형사정책연구 Korean Criminological Review
제23권 제3호(통권 제91호, 2012 · 가을호)

산업스파이범죄의 실태와 법적 규제의 문제점*

박 강 우**

국 | 문 | 요 | 약

형법, 부정경쟁방지법, 산업기술유출방지법 등에 의한 영업비밀 및 산업기술의 보호는 우리 기업의 기술수준이 높아짐에 따라 앞으로 더욱 실효성있게 집행되어야 할 분야이다. 하지만, 위 법률의 실무적용시 여러 가지 문제점과 해석상 논란이 제기된다. 우선, 영업비밀의 절취에 대해서는 영업비밀이 유체물이나 관리가능한 동력이 아니므로 재물성이 부정되어 형법상 절도죄의 적용이 불가능하며, 산업스파이 행위로 인하여 발생하는 기업의 손해가 매우 추상적이고 특정하기가 곤란하여 업무상 배임죄의 적용도 용이하지 않다. 다음, 부정경쟁방지법상 영업비밀로 보호받기 위해서는 소송과정에서 영업비밀침해를 입증하는 바, 그 입증이 쉽지 않다. 뿐만 아니라, 소송이라는 과정이 영업비밀이 유출되거나 획득되는 경로로 사용될 가능성도 배제할 수 없다. 결국 영업비밀에 대한 침해가 발생하기 전에 회사내부에서 영업비밀을 잘 관리하여 접근통제나 접근기록을 남기는 등의 방법으로 예방적 방법으로 관리하는 것이 가장 바람직하다. 산업기술유출방지법의 경우 국가핵심기술을 특별한 보호대상으로 삼고 있는데 우선, '국가핵심기술'이라는 정의에 부합하는 기술의 종류와 범위를 정하는 것이 쉽지 않다. 또한, 국가핵심기술로 지정할 때에는 단순히 고도한 첨단기술이라는 점만이 고려되어서는 안되며, 해당기술이 국가산업발전에 기여하는 정도와 다른 기술분야와 융합에 의한 시너지효과의 여부, 기술개발자의 창작의욕을 저해하지 않고 활성화시킬 수 있는지의 여부, 개인이나 민간기업 등의 국가핵심적 기술에 대한 취급과 그에 대한 적절한 보상과 같은 인센티브 등이 종합적으로 고려되어야 할 것이다.

❖ 주제어 : 산업스파이, 영업비밀, 산업기술, 부정경쟁방지법, 산업기술유출방지

* 이 논문은 2011년도 충북대학교 학술연구지원사업의 연구비지원에 의하여 연구되었음(This work was supported by the research grant of the Chungbuk National University in 2011).
** 충북대 법전원 교수, 법학박사

I. 머리말

1990년대 이후 세계는 선진국을 중심으로 지식의 창출・확산・활용・보호가 경제활동의 핵심이 되며 정보・지식에 근거한 무형자산이 노동・자본 등 유형자산보다 경제성장의 원동력이 되는 지식기반 경제로 전환되고 있다. 이러한 지식기반경제하에서 우리나라가 생산성 향상을 통해 지속적으로 성장하기 위해서는 창의성과 이에 기반한 지식재산의 축적 및 활용, 지식재산의 체계적인 보호가 필수적이다.

그러나 우리나라의 지식재산 활동을 살펴보면, 특허출원 건수로는 2011년 현재 세계 5위를 차지할 정도로 급성장하는 등 양적인 측면에서는 세계적인 수준에 도달한 반면[1] 질적 측면에서는 여전히 미흡한 수준이며, 보호 및 정책 인프라도 아직 낮은 실정이다. 기술무역 수지는 적자를 기록하고 있으며[2] 저작권 시장규모도 전 세계의 2% 수준에 불과하고 지식재산 보호 순위도 33위에 그치고 있다. 특히 핵심기술의 국내외 유출 및 이로 인한 피해는 증가하고 있으나 이에 대한 예방이나 피해방지, 손해복구를 위한 법제도는 매우 미흡한 실정이다.

이에 본고에서는 우리나라의 산업스파이범죄 내지 기술유출 실태, 특징을 살펴보고 이에 대한 법적 대응책으로서 형법 및 특별법(부정경쟁방지 및 영업비밀보호에 관한 법률, 산업기술의 유출방지 및 보호에 관한 법률)에 의한 영업비밀과 산업기술보호의 한계와 문제점을 분석해보고자 한다. 이를 통하여 영업비밀 및 산업기술보호를 위반 법체계의 정합성을 제고하고 영업비밀 내지 산업기술 보호의 효율성 제고에 기여할 수 있기를 희망한다.

---

1) WIPO, Statistics, 2011. 파이낸셜 뉴스 2012. 8. 7. 기사

2) 2009년 우리나라 기술무역수지는 4,856백만달러 적자를 기록하고 있으며, 적자폭이 점차 증가하고 있다. 이에 대하여 미국, 일본, 영국은 2001년이후 기술무역수지 흑자폭이 지속적으로 증가하고 있다. OECD, Main Science & Technology Indicators 2010-1; 교육과학기술부, 2009년도 기술무역통계조사보고서.

II. 산업스파이범죄의 실태 및 주요사례

1. 산업스파이범죄의 실태

국가정보원 산업기밀보호센터에 의하면[3], 국내 산업스파이 적발건수는 지난 2005년 29건에 불과했으나 2006년 31건, 2007년 32건, 2008년 42건, 2009년 43건, 2010년 41건, 2011년 46건으로 매년 꾸준한 증가세를 보이고 있다.[4]

지난 7년간 국내 발생 기술유출 사건을 분야별로 살펴보면 전기전자분야가 전체의 37%(75건)로 가장 많았으며, 이어 정밀기계분야 27%(55건), 정보통신분야 15%(32건), 정밀화학분야 9%(18건), 생명공학분야 3%(6건) 등의 순이었다.

산업기술유출 유형의 경우 무단 기술 보관을 통한 기술유출이 전체의 42%(86건)로 가장 많았으며, 이어 내부공모 25%(51건), 매수 23%(47건), 공동연구 2%(4건), 위장합작 1%(2건) 등으로 집계됐다.

이밖에 2005~2011년 기술유출의 주체는 전직 직원에 의한 사례가 62%(127건)이며, 현직 직원에 의한 사례가 17%(34건)를 차지했다. 이어 협력업체 13%(26건), 유치과학자 2%(5건), 투자업체 1%(1건) 등의 순이었다. 이렇게 최근 산업스파이범죄의 특징은 내부자에 의한 기술유출이 많다는 것인데. 이것은 최근 기업들이 산업보안에 대한 인식이 높아지면서 핵심기술 보안대책을 강화해 상대적으로 외부인의 접근이 어렵기 때문인 것으로 분석된다.

산업스파이의 기술유출의 동기는 개인의 영리를 위해 기술을 유출한 사례가 61%(125건), 금전유혹이 20%(41건)로 대부분을 차지했다. 이어 인사불만 8%(16건), 처우불만 6%(13건) 등이 뒤를 이었다.

이와 같이 산업스파이범죄는 기술개발 참여자가 별다른 죄의식 없이 자행하고 있으며 피해가 기업차원에 그치지 않고 국가경제에까지 손실을 준다는 점에서 문제의 심각성이 있다. 아래에서 대표적 사례 몇 가지를 살펴보기로 한다.

---

3) http://service4.nis.go.kr

4) 이투데이 2012. 6. 12. 기사.
http://www.etoday.co.kr/news/section/newsview.php?TM=news&SM=2301&idxno=594947

2. 주요사례

2011년 국내 모 조선업체에서 기술팀장으로 재직하던 엄 모씨는 퇴사하면서 35조원의 경제적 가치를 지닌 고급대형선박의 설계도면과 선박건조에 필수적인 공정도 등 최신 기술을 빼냈다. 그는 이후 중국 회사와 손을 잡은 국내설계 전문업체에 입사한 뒤 이 기술을 중국 조선업계에 팔아 넘기려다 국가정보원과 검찰에 검거되었다.

2010년 3월 국내 전자기업인 A사의 협력사 B사 대표 K씨는 A사 부장 Y씨 등을 통해 양문형 냉장고 설계도면을 빼내어, 중국 H사와 기술자문계약을 체결한 뒤 핵심기술 유출을 시도하다가 검거되었다[5].

2010년 12월 S사 책임연구원 L씨는 연구실에서 차세대 디스플레이 관련 핵심 제조기술과 원가정보 등 자료를 출력해 특수용지에 옮겨 적는 형태로 유출했다. L씨는 이렇게 유출한 기술을 중국 B사 직원에게 넘겼다. 대신 L씨는 중국 B사에 좋은 조건으로 입사키로 예정되었다. L사 K씨도 지난 2011년 1월 자신이 근무하는 연구실에서 차세대 디스플레이 사업 계획서 파일을 휴대폰으로 촬영하는 수법으로 중국 B사에 넘겼다. L씨와 K씨는 2011년 수사기관에 의해 적발되었다.

2010년 4월에는 국내 3D 제조업체 A사 연구소장 서모씨와 동종업체 B사의 대표 곽모씨가 중국에 3D입체영상을 만드는 자회사를 설립키로 하고 중국통신장비업체 D사에 A사의 3D제조기술이 담긴 파일을 빼내 이를 유출하려다 적발되기도 하였다. A사의 3D기술은 특수안경 등 별도의 장비 사용없이도 화면에 입체감을 구현하는 입체영상 제조기술로 중국으로 유출시 막대한 국부유출의 위험이 있었다.

