첨단기술의 유출방지를 위한 관련법규의 형사법적 문제점과 개선방안에 관한 연구

홍민지*

■ 목 차 ■

Ⅰ. 서 론

정보화 사회로 불리는 오늘날, 각종 과학기술 특히 컴퓨터 및 IT분야의 발달로 인해 기술은 정보라는 형태로 저장되고 보관된다. 이러한 기술정보는 이제 단순히 하나의 기록매체라는 수단적 성격을 넘어 경제적 가치를 지닌 것으로 평가받고 있으며, 더 나아가 지식재산권의 하나로써 개인적인 재산적 가치가 있는 것으로 인정받아 '재산적 가치 있는 정보' 즉 신지식재산권으로 평가받고 있다. 여기에는 정보산업재산권으로써 영업비밀과 산업기술, 첨단산업재산권으로써 반도체칩, 산업적 저작권인 컴퓨터프로그램 등이 포함된다.[1)]

첨단기술정보는 또한 개인의 재산적인 가치뿐만 아니라, 나아가서는 국가경쟁력으로까지 직결될 수 있기 때문에 현재 세계 각국은 이른바 치열한 '정보경쟁'을 벌이고 있다.[2)] 이러한 경쟁은 두 가지 측면으로 나누어 생각해 볼 수 있는데, 첫 번째는 소극적인 측면으로 자국 내에서 개발한 첨단기술을 강하게 보호하는 것이며, 두 번째는 적극적인 측면으로 다른

* 인하대학교 대학원 법학과 공법전공 박사 1차 과정

1) 홍승희, 정보재산권의 형사법적 보호와 한계, 한국형사정책연구원, 연구총서 05-13 사이버범죄연구, 2005, 19-36면 참조.

2) 첨단기술의 유출실태는 국제적으로 심각한 실정이라 하겠다. 먼저 외국의 경우를 살펴보면, 미국은 기술유출과 관련하여 연간 2,500억 달러의 손실이 발생하고 있는 것으로 추정하고 있고, 독일은 산업스파이로 인해 연간 5만 명의 실업자가 발생하는 것으로 알려지고 있다(김재봉, 영업비밀의 형사법적 보호방안, 형사정책 제14권 제1호, 2002, 175면 참조). 일본에서도 일본 기업의 해외진출이 확대되면서 기술유출 등 지적재산의 피해를 본 기업이 1996년 16.7%에서 2002년에는 28.8%로 급증하고 있어 이에 대한 대책마련이 시급하다고 한다[노상헌, 일본의 지적 재산권 강화와 근로자의 의무에 관한 법적 쟁점, 기업법연구 제20권 제3호(통권 제26호), 2005, 432면 참조].

나라에서 독자적으로 개발한 기술을 불법유출을 통해 취득하는 것이다. 우리나라 역시 최근 정보통신기술 등 첨단산업기술의 눈부신 발전으로 자국 내에서의 기술유출 뿐만 아니라 해외로의 불법적인 기술유출 또한 심각한 실정이다.[3] 이에 따라 각국은 정보획득의 끊임없는 침해 시도와 불법적인 유출발생의 심각성에 대응하기 위한 기술적 장치와 법적·제도적 처벌 장치를 마련하고 있다. 그러나 우리나라는 기술유출에 대한 형사적 처벌이 미흡한 실정이다. 현재 우리나라에 제정되어 있는 첨단기술의 유출방지를 위한 관련법규[4]에 규정되어 있는 형사적 처벌조항은 불법유출을 효과적으로 방지하는 데에 있어서 한계가 있다고 하겠다.[5]

따라서 본 연구는 첨단기술의 유출을 방지하기 위한 법적 처벌의 실효성을 제고하기 위하여 현행 관련법규를 형사법적 관점에서 고찰하도록 한다. 특히 본 논고에서는 첨단기술 유출방지 관련특별법 중에서 2006년 제정되어 2007년 4월 시행되고 있는 산업기술의 유출방지 및 보호에 관한 법률(이하 '산업기술유출방지법'이라고 약칭한다)의 문제점을 집중적으로 검토한다. 다음으로는 첨단기술의 유출방지를 위한 개선방안으로, 관련법규의 형사적 처벌 관련규정과 형사소송 관련규정의 문제점 검토를 통한 타당한 개선안을 제안하면서 본 연구를 마치고자 한다.

Ⅱ. 첨단기술 유출방지 관련법규의 주요내용

1. 주요국의 첨단기술 유출방지 관련법규

세계 각국은 첨단기술의 유출을 방지하기 위해 관련법규에 형사적 처벌을 규정하고 있다. 이에 관하여 주요국인 미국과 독일, 일본 및 중국의 관련법규를 살펴보도록 한다.

