보를 기반으로 프로파일링을 하는지, 만일 한다면 프로파일링에 영향을 미치는 요소는 무엇이며, 노동자에게 어떠한 결과를 야기하는지에 대해 사전에 설명을 들을 권리를 보장받는다. 또한 회사가 '정당한 이익'을 근거로 프로파일링을 수행하는 등 특정한 상황에 해당한다면, 노동자는 이에 대해 거부할 권리도 갖는다.

만일 프로파일링이 개인에 대해 체계적이고 광범위한 평가를 수행하고, 프로파일링에 근거한 의사결정이 법적이거나 중대한 영향을 미치는 경우 회사는 개인정보 영향평가를 의무적으로 실시해야 하며, 영향평가 결과 드러난 위험성을 최소화하기 위한 조치를 취해야 한다. 이러한 보호조치에는 프로파일링에 대해 정보주체인 노동자가 자신의 의견을 피력할 권리 및 결과에 이의를 제기할 권리 등을 보장하는 것이 포함된다.

둘째, GDPR은 ① 정보주체에게 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 의사결정이고 ② 자동화로 처리되는 의사결정을 ③ 오로지 자동화된 처리 방식에만 의존하여 이루어지는 경우를 일반적으로 금지하고 있다. 이때 '유사하게 중대한 영향'의 경우란, 법적 권리나 의무에 변화가 없더라도 '인적 개입 없이 이루어지는 전자채용' 등 개인의 상황, 행동 또는 선택에 중대하게 영향을 미치거나, 정

보주체에 지속적이거나 영구적인 영향을 미치는 경우, 또는 개인이 배제되거나 차별을 받게 되는 경우를 포함한다.
다만 계약의 체결 또는 이행을 위해 필요한 경우, 법률이 허용하는 경우, 정보주체의 명시적인 동의에 근거한 경우는 예외적으로 완전 자동화 의사결정이 허용된다. 특히 근로 계약 등 계약의 체결 또는 이행의 사유로 완전 자동화 의사결정을 실시하기 위하여는 자동화가 목적 달성에 필요한 최소한의 처리여야 하고, 동일한 목표를 달성할 수 있는 덜 침해적인 수단이 있는 경우는 해당하지 않는다. 완전 자동화 의사결정이 민감정보에 근거하여 이루어질 수 있는 경우로는 정보주체의 명시적인 동의에 의하거나, 법률에 기반한 상당한 공익상의 이유로 처리가 필요하며 정보주체를 보호 조치가 존재하는 경우뿐이다.
회사가 예외적으로 완전 자동화 의사결정을 실시하는 경우에도, 정보주체 노동자의 권리와 자유 및 정당한 이익을 보호하기 위한 보호 조치가 반드시 마련되어야 한다. 이때의 보호 조치는 프로파일링 및 완전 자동화 의사결정의 유무, 관련된 로직에 관한 구체적이고 유의미한 정보, 처리의 중대성과 이로 인해 발생할 수 있는 결과 등을 노동자에게 사전적으로 설명하고, 그에 대하여 노동자가 인적 개입을 요구할 권리, 본인의 의견을 피력할 권리, 결정에 대한 설명을 들을 권리 및 결정에 이의를 제기할 권리 등을 보장하는 것을 포함한다. 더불어 회사는 처리한 데이터셋에서 편견이 있는지 확인하고, 이를 해결할 수 있는 방법을 개발해야 한다. 또 알고리즘을 검사하고 자동화 의사결정의 정확성과 관련성을 주기적으로 검토하여 그 개선에 반영하여야 한다.

그러나 아직 국내 개인정보보호법은 이와 관련한 조항을 포함하고 있지 않다. 다만, 2021년에 개인정보보호위원회가 국회에 발의한 개인정보보호법 개정안은 관련 조항을 신설하는 내용을 담고 있다.

3) 인공지능 노동감시에 대한 대응 방안

① 인공지능의 학습과 활용, 알고리즘을 통한 프로파일링 역시 개인정보의 수집과 처리를 동반한다. 인공지능을 통한 개인정보 처리가 개인정보보호법을 준수하는지 감시할 필요가 있다.