이와 같이 국내에서 일어나는 산업기술유출 사건의 50% 이상은 중국과 관련된 사건들이다. 국가정보원 산업기밀보호센터에 의하면, 지난 2005년부터 2011년까지 국내 첨단 기술을 해외로 불법유출했거나 유출을 시도하다가 적발된 사건 총 264건 중에서 130건 이상이 중국으로의 유출이었던 것으로 나타났다. 유출 기술도 반도체, 조선, 디스플레이 등 첨단 산업분야가 모두 포함되어 있어 한국 경제의 경쟁력에 치명적인 초래할 수 있다는 우려를 낳았다[6]. 특히 문제가 되는 것은 중국 현

5) 파이낸셜뉴스 2012. 8. 23. 기사.

지에 진출한 한국 기업들 중에서 대기업보다 중소기업이 기술유출 위험에 취약하다는 점이다. 중소기업청과 중소기업진흥공단 등에 따르면 중국 진출 중소기업 100개를 대상으로 '기술보안 실태조사'를 진행한 결과 응답기업의 75%는 기술유출시 특별한 조치를 취하지 않은 것으로 확인되었다[7].

3. 주요국가의 영업비밀보호법

1) 미국

미국은 일찍이 20세기 초부터 영업비밀을 침해하는 행위를 불법행위법에 의하여 규율하다가 이후 1975년 통일영업비밀보호법(Uniform Trade Secrets Act, USTA)을 제정하고 이 법을 모델로 제정된 각주법에서 영업비밀을 민사적으로 보호하기 시작하였다. 그러나 기업들이 영업비밀침해에 대하여 민사적 구제방법의 사용을 꺼렸는데, 그 이유는 민사소송이 대단히 비용이 많이 들고 손해배상청구를 위하여 가해자의 영업비밀 침해 사실을 조사할 수 있는 능력이나 수단을 갖고 있지 못하였기 때문이다[8].

그리하여 1996년 경제스파이법(EEA, Economic Espionage Act)가 제정되어 영업비밀을 침해하는 행위에 대하여 형사적 처벌을 도모하게 되었다. 구체적으로 보면, 이 법률 제1831조(18 U.S.C. 1831)는 외국정부나 기타 외국의 기관을 이롭게 할 목적으로 영업비밀을 침해한 경우, 즉 경제간첩을 가중처벌하는 규정을 두고 있고, 제1832조는 영업비밀의 소유자 이외의 자를 이롭게 할 목적으로 영업비밀을 침해한 경우 처벌하는 규정이다. 전자, 즉 경제스파이죄에 의하여, 외국정부가 직접 범하거나 지원한 산업스파이 행위에 대해서는 미국내 기업간 영업비밀침해 행위보

6) 한국경제신문 2012. 6. 5. 기사. “이런 점에서 독일의 기계제조사 만츠(Manz)가 마련한 간단하면서도 효과적인 대응책이 주목을 받고 있다. 만츠는 중국 기업의 복제를 막기 위해 부품을 나사로 고정하는 대신 접착제로 고정시키는 방식을 도입했다. 이렇게 되면 복제품 생산을 위한 분해 및 분석작업이 어렵게 된다. 아울러 고객이 제품을 자사에 돌려 줄 경우에 한해 대체 부품을 공급하고 있고, 신모델 개발 때 시제품 제조는 독일 내에서만 수행하고 있다”.

7) 파이낸설뉴스 2012. 8. 23. 기사.

8) 한상훈, 산업스파이에 대한 형사법적 대응방안, 한국형사정책연구원 보고서, 2000, 19면.

다 중하게 처벌하여, 15년 이하의 자유형 또는 5십만달러 이하의 벌금에 처할 수 있도록 하고 있다. 단순 영업비밀침해에 대해서는 10년 이하의 자유형 또는 벌금에 처한다.

2) 독일

독일은 일찍이 1909년 제정되고 1932년 개정된 부정경쟁방지법(UWG, Gesetz gegen den unlautern Wertwerb)에 의하여 기업의 영업비밀을 보호하여 왔다. 하지만 동 법률에서는 회사와 근로계약을 맺은 자의 누설행위만을 처벌하도록 하고 있어서 제3자, 특히 산업스파이의 영업비밀탐지행위는 처벌하지 못하였다. 그리하여 1986년 종래 부정경쟁방지법상의 영업비밀조항을 개정, 강화하는 개정법을 컴퓨터범죄, 경제범죄의 일환으로 통과시켜 오늘날에 이르고 있다. 독일 부정경쟁방지법의 특징은 개별기업의 영업비밀의 보호하는데 그치지 않고 공정한 경쟁상태의 유지라는 일반적 법익도 보호한다는데 있다[9].

독일 UWG상 영업비밀의 보호는 제17조 내지 제20조의 a에서 규정하고 있는 바, 동법 제17조 1항은 “사업체의 피용자, 근로자 또는 견습생으로서, 고용관계에 기하여 위탁받거나 접근하게 된 영업상 또는 경영상의 비밀을, 고용관계의 계속 중에 권한없이 경쟁의 목적으로, 자신의 이익을 위해 또는 제3자를 위하여, 또는 사업주에게 손해를 가할 목적으로 타인에게 누설한 자는 3년 이하의 자유형 또는 벌금형에 처한다”고 규정하고 있다. 또한, 행위자가 누설시에 당해 비밀이 외국에서 이용된다는 사실을 알고 있거나 행위자 스스로 외국에서 이용한 경우에는 5년 이하의 자유형 또는 벌금형에 처할 수 있다고 규정하고 있다(동법 제17조 4항).

3) 일본

일본에서는 1911년 독일의 부정경쟁방지법을 모델로 영업비밀보호에 관한 법을 준비하였으나 시기상조론이 대두하여 연구와 논의만 계속되었고, 당시 영업비밀의 보호는 절도, 횡령, 배임 등 형법상의 재산범죄 규정을 적용하거나 민사상 손해배

9) 한상훈, 위의 보고서, 21면.

상청구를 통하여 가능했었다.

그러나 1986년 UR의 지적재산권문제가 대두되면서 1990년 부정경쟁방지법을 제정하였다. 하지만, 우리와 달리 동법상 영업비밀침해 행위에 대한 형사처벌규정은 신설되지 않았으며, 1993년 개정에서도 포함되지 않았었다. 하지만, 2006년 개정에서 일본도 형사처벌 규정을 광범위하게 도입하여 영업비밀 침해 행위를 규율하도록 하였다.

우리 법이 부정경쟁 행위와 영업비밀 침해 행위를 구분하여 별개의 장에서 다루고 있는 것과 달리, 일본 부정경쟁방지법의 특징은 양자를 통합된 형태로 규율하고 있다는 점이다. 아울러, 우리 부정경쟁방지법에서 두고 있지 않은 기술적 제한수단에 대한 무력화행위나 신용훼손행위에 대한 처벌규정을 두고 있다(우리의 경우 기술적 보호조치에 대한 침해는 컴퓨터프로그램보호법(2009년 폐지), 저작권법 등의 개별법에서 명문화된 처벌규정을 두고 있다).

또한, 우리의 부정경쟁방지법이 단순히 손해산정에서 서류제출만을 명하고 정당한 이유가 없는 경우에 이를 거절할 수 있도록 하는 조항만을 두고 있는 비하여(제14조의3), 일본의 부정경쟁방지법은 그 거절에 정당한 이유가 있는지 여부를 판단하기 위하여 필요한 경우 서류소지자에게 제시를 명할 수 있고, 법원에 제출하는 서류에 대한 공개금지에 대한 조항을 두는 등 우리 법보다 실효성있는 절차규정을 두고 있는 점이 눈에 띈다(제7조 1항, 2항, 3항 참조).

III. 영업비밀의 개념

「부정경쟁방지 및 영업비밀보호에 관한 법률」(이하 '부방법'이란 칭한다) 제2조 2호는 영업비밀을 "공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 생산방법・판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보"라고 정의하고 있다. 이 법에 의하여 영업비밀로 보호받기 위해서는 ① 공연히 알려져 있지 않을 것(비공지성), ② 독립된 경제적 가치를 가질 것(경제성), ③ 비밀로서 관리되고 있을 것(비밀관리성), ④ 생

산방법 · 판매방법 기타 영업활동에 유용할 것(유용성), ⑤ 기술상 또는 경영상의 정보이어야 한다.

1. 비공지성

부방법상 영업비밀로 인정되기 위해서는 공연히 알려져 있지 않아서 누구나 알고 있는 정보가 아니라는 비공지성을 필요로 한다. '공연히 알려져 있지 아니한' 상태란 영업비밀정보가 간행물 등 전파매체 등에 의해 공개되어 있지 않기 때문에 일반인이 언제, 어디서나 쉽게 구입 · 열람 · 복사 등을 통해 영업비밀의 내용을 파악할 수 없는 상태를 의미한다. 따라서 제한된 범위의 특정한 사람들만이 알고 있어야 하지만 영업비밀이 소수의 특정인만 알고 있을 필요는 없다. 극소수의 사람들만이 알고 있다고 하더라도 그 사람들이 비밀을 지킬 의무가 없다면 그 정보는 비공지성을 인정할 수 없으며, 아무리 많은 사람들이 알고 있다고 하더라도 그들이 비밀을 지킬 의무가 있는 경우에만 비밀로 유지된 정보라고 할 수 있다.