먼저 미국은 기술유출 및 침해행위에 대하여 경제스파이처벌법(Economic Espionage

3) 우리나라 또한 외국과 비슷하게 기술유출에 대한 심각성이 나타나고 있다. 최근 국내에서 발생한 기술유출 현황에 대해 살펴보면, 국가정보원은 2003년부터 2006년 12월까지 첨단기술을 국내에서 해외로 불법유출하기 위해 기도한 총 92건의 사건을 적발하였다. 연도별로는 2003년 6건에 불과하던 것이 2004년 26건, 2005년 29건, 2006년 31건 등으로 지속 증가하고 있는 추세로, 그 피해 예방액만도 82조 3천억원에 달하는 것으로 평가하고 있다(국가정보원 산업기밀보호센터, 기술유출현황, 2007. 2, 20면 참조).

4) 우리나라의 첨단기술 유출방지 관련법규에는 일반법으로 형법과 특별법으로 부정경쟁방지 및 영업비밀보호에 관한 법률, 산업기술의 유출방지 및 보호에 관한 법률, 컴퓨터프로그램보호법, 반도체집적회로의 배치설계에 관한 법률, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 통신비밀보호법 등이 있다.

5) 먼저 정보는 무체성, 즉 물리적으로 존재하지 않는다는 특성을 갖는데 이는 곧 현실적인 지배나 관리가 '객관적으로 명확하지 않다'는 의미로 결국 제3자에 의한 용이한 침해로 이어진다. 또한 무체재산(Immaterialgüter)은 '재물'로 간주되기 어렵기 때문에 이는 형법상 재물을 보호하는 법익으로 적용할 수 없다. 둘째, 공간적으로 제약을 받지 않는다는 국제성의 특징인데, 이로 인해 인터넷 등 정보통신망의 세계적 확산은 정보의 침해를 용이하게 만들었다. 최근 실질적으로 첨단기술을 유출하는 수단 및 방법에 해킹, E-mail, 도청 등이 가장 많이 사용되고 있어 기존의 법률만으로는 그 규제에 한계가 있다 하겠다(홍승희, 지식재산권 관련 형벌법규 정비방안, 한국형사정책연구원, 연구총서 06-05, 2006, 23-27면 참조).

Act, 이하 'EEA'로 약칭한다)으로 형사적 처벌을 규정하고 있는데, 동법은 주로 형사상의 보호수단에 관한 사항이 규정되어 있는 이른바 '형사영업비밀보호법'이라 할 수 있다.[6] EEA는 미연방법전 제1831조에서 제1839조까지의 경제스파이 관련 규정을 지칭하는 것으로 영업비밀 침해행위 또는 영업비밀에 대한 부정행위 중 처벌의 대상이 되는 행위로서 외국을 위한 경제스파이행위(Economic espionage)와 개인을 위한 영업비밀 침해행위(Theft of trade secret)를 설정하고 있다.[7] 그 밖에도 동법은 형사몰수(Criminal forfeiture)[8]나 소송절차에 있어서의 비공개조치(Orders to Preserve confidentiality)[9] 및 역외관할권(Applicability to conduct outside the United States)[10] 규정을 두고 있다.

독일은 주로 부정경쟁방지법(Gesetz gegen den unlauteren Wettbewerb, 이하 'UWG'로 약칭한다)을 통하여 기술유출에 대응하고 있는데, 동법에 영업비밀침해죄를 규정하고 외국으로의 기술유출에 대해 가중처벌토록 하고 있다. UWG는 2004년 전면개정을 통하여 현재 산업기밀을 보다 강하게 보호하고 있으며[11] 이는 비밀정보의 부정이용방지를 위한 형사적 처벌을 중심으로 발전하였다는 데에 그 특색이 있다.[12]

일본은 종래 영업비밀 침해에 대해서 형법을 통하여 규율하고 있다가 2003년 개정으로

---

6) 윤해성, 영업비밀보호에 관한 형사법적 연구, 성균관대학교 박사학위논문, 2006. 4, 85면 참조.

7) 먼저 경제스파이죄에 관한 규정인 제1831조는 스파이행위와 같은 간첩행위를 처벌하고자 하는 조항으로, 외국을 이롭게 하려는 의도 또는 인식이 있는 경우에 성립한다. 본죄에 관하여 EEA는 적용대상에 관한 행위태양을 세 가지 유형으로 구분하여 규정하고 있다. 다음으로 영업비밀절취죄에 관한 규정인 제1832조는 일반적인 영업비밀 침해행위를 처벌하고자 하는 조항으로, 본죄의 기본적 침해태양에 있어서는 전술한 경제스파이죄의 구성요건과 동일하다. 다만 경제스파이죄와 구별될 수 있는 점은, 영업비밀의 범위가 제한된다는 점과 소유자를 해한다는 인식을 요한다는 점이다(백성근, 미국의 지적재산권 보호 체계, 해외연수검사 연구논문, 서울북부지방검찰청, 2006. 6, 4-5면 참조).