② 노동자는 인공지능 알고리즘이 자신에게 어떠한 영향을 미치는지 알 권리가 있다. 사용자에게 노동자의 개인정보를 프로파일링하는지 여부, 관련된 로직과 영향을 미치는 주요 요소, 노동자에게 미치는 영향 등에 대해 투명하게 공개할 것을 요구해야 한다. 이러한 정보는 비전문가인 노동자가 이해할 수 있는 방식으로 쉽게 설명되어야 한다.

③ 노동자는 자신에게 부정적 영향을 미치는 인공지능에 대해 문제제기할 권리가 있다. 인공지능을 통한 자동화된 의사결정의 기준이 무엇인지 설명을 요구하고 자신의 견해를 표명할 권리를 가진다. 인공지능을 통해 어떠한 결정이 내려졌다면, 그 이유와 결정 요소들이 사후에 검증이 가능할 수 있도록 기록되어야 한다.

④ 회사가 인공지능을 개발하거나 혹은 구매할 경우, 해당 인공지능이 특정 목적 달성에 효과적인지, 공정하고 차별적이지 않은지 검증할 수 있는 절차가 마련하도록 요구한다. 인공지능의 개인정보 침해 위험을 사전에 평가할 수 있는 개인정보 영향평가, 인권에 미치는 영향을 평가할 수 있는 인권영향평가, 혹은 독립적인 기관에 의한 감사 등을 활용할 수

있다.

⑤ 인공지능을 개발하거나 구매할 때 도입의 필요성, 기능의 범위나 작동방식 등에 대해 노동조합 혹은 노동자 대표와 사전에 협의하도록 요구해야한다.

⑥ 인공지능의 도입은 노동자의 노동 과정과 권리에 커다란 영향을 미칠 수 있기 때문에, 인공지능 도입 과정에서 노동자의 권리 보호를 위한 국가적인 차원의 입법 마련도 촉구할 필요가 있다. 유럽연합 인공지능 법안에서 규정했듯이, 특정 노동자를 차별하거나 노동자의 권리에 부정적 영향을 미칠 수 있는 고위험 인공지능을 규율할 수 있는 법안이 마련될 필요가 있다. 개인정보보호법에 노동자에 대한 프로파일링과 자동화된 의사결정에 대응할 수 있는 정보주체의 권리도 포함되어야 한다.

> **유럽연합 인공지능 법안**
>
> 2021년 4월 21일 유럽 집행위원회는 "인공지능 법안"을 유럽의회에 발의하였다. 유럽연합은 이를 통해 채용, 고용, 노무 관리 등의 분야에 사용되는 인공지능에 대하여 법적 의무 부과를 추진하고 있다. 이 법안은 플랫폼 노동을 비롯하여 채용 및 고용, 노무 관리에 사용되는 인공지능을 '고위험'으로 규정하였다. 특히 인력 채용 및 선발, 승진 및 해고 결정, 근로 관련 계약 관계로 종사하는 사람에 대한 업무 할당, 모니터링 또는 평가에 사용되는 인공지능 시스템은 고위험으로 분류된다. 이러한 시스템이 사람들의 장래 직업 전망과 생계에 현저한 영향을 미칠 수 있기 때문이다. 여기서 "근로 관련 계약 관계"는 피고용 노동자 뿐만 아니라 플랫폼을 통해 서비스를 제공하는 사람들을 포함한다. (전문 36)[31]