결국 비공지성이란 어떤 사실이나 정보가 일반적으로 알려져 있거나 임의의 접근에 노출되어 있어서 이에 관심을 가지는 누구나 정당한 방법으로 큰 어려움없이 획득할 수 있는 경우에는 인정되지 않는다[10]. 따라서 영업비밀로 인정되기 위해서는 일반적으로 입수하기가 곤란한 정보로서 한정된 자에게만 알려져 있고 공개나 사용에 의해 경제적 가치를 얻을 수 있는 자에게는 알려져 있지 않아야 한다.

2. 비밀관리성

영업비밀은 보유자가 당해 정보를 상당한 노력에 의하여 비밀로서 관리하고 있는 것이어야 한다. 당해 영업비밀에 관하여 보유자가 주관적으로 비밀로 할 의사를 갖고 있을 뿐만 아니라, 종업원 · 외부자로부터 객관적으로 비밀로서 관리되고 있다고 인정되는 상태에 있을 것"이 요구된다[11].

10) BGH NJW 1958, 671; NJW 1963, 2122.

11) 박상열, "부정경쟁방지법에 의한 영업비밀의 형사법적 보호", 지식재산연구 제6권 제3호, 2011.

만약 영업비밀이 비밀로서 관리되지 않으면 법적 보호를 받을 수 없다. 이것은 영업비밀보호의 목적이 영업비밀의 보호 자체에 있는 것이 아니라 비밀로 관리되고 있는 타인의 정보를 부정한 수단으로 취득하여 경쟁상 유리한 지위를 차지하는 행위를 막아 건전한 경쟁질서를 유지하는 것에 있음을 말한다[12]. 만약 비밀로 관리되고 있지 않는 정보까지 법적 보호의 대상으로 하면 재직 중에 정보를 알고 있던 직원이 전직 후에 당해정보를 이용하려 할 때 그것이 비밀로 관리되고 있지 않더라도 영업비밀에 대한 침해가 인정되는 문제가 발생한다. 이와 관련하여 직원이 퇴사하면서 가지고 나온, 자신의 컴퓨터에 저장된 회사의 영업관련자료는 상당한 노력에 의하여 비밀로 유지된 정보라고 볼 수 없어, 위 부방법상 영업비밀에 해당하지 않는다고 한 판례[13]가 있다.

정보의 보유자에게 요구되는 관리의 정도는 ① 그 정보가 비밀이라고 인식될 수 있는 표시를 하거나, 특정장소에 보관하는 등 당해정보 접근자에게 영업비밀이라는 것을 알 수 있도록 하여야 하며, ② 비밀취급인가자나 담당자 이외에는 접근할 수 없도록 하는 조치(암호 등의 부여) 등이 있어야 한다. 외부의 침입자에 대해서는 영업비밀이 기재된 문서 등이 있는 곳에 시건장치가 있는 경우만으로도 비밀유지성을 인정할 수 있겠지만, 내부의 종업원에 대해서는 시건장치가 있는 것만으로는 부족하고 당해 정보에 대외비표시가 되어 이를 유출하는 것을 금지하는 등의 조치가 되어 있는 등 구체적 상황에 따라 개별적으로 비밀관리성 유무를 판단하여야 한다.

3. 경제성

영업비밀의 경제성이란 그 보유자가 그 정보를 사용함으로써 생산비용을 절감하거나 판매를 보다 효과적으로 수행하는 등 경제적인 이익을 얻거나 상대방 경쟁자에 대하여 자신의 경쟁상의 지위를 제고함에 도움이 될 때, 또는 그 정보의 취득과

9, 108면.

12) 전지연, “영업비밀의 형사법적 보호”, 형사법연구 제20권 제4호, 2008, 253면.

13) 대법원 2009. 9. 10. 선고, 2008도3436 판결.

사용에 있어 대가나 사용료를 지불하거나 혹은 그 정보의 독자적인 개발을 위해서 상당한 노력과 비용이 필요할 때 인정된다[14]. 즉, 여기에서 말하는 경제적 가치란 정보 자체가 경제거래의 대상이 되는 독자적인 재산적(금전적) 가치를 가져야 하는 것이 아니라, 비밀로 소유・관리할만한 정당한 이익이 있어야 하는 것으로 이해된다[15]. 따라서 경제적 유용성이 낮다는 이유로 법적 보호를 부정해서는 안된다. 이러한 맥락에서 일본의 부정경쟁방지법에서는 영업비밀을 “비밀로 관리되고 있는 생산방법, 판매방법 등의 사업활동에 유용한 기술상 또는 영업상의 정보로서 공연하게 알려져 있지 않은 것”(일본 부정경쟁방지법 제2조 4항)이라고 규정할 뿐 독립된 경제적 가치를 가질 것을 요구하지 않고 있다.

4. 유용성

정보의 유용성이란 당해 정보가 사업활동에 효용성이 있는 유익한 정보인가의 문제이다. 따라서 영업활동에 필요한 정보로서 생산공정이나 제품 또는 서비스, 가격책정 등에 실질적으로 이용할 수 있어야 한다. 물론 유용성이 있는 정보가 모두 영업비밀이 되는 것은 아니며 법적 보호를 하는데 충분한 사회적 의의와 타당성을 가져야 하고, 보호의 필요성이 있는 정보이어야 한다. 따라서 공해물질의 배출방법이나 로비의 대상이나 금액, 세금포탈의 유형이나 방법에 대한 정보는 정보의 보유자에게는 영업상 유용할지 모르나 반사회적 정보이기에 법적으로 보호받는 영업비밀이 되지 못한다[16].

5. 기술정보와 경영정보

기술상의 정보는 제조방법, 제조공정, 화학방법, 성분원료의 배합비율, 강도계산의 운용방법, 설계방법, 설계도면, 청사진, 제조원가, 실험자료, 연구보고서를 들 수

14) 윤선희, “영업비밀에 있어서의 경영상 정보”, 창작과 권리 제39호, 2005, 94~95면.
15) 송영식·이상정·황종환, 지적소유권법(하), 육법사, 2003, 443면.
16) 최호진, “기업의 영업비밀에 대한 형사법적 보호”, 형사법연구 제25호, 2006년 여름, 384면.

있고, 영업상의 정보로는 고객명부, 거래선의 루트, 판매지침서, 시장정보조사결과, 고객관리기법, 판매메뉴얼, 제품의 할인시스템 등을 들 수 있으며, 기타 경영상의 정보로는 재무관리정보로 자금조달계획, 자산구입, 설비투자계획, 예산분배계획을 들 수 있고, 조직관리정보로 인사기록카드, 조직관리기법 등의 정보를 들 수 있다. 사무관리정보로는 시설이나 차량관리정보에 관한 정보, 영업전략정보, 사업계획자료, 사업성 검토자료, 선전광고기법 등을 들 수 있다.

IV. 형법에 의한 영업비밀 보호의 한계

형법상 국가기밀이나 개인비밀은 간첩죄, 외교상 비밀누설죄, 공무상 기밀누설죄, 비밀침해죄 등에 의해서 보호되고 있는 반면, 영업비밀을 직접적으로 보호하는 형법규정은 존재하지 않았다. 1985년 형사법개정 특별심의위원회에서 산업스파이 행위에 대한 처벌규정의 신설을 개정의견으로 내놓았지만 입법화되지는 못했다[17].

따라서 현행 형법에서 영업비밀침해 자체를 직접적으로 처벌하는 규정은 없다. 하지만, 영업비밀을 침해하는 과정에서 발생하는 개개의 행위가 절도죄・주거침입죄・사기죄・배임죄・횡령죄 등에 해당할 경우 그 행위를 처벌함으로써 간접적으로 영업비밀을 보호할 수 있을 뿐이다. 하지만, 이러한 보호방법은 다음과 같은 한계를 갖는다.

1. 절도죄의 성립가능성

기업의 영업비밀이 문제될 수 있는 행위유형으로는 ① 영업비밀이 화체된 문서, 디스켓 또는 CD 등을 절취한 경우, ② 영업비밀이 화체된 문서를 현장에서 복사, 촬영하여 그 내용을 파악해 간 경우, ③ 영업비밀이 화체된 문서 등을 가지고 나가 복사, 촬영 등을 하고 제자리에 갖다 놓은 경우이다.

17) 구체적 이유에 대해서는 권문택, 형법각칙에서 검토하여야 할 문제, 형사법개정특별위원회 편, 형법개정의 제논점, 형법개정자료(III), 1985, 210~211면 참조.

①의 경우 절취한 문서, 디스켓 자체에 대해여는 절도죄가 성립한다는 점에 의문이 없다. 대법원도 “사원이 회사를 퇴사하면서 원료의 배합비율, 제조공정, 시제품의 품질확인이나 제조기술 향상을 위한 각종 실험결과 등을 기재한 자료를 가져간 경우 이는 절도에 해당하고, 위 자료는 구 부정경쟁방지 및 영업비밀보호에 관한 법률에 정한 영업비밀에 해당한다”[18]고 판시하였다.

그러나 이렇게 절도로 처벌함으로써 행위불법의 양과 책임의 양이 균형을 이룰 수 있는지는 의문이다[19]. 예컨대 시가 10억원 상당의 기업비밀이 들어있는 A4용지 2장을 절취한 경우에 행위자를 A4 용지 2장에 대한 절도로 처벌할 수 있을 뿐이지 10억 상당의 영업비밀에 대한 절도로는 처벌할 수 없기 때문이다[20].