8) 형사몰수제도를 규정한 제1834조는 본형에 부과되는 것으로 본 조항에 의하면, 위법행위를 행한 자에 대하여 형을 선고함에 있어서 달리 선고된 형에 부과하여 그 위반행위자가 위반행위를 촉진하기 위하여 어떠한 방법으로 또는 부분적으로 사용하였거나 사용하려고 의도한 위반행위자의 재산을 몰수할 수 있다(윤해성, 앞의 논문, 90-91면 참조).

9) 동법 제1835조는 영업비밀 침해행위의 피해자가 형사소송과정에서 영업비밀이 대중에게 공개되는 것을 우려하여 고소를 기피하는 것을 방지하기 위하여 법원으로 하여금 영업비밀의 비밀성을 유지하기 위한 필요하고도 적절한 명령 및 기타 조치를 취하도록 하고 있다. 이러한 조치의 예로서 소송에서 영업비밀의 상세한 내용에 대한 전문가의 증언 시 대중의 방청 제한과 소송기록 열람의 제한, 증거개시의 제한 등을 들 수 있다[곽경직, 영업비밀침해에 대한 형사적 보호, 법조 제47권 9호(통권 504호), 1998. 9, 71면 참조].

10) 동법 제1837조는 일반관할규정에 대한 예외인 역외관할권을 인정하고 있다. 동 규정은 범죄행위가 미연방이외의 지역에서 행하여진 것이라 하더라도 예외적인 경우에 한하여 역외관할권 적용이 가능하다. 이처럼 EEA가 역외관할권을 인정한 것은 경제활동의 세계화현상을 반영한 것이며[Kent B. Alexander/Kristian L. Wood, The Economic Espionage Act: Setting the Stage for a New Commercial Code of conduct, 15 Ga. St. U.L. Rew. 922(1999)] 영업비밀이나 여타 지적재산권에 대한 보호가 미약한 국가에 사무소를 갖는 기업에게 중요한 의미를 갖는다고 한다[그러나 EEA가 역외관할권을 규정하여 그 적용범위를 넓히고 있지만 인터넷 등 다양한 현대적 통신수단이 발달한 오늘날에 있어서 외국인이 외국에 머물면서 타국의 영업비밀을 침해하는 경우에는 적용될 수 없는 한계가 있다는 견해로는 류병운, 경제스파이(Economic Espionage)로부터 영업비밀(Trade Secret)의 법적보호 : 국제법 및 미국법적 제도의 검토를 통한 한국과 국제사회의 대응방향 모색, 외법논집 제17집, 2004. 11, 232-233면 참조].

11) Henning-Bodewig, Das neue Gesetz gegen den unlauteren Wettbewerb, GRUR 2004, Heft9, S.715(윤해성, 위의 논문, 101면에서 재인용).

12) 컴퓨터프로그램심의조정위원회, 주요국의 기술유출방지대책 현황 및 관련법령에 대한 검토, 연구자료, 2005, 10면 참조.

부정경쟁방지법상 형사적 처벌규정이 처음 도입되어 그 보호를 강화하였다. 이어 2005년 개정으로 동법은 영업비밀의 차원을 넘어서 '지적재산'을 보호한다는 국가전략에 따라 그 보호를 한층 강화하기 위하여 형사적 처벌이 개정되었다.[13]

중국은 산업기밀을 보호하는 '국가안전법'과 상업비밀을 보호하는 '부정경쟁방지법',[14] 인터넷관련 기밀보호법 및 대외무역법[15] 등을 통해 산업기술 및 영업비밀 유출을 방지하고 있다.

주요국의 첨단기술 유출방지 관련법규를 살펴보면, 대부분의 국가들은 기술유출 방지를 위하여 기존의 일반법보다는 특별법을 별도로 마련하여 보다 강화된 형태로 보호하고 있음을 알 수 있다. 이에 따라 우리나라 역시 일반법체계만으로는 첨단기술의 유출 및 침해행위에 대한 효과적인 방지를 기대하기 어렵다 할 수 있으므로, 이러한 측면에서 기술유출방지 관련특별법을 고찰할 실익을 찾을 수 있는 것이다.