후주

1 국가인권위원회,「사업장 전자감시로부터 근로자 정보인권 보호를 위한 제도 개선 권고」결정(2017.2).
2 헌법재판소 2005.5.26. 99헌마513 등.
3 진보네트워크센터·재단법인 공공상생연대기금,「디지털 노동감시 실태조사 및 법제도 개선방안」, 2021.
4 WP29,「사업장 개인정보 처리에 대한 의견서」(Opinion 2/2017 on data processing at work), 2017.6.8., WP249.
5 양승엽,「사업장 전자감시 규제에 관한 이론적 고찰」, 사업장 전자감시의 문제점과 제도 개선 방안 토론회(2021.9.15) 자료집, p.6.
6 김하나,「사업장 전자감시 사례 및 입법의 필요성」, 사업장 전자감시의 문제점과 제도 개선 방안 토론회(2021.9.15) 자료집, 57~58쪽.
7 개인정보보호위원회,「개인정보보호 법령 및 지침·고시 해설서」, 2020.12., 92쪽.
8 김하나,「사업장 전자감시 사례 및 입법의 필요성」, 사업장 전자감시의 문제점과 제도 개선 방안 토론회(2021.9.15) 자료집, 62~63쪽.
9 한겨레,「아마존 배달차량의 인공지능 감시 카메라 논란」, 2021.8.5.
10 김하나,「사업장 전자감시 사례 및 입법의 필요성」, 사업장 전자감시의 문제점과 제도 개선 방안 토론회(2021.9.15) 자료집, 52~53쪽.
11 경향신문,「구조조정 뒤 '명퇴 거부자 감시 CCTV' 논란…정부, 3년 만에 KT 현장 조사」, 2017.7.26.
12 개인정보보호위원회,「2015 개인정보보호 연차보고서」, 2015.8., 88쪽.
13 노동부,「최신 사례로 보는 부당노동행위: 부당노동행위 사례 및 실무」, 2009. 5., 142쪽.
14 WP29,「사업장 개인정보 처리에 대한 의견서」, p.19.
15 정보통신신문,「[이슈] 재택근무 위치정보 수집, 기본권 침해 논란」, 2020.09.21.
16 ITWORLD,「모바일 관리 솔루션 MDM, MAM, EMM, UEM의 차이」, 2017.7.11.

17 진보네트워크센터 등,「[공동논평] 노동자의 개인정보에 대한 권리 인정한 법원 판결을 환영한다!」, 2018.8.13.

18 WP29,「사업장 개인정보 처리에 대한 의견서」.

19 광주드림,「포스코, 스마트폰 감시 어플 강요」, 2014.2.14.

20 투데이신문,「현대차, 하청직원 새 출입시스템 도입 잡음…노조 "불법파견 회피·개인정보유출" 반발」, 2020.5.13.

21 매일노동뉴스,「삼성 모바일 앱으로 삼성반도체 건설노동자 실시간 감시?」, 2021.6.17.

22 한국정경신문,「"회사가 내 사생활까지"..현대중공업 'MDM' 설치 권고에 노조 강력 반발」, 2021.10.7.

23 개인정보보호위원회,「생체정보 보호 가이드라인」, 2021.

24 아시아 경제,「취준생 SNS 엿보는 기업들… 당신의 SNS 안녕하신가요」, 2018.2.6.

25 미디어오늘,「"엠병신 PD입니다" 권성민 해고 무효가 의미하는 것」, 2016.5.13.

26 라이더유니온, 라이더유니온 3개 플랫폼사 AI 검증 결과 발표 기자간담회, 2021.6.28.

27 한국경제연구원 보도자료,「대기업 채용 "줄인다" 34% "늘린다" 18%」, 2019.9.16.

28 진보네트워크센터 보도자료,「시민단체, 인공지능 채용 공공기관 13곳에 정보공개 청구 및 결과 발표」, 2020.10.27.

29 한겨레21,「AI 면접관이 말했다 "너 인성 문제 있어?"」, 제1335호, 2020.10.23.

30 WP29,「자동화된 의사결정과 프로파일링에 대한 가이드라인」(Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679), 2018.2.6., WP251rev.01.

31 European Commission,「인공지능 법안」(Proposal for a Regulation laying down harmonised rules on artificial intelligence. Artificial Intelligence Act), 2021.4.21.

후주

이 가이드라인은 '노동감시 대응 사업단'이 집필·검수하였습니다.

'노동감시 대응 사업단'은 지속적으로 증가하고 첨단화되어 가는 노동감시에 대응하기 위해 활동합니다. 우리는 노동감시에 대응하기 위한 방안을 모색하고 법제도 개선을 위한 활동을 이어가고 있습니다.

노동감시 대응 사업단에 함께하는 사람들

권석현(직장갑질119 변호사)
김영선(노동권연구소 연구위원)
김태욱(민주노총법률원 변호사)
김하나(해우법률사무소 변호사)
오병일(진보네트워크센터 대표)
이미루(진보네트워크센터 활동가)
이상윤(한국노총 정책차장)
장여경(정보인권연구소 상임이사)
조현재(재단법인 공공상생연대기금)