또한, 영업비밀이 유체물에 화체되어 있지 않은 경우 또는 유체물에 화체되어 있더라도 그 내용을 복사 또는 촬영하거나, 인터넷을 통하여 전송케 한 경우에 절도죄의 객체인 재물성과 절취행위성을 인정할 수 있을 것인가가 문제된다. 형법은 관리가능한 동력을 재물로 간주하지만(제346조), 이 경우 동력은 물리적으로 관리가능한 자연적 에너지에 국한하고 있기 때문에 자연적 에너지에 해당하지 않는 정보, 사상, 아이디어로서의 기획, 이념적 가치, 권리 자체 등은 재물에 해당하지 않으므로 영업비밀은 재물개념에 포섭되지 않는다. 물론, 영업비밀이 전자정보의 형태로 존재하는 경우 소유자 또는 이용자가 외부인의 접근을 막기 위해서 영업비밀에 비밀번호를 설정하거나 접근권한을 구분하는 경우 관리가 가능하게 된다. 그러나 전자정보 형태의 영업비밀의 관리는 현실세계의 재물에 적용되는 물리적 관리가 아니라 전자적 관리나 통제에 해당하므로 관리가능성설에 의하더라도 영업비밀을 재물로 볼 가능성은 희박하다. 앞으로 관리가능성설의 입장에서도 영업비밀이나 전자정보형태의 권리나 아이디어를 재물로 포섭할 수 있는 해석론의 개발이 필요하다고 생각된다.

---

18) 대법원 2008. 2. 15. 선고 2005도6223 판결.

19) 최호진, 앞의 논문, 390면.

20) 대법원은 영업비밀이 담겨있는 타인의 재물을 절취한 후 그 영업비밀을 사용하는 경우, 영업비밀의 부정사용행위는 새로운 법익의 침해로 보아야 하고 불가벌적 사후행위로 보아서는 안된다고 한다. 따라서 절도죄와 별도로 부정경쟁방지 및 영업비밀보호에 관한 법률상 영업비밀부정사용죄가 성립한다. 대법원 2008. 9. 11. 선고 2008도5364 판결.

여기서 영업비밀을 시대의 요청, 즉 정보통신기술의 발전에 따라 변화될 수 있는 것으로 보아 목적론적 확장해석을 통하여 재물개념에 포섭시킬 수 있는 가능성은 없는 것인가? 다수설과 같이 유추해석은 금지되지만, 목적론적 확장해석은 허용된다는 입장을 취하다하더라도 확장해석과 유추해석의 한계인 '문언의 가능한 의미'를 넘는 해석은 국민의 법률에 대한 예측가능성을 보장할 수 없기 때문에 허용될 수 없다. 영업비밀을 재물개념에 포섭하기 위해서는 무형적 재화의 특성에 대한 보다 엄밀한 논증이 필요하며, 그러한 논증없이 재산적 침해에 대한 형법적 보호의 필요성이라는 현실적인 이유만으로 재물개념에 포함시키는 것은 죄형법정주의의 요청상 금지된 유추해석이 될 가능성이 높기 때문이다[21].

따라서, 영업비밀과 같은 정보는 현행 형법의 해석상 재물개념에 포섭될 수 없다. 그러나 그 재산적 가치가 증대함에도 불구하고 형법에 의한 보호대상이 될 수 없다는 점에서 전통적 재물개념을 현대적 시각에서 재해석할 필요성은 여전히 존재한다고 할 것이다[22].

2. 업무상 배임죄의 성립가능성

(1) 타인의 사무처리자

회사직원이 영업비밀을 유출하는 행위는 회사에 대한 신임관계에 위배되는 행위이므로 행위 자체의 배임성을 인정하는 것에는 별문제가 없다. 그러나 업무상 배임죄를 적용할 경우 회사내부자의 비밀유출행위만이 처벌대상이 되기 때문에, 기업의 외부자의 비밀탐지행위는 처벌하지 못하는 문제점이 있다. 또한, 내부자로 하더라도 경비 등 순전히 기계적 업무에 종사하는 자이거나, 비밀을 자기관리하에 두지 않는 경우에는 사무처리자라고 보기 어려우므로 이들의 비밀유출행위에 대해서는 업무상 배임죄로 처벌할 수 없다.

배임죄의 성립요건인 '타인의 사무'에서 사무의 성격에 대하여 재산적 사무설[23],

21) 변종필, "인터넷게임 아이템과 재산범죄", 인터넷법률 제5호, 2001면, 44면; 하태훈, "인터넷과 형법의 변화", 인터넷법률 창간호, 2000, 99면.

22) 박상기, 형법각론(제7판), 2008, 248면.

재산상의 사무는 아니어도 재산적인 이해관계를 가지는 사무라는 견해(재산적 이해관계설), 재산상의 사무일 것을 요하지 않는다는 견해(일반적 사무설)[24]가 대립한다. 만일 재산적 사무설을 따른다면 영업비밀 침해사건에서 타인의 사무를 인정할 여지는 협소해진다. 기술상 영업비밀의 생산, 관리를 재산상의 사무로 보기는 곤란하기 때문이다.

그런데 대법원은 통상의 배임죄 사건에서 타인의 사무라 함은 타인의 재산을 보호 내지 관리할 의무를 의미한다고 하여, 재산관련사무일 것을 요구하고 있다[25]. 산업스파이가 관심을 가질만한 고도의 생산기술, 제조기술을 보유하고 있는 기업은 대부분 대기업이고, 대기업의 내부는 각 부서별로 세분화되어 있다. 이러한 대기업 내부에서 기술상, 산업상의 비밀을 취급, 관리하는 임직원은 대부분 연구개발부서에 근무하는 이공계출신의 연구원이며, 이들은 재산을 관리하는 자금부, 금융부와는 조직적으로 구별되기 때문에 이들에게 회산의 재산을 보호 내지 관리할 의무가 있다고 인정할 수 있을지는 의문이다. 두 가지 방안이 가능한데, 첫째는 기술상의 영업비밀에 대하여 재산성을 인정하는 것이고, 두 번째는 타인의 사무의 해석론에서 재산적 이해관계설을 취하는 것이다. 현재로서는 기술상의 영업비밀에 대하여 재산성을 인정하는 무리한 해석론 보다는 '타인의 사무'의 해석범위를 확장하는 두 번째 방법이 타당하다고 생각된다[26].

(2) 재산상 이익

현재의 해석론으로 영업비밀을 재물개념에 포섭시킬 수는 없지만 재산상 이익을 행위객체로 포함하는 사기죄, 공갈죄, 배임죄 등과 같은 이득죄의 행위객체에는 포함시킬 여지가 있다. 이득죄의 객체인 재산상 이익에 관하여 법률적 재산설에 따르

23) 다수설. 김일수/서보학, 형법각론(제7판), 2007. 484면; 배종대, 형법각론(제7전정판), 2010, 80/5, 이재상, 형법각론(제6판), 2009, 21/11.

24) 임웅, 형법각론(개정판 보정), 2006, 415면.

25) 대법원 1984. 12. 26. 선고, 84도2127 판결; 대법원 1987. 4. 28. 선고 86도2490 판결; 대법원 19994. 9. 9. 선고 94도도902 판결.

26) 한상훈, "영업비밀침해에 대한 형사처벌의 가능성과 개선방안", 국민대 법학연구 제14호, 2002, 236면.

면 영업비밀의 경제적 가치는 인정할 수 있다고 하더라도 그것이 현행법상 구체적 권리의 대상이 되지 않는 한 재산상 이익이라고 볼 수 없다. 이에 대하여 경제적 재산설[27]은 재산상의 이익을 순수하게 경제적 관점에서 파악하여 경제적 교환가치가 없는 개인의 사법상 권리는 재산이 아니며, 경제적 가치있는 사실상 이익과 노동력을 비롯하여 기대권, 상인의 영업정보 등도 재산상 이익이 될 수 있다고 주장한다[28]. 경제적 재산설에 의하면 영업비밀은 현실의 거래계에서 현금으로 거래되는 한 경제적 가치가 있는 사실상의 이익이라고 볼 수 있으므로, 영업비밀도 형법상의 재산상 이익에 포함될 수 있다. 법률적・경제적 재산설[29]은 경제적 교환가치가 있는 재화가운데 법질서에 의하여 승인된 것만을 재산이라고 보는 견해로 합법적인 기업의 기술정보와 같은 경우에는 경제적 가치성을 인정할 수 있을 뿐만 아니라 법질서 전체에서 승인된 것이라 볼 수 있으므로 재산상 이익으로 인정된다.

(3) 손해의 발생

형법상 배임죄가 성립하기 위해서는 배임행위로써 재산상 이익을 취득하여 본인에게 손해를 가해야 한다. 여기의 손해는 재산상의 손해로서 반드시 현실적으로 발생할 것을 요하지는 않고 손해발생의 위험을 초래케 한 경우도 포함한다[30]. 따라서 그 피해액이 구체적이지 못하고 추상적이라 하더라도 재산적 손해가 발생한 것으로 인정되는 이상 배임죄가 성립한다고 볼 수 있다.

산업스파이 행위로 인하여 발생하는 기업의 손해는 매우 추상적이어서 특정하는데 어려움이 많고 손해발생의 위험 역시 경제적으로는 현실의 손해가 발생하고 있지만 그 산정이 용이하지 않은 경우가 많다. 그리하여 기업경쟁상 불리하게 될 우려가 있다는 것만으로는 배임죄의 요건으로서 재산상 손해가 발생하였다고 볼 수

27) 김성돈, 형법각론(제2판), 2009, 287면; 손동권, 형법각론(개정판), 2005, 316면; 오영근, 형법각론(제2판), 2009, 18/6; 임웅, 앞의 책, 314면; 정/박, 형법각론, 2002, 322면; 이재상, 앞의 책, 17/11.

28) 대법원 2001. 10. 23, 2001도2991.