2. 우리나라의 첨단기술 유출방지 관련법규

우리나라의 첨단기술 유출 및 침해행위처벌 관련법규에는 일반법인 형법을 비롯하여 특별법이 다수 포함되어 있다. 그러나 첨단기술의 유출 및 침해행위에 관하여 형법이 직접적으로 규율하고 있는 규정은 없고, 단지 침해행위의 특수한 형태 또는 이에 부수하는 행위만이 형법상의 범죄에 적용될 수 있을 뿐이다.[16] 이렇듯 현행 형사법규에는 첨단기술의 취득이나 누설 등의 침해행위 그 자체를 범죄행위로 보아 직접적으로 처벌하는 규정이 없기 때문에, 이 점에 있어 기술유출행위의 규제에 한계가 있는 것이라 하겠다.[17]

---

13) 2005년 개정법은 지적재산을 보호한다는 국가전략에 따라 영업비밀의 보호를 한층 강화하는 내용을 담고 있다. 그 특징으로는 우선, 법정형에 있어서 종전의 형량을 강화하였고, 침해주체의 범위를 확장하여 처벌대상에 국외범을 포함하여 확대하였다. 또한 법인의 양벌규정을 도입하고 벌칙을 강화하는 동시에 퇴직자에 의한 영업비밀의 부정사용·개시에 있어서 퇴직자의 직업선택의 자유에 대한 권리를 침해하지 않는 범위에서 악질적인 행위태양을 처벌하도록 규정하였다. 이에 더하여 이차적 취득자도 정범으로 규정함으로써 최종 취득자를 공범으로 처벌하고 있다[노상헌, 앞의 글, 422-423면 참조].

14) 먼저 '국가안전법'은 산업기밀을 국가안전의 위해로 판단하여 중형으로 처벌하고 있고, 우리나라의 부정경쟁방지법과 유사한 '반부정당경쟁법(反不正當競爭法)'은 보호대상에 관한 정의와 침해유형만 비교적 간단하게 규정하고 있는데, 처벌에 관한 규정은 형법의 규정에 의한 형사책임을 적용하고 있다(정덕배, 중국의 영업비밀 보호제도 고찰, 지식재산21, 특허청, 2002, 153면 참조).

15) '인터넷관련 기밀보호법'은 인터넷상 검열을 통해 첨단기술 및 국가기밀 유출 시에 최고형까지 처벌할 수 있는 규정을 두고 있고, '대외무역법'은 국내 특정산업의 육성 또는 그 가속화를 위한 경우 해당기술의 금지 또는 제한을 허용하는 규정을 마련하고 있다(컴퓨터프로그램심의조정위원회, 앞의 보고서, 13면 참조).

16) 형법상 적용이 가능한 관련규정으로는 '비밀침해'와 관련하는 비밀침해죄와 공무상 비밀침해죄, 비밀누설죄 및 공무상 비밀누설죄가 적용되고, '주거침입'과 관련하는 주거침입죄 및 야간주거침입절도죄와 재산범죄와 관련하는 절도죄와 횡령죄(업무상 횡령죄) 및 배임죄(업무상 배임죄), 장물죄가 적용될 수 있다. 그러나 통설과 판례의 태도에 의하면, 첨단기술'정보' 자체에 대하여 형법상 절도죄 등은 적용될 수 없고 첨단기술이 화체된 매체에 대하여만 그 매체 자체의 경제적 가치가 감소 또는 소멸되어 불법영득의 의사가 인정될 경우에 한하여 절도죄 등이 성립한다고 본다.

17) 예를 들어, 침해자가 기술이 담긴 내용에 대해서 탐지만 하고 유출시킨 경우에는 현행 형사법규상의 처벌이 불가능하다고 하겠다(권오걸, 장물의 성립요건과 범위-컴퓨터등사용사기죄와 배임죄를 중심으로-, 한국비교형

첨단기술 유출방지와 관련된 특별법에 속하는 법률들은 보호목적과 그 대상에 있어 특수성을 가지고 제정된 것이다. 부정경쟁방지 및 영업비밀보호에 관한 법률(이하 '영업비밀보호법'이라고 약칭한다)은 민간기업의 '영업비밀'을 보호대상으로 하는데, 동법은 이를 보호하기 위해 침해행위의 유형과 처벌행위 및 형사적 처벌에 관하여 규정하고 있다.[18] 산업기술유출방지법은 '산업기술'과 '국가핵심기술'을 보호대상으로 하며 그에 대한 유출 및 침해행위의 금지 및 형사적 처벌을 규정하고 있다.[19]

그 밖에도 컴퓨터프로그램의 불법복제행위나 반도체유출행위의 효율적인 규제를 위한 컴퓨터기술을 보호하는 관련법규에는, 컴퓨터소프트웨어를 보호하는 '컴퓨터프로그램보호법'과 컴퓨터반도체회로를 보호하는 '반도체집적회로의 배치설계에 관한 법률'이 있다.[20] 또한 첨단기술의 보호를 직접 목적으로 하는 것은 아니나, 정보기술을 보호하는 관련법규로, '정보통신망'을 보호하기 위하여 해킹과 바이러스를 통한 산업스파이 행위를 규제하는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라고 약칭한다)과 통신 및 대화비밀의 감청 등을 처벌하는 통신비밀보호법[21] 등이 있다.

Ⅲ. 산업기술유출방지법의 형사법적 문제점 검토

첨단기술의 영역에 속하는 '산업기술'과 '국가핵심기술'은 국책사업으로 진행되는 연구·개발분야를 포괄하는 개념으로 그 범위에 있어 모든 기술을 포함하기 때문에 광의의 개념이라 하겠다. 따라서 기존의 법률만으로는 그 보호에 한계가 있기 때문에 산업기술유출방지법이 특별법의 형태로 제정되어 시행되고 있는 것이다. 그러나 동 법률은 보호대상의 개념정의규정과 유출 및 침해행위태양, 중과실 및 미수범의 처벌성립여부에 있어 형사법적으로 문제시

사법학회, 비교형사법연구 제8권 제2호, 2006, 11-12면 참조). 따라서 이를 극복하기 위하여 첨단기술은 그 자체가 개개단위의 정보가 합체된 하나의 종합정보와 함께 단편으로 된 부분정보도 포함해야 하며 유·무형적인 정보를 모두 포함해야 적용이 가능할 것이다.

18) '영업비밀'에 관하여는 동법 제2조 제2호에서 규정하고 있는데, 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서 노력에 의하여 비밀로 유지된 생산방법·판매방법 기타 영업활동에 유용한 기술상 또는 경영상 정보라고 정의하고 있다. '영업비밀 침해행위'에 관하여는 동조 제3호에서, 미수와 예비·음모에 관한 처벌규정은 제18조2와 3에서 규정하고 있다. 그 밖에도 동법은 병과규정 및 양벌규정도 마련하고 있다.

19) 산업기술유출방지법은 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하며 국가의 안전보장과 국민경제의 발전에 이바지함을 목적으로 한다. 동법은 산업기술과 국가핵심기술을 유출 및 침해하는 행위에 대하여 '국외'유출행위와 '국내'유출행위를 구분하여 전자를 가중처벌하고 있으며, 동 행위에 대한 미수범처벌과 이를 범할 목적으로 예비 또는 음모하는 행위의 처벌에 있어서도 형량에 차등을 두고 있다. 그 밖에도 몰수 및 추징에 관한 규정과 병과규정 및 양벌규정도 마련하고 있다(동법 제36조 내지 제37조 참조).

20) 최근 첨단산업기술이 유출되는 분야에 있어서 소프트웨어 및 반도체기술이 대다수를 차지하고 있는 점에 비추어 일반적인 기업의 영업비밀이나 산업기술의 범위만으로는 이를 보호하는 데에 한계가 있다고 할 수 있다.

21) 통신비밀보호법은 통신 및 대화비밀의 보호규정에 위반하는 행위를 금지하고 있는데, 이는 컴퓨터통신을 이용하여 영업비밀을 송수신하는 경우에 해킹을 통하여 알아내는 것 또한 동법으로 금지·처벌하는 전기통신의 감청에 해당된다고 규정하고 있다(강동범, 사이버범죄와 형사법적 대책-제25회 형사정책세미나 자료집, 한국형사정책연구원, 2000, 82면 참조).

되고 있으므로 이에 관하여 논의하도록 한다.

1. 보호대상의 개념정립 문제

(1) 정의 개념의 명확성 문제

동법 제2조 제1호·제2호는 보호대상인 '산업기술' 및 '국가핵심기술'에 관하여 개념을 정의하고 있는데, 이를 정의한 규정에서 일부 법문[22]이 가치개념에 속하는 것으로 형법의 기본개념인 죄형법정주의의 명확성원칙에 반하는 것이 아닌지 검토가 요청된다.

1) 죄형법정주의의 명확성원칙 위배 문제

어떤 행위가 범죄로 되고 그 범죄에 대하여 어떤 처벌을 할 것인가는 미리 성문의 법률에 규정되어 있어야 한다는 원칙을 죄형법정주의라고 한다.[23] 죄형법정주의의 원칙 중 명확성의 원칙(lex certa, Bestimmtheitsgrundsatz)은 법률에 범죄와 형벌을 가능한 한 명확하게 확정하여야 법관의 자의를 방지할 수 있고 국민으로서도 어떤 행위가 형법에서 금지되고 그 행위에 대하여 어떤 형벌이 과하여지는가를 예측하게 되어 규범의 의사결정효력을 담보할 수 있다는 데 그 근거가 있다.[24]