29) 김일수/서보학, 앞의 책, 315면; 배종대, 앞의 책, 67/7.

30) 대법원 1987. 7. 21, 87도546; 배임죄에서 손해를 가한 때라 함은 현실적으로 실해를 가한 경우뿐만 아니라 실해발생의 위험을 초래케 한 경우도 포함하는 것이고, 손해액이 구체적으로 명백하게 확정되지 않았다고 하더라도 배임죄의 성립에는 소장이 없다.

없다는 견해도 있다. 그러나 회사비밀을 경쟁회사에 팔면 막대한 개발비용 등 기업비밀의 재산적 가치가 감소되거나 상실되기 때문에 재산상 손해발생의 위험을 인정하는 데에는 별다른 어려움이 없다. 실제로는 영업비밀 침해사건에서 구체적 손해액 내지 이득액 확정이 쉽지 않기 때문에 「특정경제범죄 가중처벌 등에 관한 법률」상 재산상 이득액이 50억원 이상일 경우, 5억원 이상 50억원 미만일 경우 적용되는 가중처벌규정의 적용은 어렵다.

삼성전자 · LG반도체 64M DRAM사건에서 대법원은 "영업비밀을 취득함으로써 얻는 이익은 그 영업비밀이 가지는 재산가치 상당이고, 그 재산가치는 그 영업비밀을 가지고 경쟁사 등 다른 업체에서 제품을 만들 경우의 그 감소분 상당과 나아가 그 영업비밀을 이용하여 제품생산에 까지 발전시킬 경우 제품판매이익 중 그 영업비밀이 제공되지 않았을 경우의 차액상당으로서 그러한 가치를 감안하여 시장경제원리에 의하여 형성될 시장교환가격이다[31]"라고 하여 원칙적으로 시장교환가격을 기준으로 이익액을 판단하고 있다.

그러나, 시장교환가치에 근거한 이익액을 구체적으로 산정함에 있어서는 입증의 문제가 발생하는 바, 위의 64M DRAM사건에서도 원심은 시장교환가격 산정자료에 대한 활용가능성과 성패, 피고인들이 자료를 유출함으로써 얻은 재산상 이익의 정도가 불확실하다는 이유로, 피고인들이 자료를 유출함으로써 얻은 재산상 이익의 정도가 불명이라고 판단하고, 피고인들이 얻은 이익이 삼성전자가 투입한 기술개발비 상당인 것을 전제로 한 특경법위반의 점에 대해서는 무죄를 선고하였고 대법원도 이를 인정하였다.

V. 부정경쟁방지법상 영업비밀 침해행위에 대한 형사처벌의 문제점

영업비밀에 대한 절취 등 부정취득행위를 형법상 범죄로 의율함에 있어서 여러 가지 한계와 문제점으로 인하여 부정경쟁방지법이 제정되어 다음과 같은 행위를

31) 대법원 1999. 3. 12 선고 98도4704 판결.

처벌하고 있다.

1. 부정경쟁방지법상의 영업비밀 침해행위

가. 국외유출 영업비밀 취득·사용·누설행위

부정경쟁방지법 제18조 1항에서는 "부정한 이익을 얻거나 기업에 손해를 가할 목적으로 그 기업에 유용한 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알고 취득·사용 또는 제3자에게 누설한 자는 10년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금에 처한다"고 규정하고 있다. 과거 7년 이하이던 법정형이 2009년 개정에서 10년 이하로 상향되었다.

본죄가 성립하기 위해서는 '기업에 유용한 영업비밀'을 '사용 또는 누설'해야 한다. 따라서, 비밀성이 유지된 비공지의 영업비밀이라 하더라도 기업에 유용성 또는 경제성이 없는 정보[32]의 취득·사용·누설은 처벌되지 않는다. '취득'이라 함은 사회통념상 영업비밀을 자신의 것으로 만들어 이를 사용할 수 있는 상태에 이른 경우를 말한다[33]. 따라서 기업의 직원으로서 영업비밀을 인지하여 이를 사용할 수 있는 자는 이미 당해 영업비밀을 취득한 것으로 보아야 하기 때문에 그러한 자가 당해 영업비밀을 단순히 외부로 무단 반출한 행위는 경우에 따라 업무상 배임죄에 해당할 수는 있겠으나 여기의 영업비밀의 취득에는 해당하지 않는다[34].

'사용'이라 함은 영업비밀 본래의 사용목적에 따라 이를 상품의 생산 또는 판매 등의 영업활동에 이용하거나 연구, 개발사업 등에 활용하는 등으로 기업활동에 직접 또는 간접적으로 사용하는 행위로서 구체적으로 특정이 가능한 행위를 말한다[35].

'누설'이란 영업비밀을 아직 못하는 타인에게 이를 알려주는 행위를 말하며, 구두의 고지, 서면에 의한 통지 등 방법의 제한이 없다. 부정경쟁방지법 제2조 3항

32) 예컨대 공해물질의 무단배출이나 로비대상자와 금액에 대한 정보, 세금포탈방법에 대한 정보 등이 있다.

33) 대법원 2008. 4. 10, 2008도679 판결; 대법원 1998. 6. 9, 98다1928 판결.

34) 대법원 2008. 4. 10, 2008도679 판결; 전지연, 앞의 논문, 267면.

35) 대법원 1998. 6. 9, 98다1928 판결.

가목에서는 영업비밀의 침해행위 중 공개행위에 대해서 규정하면서, 공개행위는 “비밀을 유지하면서 특정인에게 알리는 것을 포함한다”고 정의하고 있으므로 공개의 개념에 누설도 포함되는 것으로 해석된다[36]. 따라서 공개라는 행위태양 이외에 누설이라는 행위태양을 별도로 규정할 필요가 있는가는 의문시된다.

누설의 경우 제3자가 영업비밀의 내용을 직접 인식할 것을 요하지 않는다고 해석해야 할 것이다. 따라서 영업비밀이 물건에 화체되어 있는 경우, 그러한 영업비밀의 지배를 제3자의 지배로 이전한 때에는 아직 제3자가 영업비밀의 존재나 내용을 인식하지 못했다 하더라도 누설행위가 인정된다. 이러한 점에서 본죄는 영업비밀이 직접 침해되지 않더라도 침해의 구체적 위험이 있을 때 성립하는 구체적 위험범이라고 할 수 있다[37].

이밖에 부정경쟁방지법상 영업비밀의 침해가 성립하기 위해서는 주관적 요건으로 행위에 대한 고의가 존재하여야 하며, 또한 “부정한 이익을 얻거나 기업에 손해를 입힐 목적으로”라는 초과주관적 요소가 필요하다. ‘부정한 이익을 얻을 목적’이란 경제적인 대가를 받거나 고용을 보장받는 등 다양한 혜택이나 이익을 받을 것을 말하고, ‘기업에 손해를 입힐 목적’은 기업의 영업비밀을 누설하는 행위 등을 통하여 기업의 매출을 감소시키거나 경쟁기업과의 경쟁으로 인하여 이익을 감소시키려는 목적 등을 의미한다.

따라서, 협상을 성공시키기 위하여 영업비밀인 설계도면을 상대방에게 설명하거나, 기술이전계약을 성사시키기 위하여 영업비밀인 제품의 제조공정과정 일부를 설명하는 과정에서 이를 누설하거나, 공중의 이익을 위하여 업체의 영업비밀의 일부인 폐수처리과정을 누설하는 등의 경우에는 부정한 이익을 얻거나 기업에 손해를 입힐 목적에 해당한다고 볼 수 없다.

나. 국내유출 영업비밀의 취득사용·누설행위

부정경쟁방지법 제18조 2항은 “부정한 이익을 얻거나 기업에 손해를 가할 목적으로 그 기업에 유용한 영업비밀을 취득·사용하거나 제3자에게 누설한 자는 5년

36) 박상열, 앞의 논문, 134면.

37) 이재상 14/23. 추상적 위험범이라는 견해로는 임웅, 형법각론, 220면.

이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금에 처한다"고 규정하고 있다. 여기서 '취득'이란 비밀이 서류나 CD 등과 같은 유체물에 고정되어 있는 경우 그 유체물을 취득함으로써 비밀을 취득하는 경우 뿐만 아니라 기억 등을 통해서 취득하는 경우 또는 산업스파이와 같이 제3자를 통하여 취득하는 경우가 있을 수 있다. 이외에도 비밀취급자를 매수나 유혹에 의하여 취득하는 경우나 절취나 기망·협박과 같은 부정한 수단에 의한 경우도 포함될 것이다.

2. 부정경쟁방지법의 문제점

가. 행위주체의 문제

종전 부정경쟁방지법은 영업비밀 침해행위의 주체를 해당기업의 전·현직 임직원으로 한정하였는데, 현행법에서는 이러한 제한을 폐지하고 침해주체를 모든 위반자로 확대하였다. 이것은 종전의 영업비밀 침해행위가 기업내부사정에 밝고 접근이 용이한 내부인에 의하여 이루어지는 경우가 대부분이었으나 최근에는 해당기업의 직원이 아닌 외부인(산업스파이, 경쟁업체 등)에 의한 침해가 빈발하고 있다는 점을 고려한 것이다[38]. 외부자의 영업비밀탐지로 인한 피해는 내부자 못지 않게 심각하며, 지식정보사회에서 국내외의 산업스파이에 의한 영업비밀 침해행위를 국가경쟁력을 저해하는 행위로 보아 이를 정책적 차원에서 방지하기 위해 관련법규를 강화한 것이다.