명확성의 원칙은 형벌법규에 범죄와 형벌을 명확하게 규정할 것을 내용으로 하는데, 그 핵심은 구성요건에 금지된 행위를 명확하게 규정하는 데 있다. 따라서 구성요건이 어느 정도 특정되어야 명확성의 원칙에 반하지 않는가를 판단함에 있어서는 예견가능성(Vorhersehbarkeit)과 가치판단(Wertentscheidung), 구체화의 가능성 및 비례성원칙의 기준을 종합하여 구체적으로 타당한 결론을 내려야 한다.[25] 다음으로 명확성의 원칙을 판단함에 있어서는 용어의 사용이 입법기술상 불가피한 것인가도 고려되어야 하는데, 별다른 어려움 없이 구체화할 수 있는 경우에는 이에 반한다고 해야 한다.[26]

---

22) "산업기술"에 대한 개념정의를 하고 있는 동법 제2조 제1호에서 가목의 '… 선진국 수준과 동등 또는 우수하고 …' 부분과 다목의 '… 국가기술력 향상과 대외경쟁력 강화에 이바지할 수 있는 기술' 부분, "국가핵심기술"에 대한 개념정의를 하고 있는 동조 제2호의 '… 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술로서 …'의 부분이 형법상 죄형법정주의 원칙 중 명확성원칙에 위배되는 것이 아닌지 검토가 요구된다 하겠다.

23) 형법 제1조 제1항이 '범죄의 성립과 처벌은 행위시의 법률'에 의한다고 규정하고 있는 것도 형법의 기본원리로서 이를 규정한 것이라고 볼 수 있다.

24) 이재상, 형법총론, 2006, 9-14면 참조.

25) 여기에서의 예견가능성은 특정한 행위가 처벌되는가가 행위 이전에 확정되어 있어야 한다는 의미에서 객관적인 의미로 이해되어야 한다. 또한 법률이 사법에 대한 믿을 수 있고 확고한 기준을 제시할 것을 요구하는데, 법률이 가치판단, 즉 구체적인 보호법익 자체를 법관에게 위임한 때에 이는 명확성의 원칙에 반한다고 해야 한다(이재상, 앞의 책, 21-23면 참조).

26) 헌법재판소도 형사적 처벌의 대상이 되는 범죄의 구성요건은 형식적 의미의 법률로 명확하게 규정되어야 하며 만약 범죄의 구성요건에 관한 규정이 지나치게 추상적이거나 모호하여 그 내용과 적용범위가 과도하게 광범위하거나 불명확한 경우에는 국가형벌권의 자의적인 행사가 가능하게 되어 개인의 자유와 권리를 보장할 수 없으므로 죄형법정주의의 원칙에 위배된다고 하여 이 원칙의 취지를 밝히고 있다(헌재 판결 1995. 9. 28, 93헌바50 참조).

2) 소결

동법이 규정하고 있는 보호대상의 범위는 영업비밀보호법상의 '영업비밀' 규정이나 'EEA의 규정'[27]에 비해 추상적이고 포괄적이라 할 수 있다. 물론 보호대상을 확대하기 위해 산업기술의 기본적인 범위를 다소 포괄적으로 명시하면서 규제적인 요소는 축소하고자 적용대상기술을 열거하고 있다는 취지라고 하겠으나, 당해 정의규정은 가치개념에 속하는 것으로 이 경우 해석상 많은 문제점을 야기할 위험을 충분히 내포하고 있다.[28] 따라서 이는 형법의 기본개념인 죄형법정주의의 명확성원칙에 반하는 것이라 할 수 있다.

실질적으로 '산업기술'이라는 개념은 국책사업으로 진행되고 있는 국공립연구소나 민간연구소, 공공기관 등이 연구·개발하는 분야를 포괄하는 것이므로, 그 범위에는 민간기업의 '영업비밀'도 포함된다고 할 수 있다. 또한 '국가핵심기술'의 개념에 있어서도 핵심기술, 즉 앞서 언급한 산업기술이나 영업비밀 등이 모두 포함되는 광의의 개념으로, 다만 해외로 유출되는 경우 국가안보나 국가경제에 손해를 끼치는 정도의 국내 자체생산 및 연구기술을 의미한다고 본다.

따라서 '산업기술'의 개념에 있어서는 문제시되는 법문을 삭제하는 것이 타당하고, 대신 '기술집약도가 높고 기술혁신속도가 빠른 기술로 산업구조의 고도화에 대한 기여가 큰 기술'이나 '신규수요 및 부가가치 창출효과와 산업간 연관 효과가 큰 기술' 등의 구체적이고 개념해석에 있어서 문제제기가 비교적 적은 명확한 개념을 사용하는 것으로 개선되어야 한다고 생각한다. '국가핵심기술'의 개념 또한 '중대한 악영향'이라는 애매모호한 개념보다는 '심각한 피해'의 표현이나 '손해' 등의 구체적인 법문의 표현으로 개선하는 것이 타당하다고 본다.

(2) 행위대상의 재물성 문제

동법 제14조 제1호 및 제2호에서는 산업기술의 유출 및 침해행위 금지에 대한 행위태양으로 '절취'를 규정하고 있는데, 여기서 문제되는 것은 절취개념에 대한 행위대상으로 '산업기술'이 과연 타당한 것인지 검토가 요구된다.

1) '산업기술'의 재물성 여부 문제

---

27) EEA에서 영업비밀에 관한 규정은 민·형사간의 구분 없이 세 가지 기본조건이 필요하다. 첫째, 영업비밀은 현실적 정보로 구성되어야 하지만 그 정보는 다양한 형태로 존재할 수도 있다. 둘째, 정보는 반드시 가치가 있어야 하므로 일반적으로 알려져 있지 않고 적절한 수단을 통하여 쉽게 확인되지 않는 실제적 혹은 잠재적 독립적 경제가치가 있어야 한다. 셋째, 소유자가 정보를 비밀로 유지하려고 해야 하는데, 그러한 정보의 비밀유지를 위하여 합리적 조치를 취하고 있을 것을 요구한다(18 U.S.C. 제1839조 참조).

28) 추상적이고 가치개념적인 요소를 내포한 정의규정은 그 개념해석에 있어서 여러 문제점을 야기할 수 있다. 보호대상에 관한 개념해석의 중요성은 범죄행위의 여부를 판단하는 기준이 될 뿐 아니라 더 나아가 형사적 처벌의 실효성까지도 담보하기 때문이다. 또한 개념의 해석에 있어서 검찰과 법원이 서로 상이할 경우, 검찰의 기소권남용과 법원의 법적용 혼란 및 처벌의 부재로 이어질 가능성도 배제할 수 없는 것이다(최호진, 기업의 영업비밀에 대한 형사법적 보호 -부정경쟁방지및영업비밀보호법을 중심으로-, 형사법연구 제25호, 2006 여름, 397-398면 참조).

‘산업기술의 유출 및 침해행위’로써 처벌대상이 되는 행위태양인 ‘절취’의 개념에 대해 형법적으로 검토할 필요가 있는데, 여기서는 산업기술을 유체물화 한 경우와 산업기술 자체에 대한 경우(무체물)를 구분하여 논의해야 한다. 절취개념은 절도죄를 구성하는 행위태양으로 그 행위대상은 ‘재물’에 한한다. 만일 ‘산업기술을 절취한다’는 규정이 타당하기 위해서는 ‘산업기술’이 절취개념의 대상인 ‘재물’로 인정되어야 하는 것이다.

형법상 ‘재물’은 재산죄의 객체로써 ‘관리할 수 있는 동력’이라고 간주하는데, 이에 관하여 다수설인 ‘관리가능성설’은 관리가 가능한 것이면 유체물 이외에 무체물도 재물이 된다고 보고 있다.[29] ‘관리할 수 있는 동력’에서 ‘관리’의 의미는 통설과 판례에 의하여 ‘물리적 관리’를 말한다. 따라서 정보·기획 등은 물리적인 관리가 불가능하므로 재물이 아니라고 하겠다. 그러나 정보가 수록된 USB 등의 물건은 재물에 해당한다.[30] 또한 ‘정보’의 재물성에 대하여 대법원은 ‘정보’ 그 자체는 유체물이라고 볼 수도 없고 물질성을 가진 동력도 아니므로 재물이 될 수 없다고 판시하였다.[31]

2) 소결

재물의 개념은 형법상 소유권범죄의 의의와 목적에 따라 결정되어야 하므로, 관리가능성설에 따라 무체물도 형법적 보호의 대상으로 해야 한다고 본다. 또한 재물로 간주되는 ‘관리할 수 있는 동력’은 물리적 관리가 가능한 것을 말하므로 ‘정보’ 자체는 재물이 아니지만, 정보가 유체물에 화체된 것은 재물에 해당한다고 하겠다. 따라서 산업기술이 ‘유체물’에 화체된 경우, 즉 CD, USB메모리 등에 저장된 형태의 경우에는 그 자체가 물리적 관리가 가능하므로 관리할 수 있는 동력인 재물로 인정될 수 있다. 그러므로 화체된 산업기술을 유출하는 행위는 절도죄가 성립되기 때문에 이에 대한 ‘절취’개념은 타당하다고 하겠다. 그러나 산업기술이 ‘정보’ 자체의 형태인 경우에는 재물로 간주할 수 없어 이를 유출하는 행위는 절도죄가 성립할 수 없게 된다. 따라서 이 경우 ‘절취’는 성립할 수 없는 개념이 된다.