하지만, 전·현직 임직원의 영업비밀 누설행위와 일반인의 침해행위의 불법성은 전자의 불법이 더 크다고 보아야 하므로, 입법적으로 양자를 구별하여 규정하고 그에 대한 처벌의 법정형도 따로 정할 필요가 있다[39]. 뿐만 아니라, 침해의 주체가 자연인인가 법인인가에 따라 그 처벌을 달리할 필요가 있다. 법인의 경우 재산상의 이익이 일반인보다 더 크기 때문에 일본의 부정경쟁방지법 제22조와 같이 법인에 대해서는 보다 중한 형벌로 대처할 필요가 있다. 또한, 미국 경제스파이법에서는 법인의 영업비밀절취에 대해서는 천만달러 이하의 벌금에 처할 수 있도록 규정하

38) 황의창, 부정경쟁방지및영업비밀보호법(3정판), 세창출판사, 2004, 261면.
39) 전지연, 앞의 논문, 272면.

고 있다(18 USC § 1831 (b)).

나. 행위태양의 문제

영업비밀 침해행위의 3가지 유형인 취득, 사용, 누설 중에서 누설행위의 기준과 한계가 명확하지 않다. 즉, 군사기밀보호법이나 형법상 비밀누설죄와 같이 누설해서는 안되는 대상이 명확한 경우에는 해석상 별문제가 없으나, 영업비밀과 같이 누설의 대상이 명확치 않은 경우 누설행위의 기준과 한계를 설정하는데 어려움에 부딪히게 된다. 더구나, 누설이란 형법상의 일반적 범죄와 같이 신체적 동작을 수반하지 않고 순수하게 언어적 거동을 통하여 이루어지는 경우가 많다. 따라서 범죄입증을 위한 구체적인 물증이 없으면 공소유지 자체가 어려워질 가능성이 높다. 이점에서 공개라는 행위태양도 마찬가지이다.

다. 탐지 · 수집행위에 대한 처벌규정의 부재

위에서 보았듯이 부정경쟁방지법은 영업비밀을 '취득, 사용, 누설'하는 행위만을 처벌의 대상으로 규정하고 있는데, 영업비밀의 사용 및 누설행위의 전제행위로서 '탐지, 수집'행위를 행위태양에 포함시킬 필요가 있다. 물론 영업비밀의 탐지나 수집행위는 미수나 예비 · 음모행위로 보아 처벌할 수도 있다. 하지만, 예비행위는 그 정형성의 결여로 인하여 구체적인 행위유형이 존재하지 않기 때문에 죄형법정주의의 명확성원칙에 반할 우려가 있다[40]. 즉, 일반적 범죄의 경우 해당 범죄행위의 정형성으로부터 해당 범죄행위의 예비행위를 어느 정도 유형화할 수 있으나, 그 자체로는 범죄행위가 아닌 취득, 사용행위로부터 유형적 예비행위를 도출하기는 쉽지 않으므로 탐지, 수집행위를 별도의 처벌대상으로 명확히 규정할 필요가 있다.

라. 영업비밀의 취득·사용·누설 상대방에 대한 처벌규정의 부재

현행 부정경쟁방지법이 갖는 가장 큰 문제는 바로 영업비밀 누설행위로 인한 영

40) 박상열, 앞의 논문, 136면 주99); 전지연, 앞의 논문 274면.

업비밀 지득자의 처벌에서 흠결이 발생한다는 점이다. 부정경쟁방지법 제18조는 영업비밀을 취득, 사용, 누설한 경우만을 처벌하고 있으며, 이러한 취득・사용・누설의 상대방, 즉 영업비밀의 최종 수혜자는 벌하지 않고 있다. 이 경우 형법에 의한 처벌로는 장물죄의 적용을 고려할 수 있다. 그러나, 무형적 영업비밀 자체는 장물죄의 객체인 재물이 아니기 때문에, 영업비밀 자체만을 사후적으로 전달, 취득, 보관하는 경우는 장물죄로도 처벌할 수 없다. 즉 배후자가 영업비밀이 화체된 비밀서류, 디스켓, USB 등을 취득, 보관하지 않는 한 장물죄로 처벌할 수 없다. 미국[41], 독일[42], 일본[43]의 경우에는 제3자인 외부자가 영업비밀을 권한없이 취득하거나 사용하는 경우까지 처벌을 확대하여 영업비밀의 직접 침해자 뿐만 아니라 그 배후자, 즉 영업비밀의 최종취득자도 처벌하도록 하고 있다.

마. 비현실적 벌금형 액수와 손해액의 추정규정

부정경쟁방지법 제14조의2에서는 부정경쟁행위로 인한 손해액의 추정규정을 두고 있다. 동조 1항에 의하면, 부정경쟁행위 또는 영업비밀 침해행위로 영업상의 이익을 침해당한 자가 이 법 제5조 또는 제11조에 따른 손해배상을 청구하는 경우 그 손해액은 영업상의 이익을 침해당한 자가 생산할 수 있었던 물건의 수량에서 실제 판매한 물건의 수량을 뺀 수량에 단위수량당 이익액을 곱한 금액이 손해액의 한도가 된다. 또 2항에서는 “부정경쟁행위, 제3조의2 1항이나 2항을 위반한 행위 또는 영업비밀 침해행위로 영업상의 이익을 침해당한 자가 제5조 또는 제11조에 따른 손해배상을 청구하는 경우 영업상의 이익을 침해한 자가 그 침해행위에 의하여 이익을 받은 것이 있으면 그 이익액을 영업상의 이익을 침해당한 자의 손해액으

41) 미국 경제스파이법(Economic Espionage Act) 제1831조 a항 3호 : 영업비밀이 절취되거나 권한없이 전용, 획득 또는 전환되었다는 정을 알고, 이를 수취하거나 구입 또는 소지하는 행위는 15년 이하의 자유형 또는 50만달러 이하의 벌금에 처한다.

42) 독일 부정경쟁방지법(Gesetz gegen den unlauteren Wertbewerb, UWG) 제17조 2항 2호 : 타인의 행위를 통하여 획득하거나 기타 권한 없이 취득 또는 확보한 영업상 또는 경영상의 비밀을 권한없이 사용하거나 타인에게 누설하는 행위는 3년 이하의 자유형에 처한다.

43) 일본 부정경쟁방지법 제21조 1항 9호 : 부정경쟁의 목적으로 제4호 또는 제6호부터 제8호까지의 죄에 해당하는 개시에 의해 영업비밀을 취득하고, 그 영업비밀을 사용하고, 또한 개시한 자는 5년 이하의 징역에 처한다.

로 추정한다"는 규정을 두고 있다.

이러한 손해액 추정규정은 특허법 제128조 2항, 실용신안법 제46조, 의장법 제64조 2항, 상표법 제67조 2항, 저작권법 제125조 2항, 컴퓨터프로그램보호법 제32조 3항(2000. 1. 28. 법률 제6233호로 개정된 것), 반도체집적회로의 배치설계에 관한 법률 제36조 2항에서도 발견할 수 있는 바, 각각 "침해자가 그 침해행위로 인하여 이익을 얻은 때에는 그 이익액을 권리자가 받은 손해의 액으로 추정한다"고 규정하고 있다. 이는 권리자가 자신에게 발생한 인과관계 있는 손해를 증명하는 것이 곤란한 점을 고려하여, 침해자가 받은 이익액을 권리자의 손해액으로 추정하는 것이다.

그러나, 이러한 손해액 추정규정과 이득액의 2배에서 10배를 벌금액으로 부과한다는 벌칙규정(제18조 1항)의 실무상 유용성은 그리 높지 않은 것으로 보인다. 통상 첨단기술의 경우 기술개발에 소요되는 비용이 수백억, 수천억원에 달하는데 현행 규정에 따라 수백억, 수천억의 벌금형을 개인에게 선고할 가능성은 없어 보인다. 실제 동법 개정(2004. 1)전에는 기술유출사범들에게 수백, 수천만원 상당의 벌금형이 선고되었으나 동법 개정이후 벌금형이 선고받은 사건이 거의 없음은 이를 반증해준다[44].

VI. 산업기술유출방지법상 처벌규정의 문제점

위와 같이 부정경쟁방지법에 의한 영업비밀보호가 일정한 한계가 있다는 지적에 따라 국가적 차원에서 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지함을 목적으로 「산업기술의 유출방지 및 보호에 관한 법률」(이하 산업기술유출방지법)이 제정되어 2007년 4월 27일부터 시행되고 있다.

이 법은 기본적으로 산업스파이 범죄를 규율하기 위한 법률이다. 종래 영업비밀

44) 백영준, "영업비밀보호법의 적용상 한계", 한국산업재산권법학회, 산업재산권 23, 2007. 8, 45면.

의 침해행위는 부정경쟁행위의 일종으로 취급되어 부정경쟁방지법에서 규율하였던 바, 이 점에서 부정경쟁방지법과 상당히 많은 부분이 중첩되어 있다. 다만 산업기술유출방지법은 단순히 기업 상호간의 영업비밀 침해행위 뿐만 아니라 국가경제적 차원에서 영업비밀 침해행위를 규제한다는 점에서, 그리고 기업의 영업비밀 뿐만 아니라 국가・연구기관 및 대학 등 산업기술의 개발・보급 및 활용에 관련된 모든 기관의 산업기술이 그 보호대상이라는 점에서 특별한 의미를 갖는다[45].

결론부터 말하자면 산업기술유출방지법상 산업기술유출에 관한 처벌규정은 불명확하고 중복된 부분이 많다. 이것은 입법자들이 모든 산업기술 유출행위에 대한 빠짐없는 형사처벌만을 염두에 둔 탓으로 다음과 같이 동일한 행위에 대한 중복적 처벌규정, 형사법이론이나 원칙과 부합하지 않는 규정 또는 과잉처벌규정 등의 문제점을 드러내고 있다.

1. 제14조 1호

산업기술유출방지법 제14조 1호에서는 대상기관의 산업기술을 부정하게 취득하는 수단으로 절취・기망・협박 그밖의 부정한 방법을 제시하고 있다. 그러나, 산업기술의 부정한 취득은 부정취득만으로 그 불법성이 충분히 드러나는 행위로서 각각의 수단을 법률에서 특별히 제한할 필요는 없는 것으로 보인다[46].

이와 관련하여 대상기관의 산업기술을 부정취득(제1차 부정취득)한 자를 기망하거나 협박함으로써 또는 산업기술을 한 자의 컴퓨터를 해킹하거나 산업기술의 도면 등을 절취함으로써 대상기관의 산업기술을 취득(제2차 부정취득)하는 경우에도 동법 제14조 1호의 부정취득에 해당하는지가 문제된다. 동 법률 제14조 1항은 단순히 대상기관의 산업기술을 부정취득하는 행위를 금지하고 있을 뿐이며, 그 취득행위가 반드시 직접 대상기관으로부터 이루어져야 할 것을 요구하지 않는다. 또한 형사정책적 관점에서도 산업기술의 부정취득행위를 제1차 부정취득에 한정할 특별

45) 김정환, “산업기술의 유출방지 및 보호에 관한 법률에 대한 형사법적 검토”, 형사정책연구 제20권 제2호, 2009, 32면.

46) 이정원, “한국의 산업기술 부정유출에 대한 처벌규정의 문제점 및 대안”, 영남법학 제30호, 2010. 3, 247면.

한 이유도 존재하지 않는다. 따라서 제1차 부정취득자로부터 대상기관의 산업기술을 부정취득하는 제2차 이후의 부정취득행위가 모두 여기에 포함된다고 해석하여야 할 것이다[47].

산업기술유출방지법 제14조 1호는 대상기관의 산업기술을 부정하게 취득하는 행위 뿐만 아니라, 취득한 산업기술을 사용하거나 공개하는 행위를 금지하고 있다. 그러나, 산업기술의 부정취득 이외 사용이나 공개행위를 독자적 범죄행위로 규정할 필요가 있는가는 의문이다. 물론 산업기술의 부정취득과 부정취득한 산업기술의 사용・공개를 별개의 행위로 파악함으로써 두 범죄의 실체적 경합을 인정하는 것도 가능하다. 그러나 이는 형법에서 절취행위로 영득한 재물을 사용하거나 처분하는 행위를 별도로 처벌하는 않는 것과 같이 불가벌적 사후행위로 파악하는 것이 타당하다.

2. 제14조 2호

산업기술유출방지법 제14조 2호는 제34조의 규정 또는 대상기관과의 계약에 따라 산업기술에 대한 비밀유지의무가 있는 자가 부정한 이익을 얻거나 그 대상기관에 손해를 가할 목적으로 유출하거나 그 유출한 산업기술을 공개하거나 제3자가 사용하는 행위를 금지하고 있다. 개정전에는 비밀유지의무가 있는 자가 대상기관의 산업기술을 부정하게 유출하는 수단으로 절취・기망・협박 기타 부정한 방법을 제시하였으나 비밀유지 의무있는 자가 산업기술을 유출하는 행위는 그 수단이나 방법과 관계없이 그 자체로 불법할 뿐만 아니라, 가벌성도 충분히 인정되므로 산업기술의 부정유출을 위한 행위수단을 법률에서 특별히 규정할 필요는 없다는 지적에 따라 위 수단들을 삭제하였다.

오히려 산업기술의 부정유출자가 부정유출한 산업기술을 사용하거나 공개하는 행위가 이 조항의 핵심적 불법내용을 구성한다. 왜냐하면, 산업기술에 대한 비밀유지 의무자는 해당 산업기술을 이미 알고 있는 자이므로 해당 산업기술을 부정한 방법으로 사용하거나 공개하지 아니하고 대상기관으로부터 산업기술을 유출하는

47) 이정원, 위의 논문, 248면.

것만으로는 산업스파이행위의 불법내용을 충분히 징표하지 못하기 때문이다.

여기서 동법 제14조 2호의 '부정유출한 산업기술을 제3자가 사용하게 하는 행위'는 불필요한 중복규정이라고 생각된다. 부정유출한 산업기술을 제3자가 사용하게 하기 위해서는 해당 산업기술을 제3자에게 공개하여야만 하기 때문이다. 즉 '부정유출한 산업기술을 제3자에게 공개하는 행위'를 처벌하면서 '부정유출한 산업기술을 제3자에게 공개하여 제3자가 이를 사용하게 하는 행위'를 동일한 법조문에서 동일한 형으로 처벌하는 것은 무의미하기 때문이다[48].

3. 제14조 3호

산업기술유출방지법 제14조 3호에서는 1호(산업기술의 부정취득・사용・공개행위) 또는 2호(산업기술의 부정유출・사용・공개행위)의 규정에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 취득・사용・공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 1호 또는 2호의 규정에 해당하는 행위가 개입된 사실을 알고도 그 산업기술을 사용하거나 공개하는 행위를 금지하고 있으며, 이에 위반된 행위는 동법 제36조 1항과 2항에서 동법 제14조 1호와 2호 위반과 동일하게 처벌한다.

그러나 이 규정의 필요성은 의문시된다. 우선 대상기관의 산업기술을 부정취득(제1차 부정취득)한 자를 기망하거나 협박함으로써 또는 산업기술을 부정취득한 자의 컴퓨터를 해킹하거나 산업기술의 도면 등을 절취함으로써 대상기관의 산업기술을 취득(제2차 부정취득)하는 경우는 새로운 불법행위로 평가되기 이전에 동법 제14조 1호의 부정취득에 해당한다. 이것은 절도범이 훔친 재물을 다른 절도범이 훔치는 경우에도 그 행위는 절도죄에 해당하는 것과 같은 이치이다.

기망・협박・해킹・절취 등의 방법이 아니라 협상이나 애원 등의 방법으로 제1차 부정취득자로부터 해당 산업기술을 구매하거나 무상으로 획득하는 경우에도 제14조 3호 전단의 악의의 취득행위로 보아야 하는지 1호의 부정취득행위로 보아야 하는지가 문제된다. 그러나 이는 1호의 부정취득행위로 보는 것이 타당하다. 행위

48) 이정원, 위의 논문, 250면.

자가 해당 산업기술이 부정취득되었다는 사실을 알면서 입수하는 경우라면 어떤 방법이나 수단을 사용하든 관계없이 이를 정당한 입수나 획득으로 해석할 수는 없기 때문이다[49].

다음 부정취득・유출된 산업기술에 대한 악의의 취득행위 뿐만 아니라 이를 사용・공개하는 행위도 동일하게 처벌하고 있으나, 부정취득・유출 산업기술에 대한 악의의 취득행위가 선행되지 않고서는 이를 사용하거나 공개하는 것이 불가능하며, 악의의 취득행위가 선행된 경우에는 그 이후의 사용이나 공개행위는 불가벌적 사후행위에 불과하게 된다.

4. 제14조 4호

산업기술유출방지법 제14조 4호에서는 1호 또는 2호의 규정에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득・사용・공개하는 행위를 금지하고 있으며, 산업기술을 취득한 후에 그 산업기술에 대하여 1호 또는 2호의 규정에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 사용하거나 공개하는 행위를 금지하고 있다. 이 조항은 산업기술의 부정취득・유출 사실의 부지에 관하여 보통의 과실이 있는 경우는 처벌범위에서 제외하고 있는데, 이것은 특허 등은 등록에 의하여 공시성을 가지지만, 산업기술은 공시성이 없으므로 부당하게 기술거래를 제한할 위험이 있다는 것을 이유로 한다[50].

그러나 위 규정 후단에서 규정하고 있는 '산업기술 취득후 중대한 과실로 부정취득・유출 사실을 알지 못하고 해당 산업기술을 사용하거나 공개하는 행위'가 과연 현실적으로 발생할 수 있는지는 의문이다. 즉 이러한 행위는 산업기술 취득 당시에는 해당 산업기술이 부정 취득・유출된 사실의 부지에 대하여 무과실 또는 보통의 과실만이 인정되고, 추후에 이를 사용・공개하는 시점에서 취득한 해당 산업기술이 부정 취득・유출된 사실을 중대한 과실로 알지 못하는 경우를 의미하는데, 이러한 경우는 거의 발생하지 않는다. 과실의 정도를 판단함에 있어서는 산업기술

49) 이정원, 위의 논문, 252면.

50) 이경렬, "산업스파이범죄의 실태와 대처방안", 2009년 한국비교형사법학회 추계학술회의 발표문, 2009. 11, 60면.

의 취득 이후에 그 부정 취득·유출 사실을 알지 못하는 과실보다도 최초 해당 산업기술의 취득시점에서 그 부정 취득·유출 사실을 알지 못하는 과실을 훨씬 중대하게 평가하는 것이 원칙적이고 일반적일 것이기 때문이다[51]. 이는 명백한 입법의 오류로 보여진다.

5. 제14조 5호

산업기술유출방지법 제14조 5호에서는 지식경제부장관의 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술의 수출을 추진하는 행위를 금지하고 있으며, 이에 위반한 행위는 1호, 2호 및 3호 위반과 동일하게 처벌된다.

그러나 산업기술유출방지법이 국가핵심기술의 수출행위가 아닌 수출추진행위를 처벌의 대상으로 규정한 것에 대해서 비판이 제기되고 있다[52]. 나아가, 동 법률은 미승인 내지 부정 승인 수출추진행위에 대해서 그 미수범(동법 제36조 제6항) 뿐만 아니라 예비·음모죄(동법 제37조)를 처벌하는 규정을 두고 있다. 수출추진행위 자체가 수출행위의 미수 내지 예비·음모행위의 성격을 갖는데, 다시 그 행위의 미수 내지 예비·음모를 상정하기는 곤란하다는 것이다. 이러한 비판은 타당하며 과잉입법의 하나로 판단된다.

VII. 맺음말

형법, 부정경쟁방지법, 산업기술유출방지법 등에 의한 영업비밀 및 산업기술의 보호는 우리 산업과 기업의 기술수준이 높아짐에 따라 앞으로 더욱 실효성있게 재편되고 집행되어야 할 분야이다.

하지만, 위에서 보았듯이 위 법률을 실무에 적용할 때, 여러 가지 문제점과 해석

51) 이정원, 앞의 논문, 254면.

52) 양영준, 산업기술 유출방지 및 보호에 관한 법률에 관한 소고 - 법률내용의 검토 및 부정경쟁방지법과 비교를 중심으로, 산업보안연구논총 제3호, 2007, 23면; 이경렬, 앞의 논문, 60~61면.

상 논란이 야기되고 있다. 우선, 영업비밀의 절취에 대해서는 영업비밀이 유체물이나 관리가능한 동력이 아니므로 재물성이 부정되어 형법상 절도죄의 적용이 불가능하며, 산업스파이 행위로 인하여 발생하는 기업의 손해가 매우 추상적이고 특정하기가 곤란하여 업무상 배임죄의 적용도 용이하지 않다. 다음, 부정경쟁방지법상 영업비밀로 보호받기 위해서는 소송과정에서 영업비밀 침해를 입증하는 바, 이것이 결코 쉬운 일이 아니다. 뿐만 아니라, 소송이라는 과정이 영업비밀이 유출되거나 획득되는 경로로 사용될 가능성도 배제할 수 없다. 결국 영업비밀에 대한 침해가 발생하기 전에 회사내부에서 영업비밀을 잘 관리하여 접근통제나 접근기록을 남기는 등의 방법으로 관리하는 것이 바람직하다고 생각된다.

산업기술유출방지법의 경우 국가핵심기술을 특별한 보호대상으로 삼고 있는데 우선, '국가핵심기술'이라는 정의에 부합하는 기술의 종류와 범위를 정하는 것이 쉽지 않다. 국가핵심기술로 지정할 때에는 단순히 고도한 첨단기술이라는 점만이 고려되어서는 안되며 해당기술이 국가산업발전에 기여하는 정도와 다른 기술분야와 융합에 의한 시너지효과의 여부, 기술개발자의 창작의욕을 저해하지 않고 활성화시킬 수 있는지의 여부, 개인이나 민간기업 등의 국가핵심적 기술에 대한 취급과 그에 대한 적절한 보상과 같은 인센티브 등이 종합적으로 고려되어야 할 것이다. 현재 정부는 지난 2007. 8 21. 국가핵심기술을 선정(40개)한 바 있는데. '국가핵심기술'은 '해외로 유출되는 경우 국가의 안전보장 및 국민경제의 발전에 중대한 영향을 줄 우려가 있는 산업기술(제2조 2항)'로 정의되어 있고 세부적으로 △ 해당기술이 국가안보 및 국민경제에 미치는 파급효과 △ 관련제품의 국내외시장 점유율 △ 해당분야의 연구동향 및 기술확산과의 조화 등을 고려하여 필요최소한의 범위 안에서 선정하도록 되어 있으나 그 구분이 애매하고 경쟁기업간의 잣대로 좌지우지될 가능성이 있다는 일부 비난여론이 있어 향후 정부의 대응이 주목된다.

또한, 국가핵심기술로 지정되었을 때의 부작용도 고려하여야 한다. 예컨대, 일단 국가핵심기술로 지정되면 사기업 등이 자체개발한 국가핵심기술을 외국기업 등에 매각 또는 이전 등의 방법으로 수출하고자 하는 경우에 산업자원부장관의 승인을 얻어야 함은 물론, 승인을 얻지 못할 경우에는 해당 사기업 등의 국가핵심기술이 활성화 내지 자본화되지 못하여 산업기술의 개발이나 장려보다는 억제와 금지에

의한 기술개발 위축효과를 가져올 수 있다. 이러한 폐해를 방지하기 위해 사기업은 국가핵심기술로서 승인을 피하면서 개발기술을 노출시키지 않고 불법으로 거래할 가능성이 있다. 이점에서 국가는 국가핵심기술로 지정했을 때의 장단점을 잘 고려하여 국가핵심기술을 지정할 필요가 있다

해당기업도 국가의 법적 규제나 처벌에만 의존하여 영업비밀을 보호받으려 하기보다는 현직사원이나 퇴직사원 등 내부인에 의한 기술유출이 많다는 점을 고려하여 회사내의 핵심기술인력 관리에 세심한 관심을 기울여야 할 것으로 생각된다. 이점에서 기업내부 핵심인력의 충성도 향상을 위한 효과적인 인력관리 및 보상체계를 확립하고 외부 인력의 내부기술에 대한 접근을 차단하기 위한 다양한 관리방안을 수립・운영할 필요가 있다.

영업비밀의 유출행위에 대한 과도한 처벌만을 염두에 둔 나머지 우리 부정경쟁방지법이나 산업기술유출방지법은 전반적으로 행위유형의 불법성이 충분히 드러나지 않고, 불명확한 구성요건이 많아 가벌성여부가 법원의 자의적 판단에 맡겨질 우려가 높고, 관련자들에게 예방적 경고기능을 수행하지 못하고 있다. 앞으로 외국법제와의 구체적 비교연구를 통하여 구성요건을 구체화하고 불법성을 분명히 하는 방향으로 입법적 개선이 이루어져야 할 것이다.

참고문헌

교육과학기술부, 2009년도 기술무역통계조사보고서

권문택, 형법각칙에서 검토하여야 할 문제, 형사법개정특별위원회 편, 형법개정의 제논점, 형법개정자료(III), 1985

김정환, “산업기술의 유출방지 및 보호에 관한 법률에 대한 형사법적 검토”, 형사정책연구 제20권 제2호, 2009

박상열, “부정경쟁방지법에 의한 영업비밀의 형사법적 보호”, 지식재산연구 제6권 제3호, 2011. 9

변종필, “인터넷게임 아이템과 재산범죄”, 인터넷법률 제5호, 2001면, 44면; 하태훈, “인터넷과 형법의 변화”, 인터넷법률 창간호, 2000

송영식·이상정·황종환, 지적소유권법(하), 육법사, 2003

양영준, 산업기술 유출방지 및 보호에 관한 법률에 관한 소고 - 법률내용의 검토 및 부정경쟁방지법과 비교를 중심으로, 산업보안연구논총 제3호, 2007

윤선희, “영업비밀에 있어서의 경영상 정보”, 창작과 권리 제39호, 2005

이경렬, “산업스파이범죄의 실태와 대처방안”, 2009년 한국비교형사법학회 추계학술회의 발표문, 2009. 11

이정원, “한국의 산업기술 부정유출에 대한 처벌규정의 문제점 및 대안”, 영남법학 제30호, 2010. 3

전지연, “영업비밀의 형사법적 보호”, 형사법연구 제20권 제4호, 2008

최호진, “기업의 영업비밀에 대한 형사법적 보호”, 형사법연구 제25호, 2006년 여름

한상훈, “영업비밀침해에 대한 형사처벌의 가능성과 개선방안”, 국민대 법학연구 제14호, 2002

황의창, 부정경쟁방지및영업비밀보호법(3정판), 세창출판사, 2004

Industrial Espionage Crimes and Its Legal Control by Criminal Law

Park, Kang Woo*

Since 1990s, the world economy has been changing to knowledge-based economy in which the intangible assets such as information, knowledge and etc. are more important than the tangible assets such as labor, capital and land etc.

In terms of patent application's number, Korea is the 4th country after the U. S., Japan, Germany and China. But, Korea is still showing a deficit regarding techniques trade balance. But also, infrastructure and legislation to protect trade secret is not in good shape. Korean companies such as Samsung, Hyundai and LG are doing leading role in relevant industry, so many industrial spies are seeking to steal the trade secret in these companies. Therefore, it is necessary for the Korean Government to revise the relevant laws and regulations for the effective enforcement on the industrial spies.

This study aims to review the statistics and types of activities of industrial spies and the problems of legislation in this field. The major law in this field is the "Unfair Competition Prevention and Trade Secret Protection Act" which was revised many times. The Act prescribes specific types of acts of infringing on trade secrets. The Act also defines trade secret as any technical or operational information useful for any production and sale methods and other business activities which is not known to the public, has an independent economic value, and has been maintained in secret by considerable efforts.

However, many remain unclear as to the scope, purpose and practical applica-

* Professor, School of Law, Chungbuk National University

tion of the Act. This study will assist you to understand the concept of the industrial spy and introduce the guidance for protection the benefit of our national property and the company's profit.

❖ Key words : industrial spy, trade secret, industrial technology, unfair competition prevention and trade secret protection act, industrial technology outflow prevention

투고일 : 8월 31일 / 심사(수정)일 : 9월 14일 / 게재확정일 : 9월 24일