생각건대 형사적 처벌을 가능하게 하는 행위유형의 규정이 동 개념을 유지한다면, 이는 형법의 기본원칙에도 위배되는 것이 되며 형법상 개념인 ‘절취’라는 용어를 사용할 필요성은 없다고 보여 진다. 따라서 산업기술이 ‘정보’ 자체의 형태인 경우에는 동 규정의 ‘절취’

---

29) ‘관리가능성설’에 의하면 유체물이 재물이 되는 것은 그것이 유체물이기 때문이 아니라 사람의 관리·지배에 귀속시킬 수 있기 때문이고, 과학기술의 진보에 따라 관리할 수 있는 무체물에 대해서도 형법상의 재산죄에 의한 보호가 필요하며 소유권이란 물권을 배타적으로 사용·수익·처분할 수 있는 권리를 의미하는데 관리가 가능하다는 것은 배타적 지배가 가능하다는 것을 의미한다는 점을 그 논거로 한다(이재상, 형법각론, 2005, 227면 참조).

30) 이재상, 위의 책, 228-229면 참조. 따라서 예를 들면, 산업정보 스파이행위는 절도죄가 성립하지 않는다.

31) 대법원 2002. 7. 12, 선고 2002도745 판결 [절도]참조, 「**컴퓨터 속의 정보를 빼내갈 목적으로 종이에 출력하여 가져간 경우**, 절도죄의 객체는 관리 가능한 동력을 포함한 ‘재물’에 한한다 할 것이고, 또 절도죄가 성립하기 위해서는 그 재물의 소유자 기타 점유자의 점유 내지 이용가능성을 배제하고 이를 자신의 점유 하에 배타적으로 이전하는 행위가 있어야만 할 것인바, **컴퓨터에 저장되어 있는 ‘정보’ 그 자체는 유체물이라고 볼 수도 없고 물질성을 가진 동력도 아니므로 재물이 될 수 없다** 할 것이며, 또 이를 복사하거나 출력하였다 할지라도 그 정보 자체가 감소하거나 피해자의 점유 및 이용가능성을 감소시키는 것이 아니므로 그 복사나 출력 행위를 가지고 절도죄를 구성한다고 볼 수도 없다.」

개념은 형법적으로 타당하다고 할 수 없으므로, 관련 규정을 '권한 없는'으로 정정하는 것이 타당하다고 생각된다.

2. 유출 및 침해행위 규정에 관한 형법적 타당성 문제

산업기술의 유출 및 침해행위를 규정한 동 조항에서 문제되는 것은 '절취'개념과 '기망·협박'개념을 같은 행위태양으로 표현한 것이 과연 법률문언에 있어서 명확성원칙에 부합하는지 검토가 요청된다.

(1) 절취와 기망·협박에 대한 규정의 문제점

먼저 절취는 보호대상에 대하여 행위주체(침해자)가 행하는 '행위'개념이고, 기망·협박은 행위객체인 보호대상의 권리자(사람)에 대하여 행위주체가 행하는 '행위수단'으로써의 개념이라고 할 수 있다. 따라서 행위로써의 '절취'와 그 수단으로써의 '기망·협박'의 개념을 구분하여 법문의 내용에 규정하는 것이 명확성에 부합하는 것인지 검토한다.

1) 행위개념의 형사법적 고찰

먼저 절취의 개념을 살펴보면, '절취'는 절도죄의 행위로써 타인점유의 재물에 대하여 점유자의 의사에 반해서 그 점유자의 점유를 배제하고 자기 또는 제3자의 점유로 옮기는 것을 말한다.[32] 이와 달리 '기망'은 사기죄의 '수단'이 되는 기망행위에 해당하는 개념으로 허위의 의사표시에 의하여 타인을 착오에 빠뜨리는 일체의 행위를 말하는데,[33] 사기죄는 편취행위를 위한 '수단'으로 기망을 요하는 것이다. 또한 '협박'은 형법상 재산범죄에 해당하는 강도죄와 공갈죄의 '수단'이 되는 개념으로, 강도죄는 강취행위를 위한 '수단'으로 협박을 요하고 공갈죄는 본죄의 수단이 되는 공갈행위에 협박을 포함한다. 양 죄에서 인정하는 협박은 정도에 있어서는 차이가 있으나, 본질에 있어서 차이가 있는 것은 아니다.[34]

2) 재산죄의 분류에 따른 각 행위개념의 구분

침해방법에 의한 재산죄의 분류를 살펴보면, 재산죄는 탈취죄(奪取罪)와 편취죄(騙取罪)로 나누어볼 수 있다. 먼저 '탈취'죄는 타인의 의사에 반하거나 적어도 그 의사에 의하지 않고 재산을 취득하는 범죄로, 절도죄와 강도죄 등이 이에 속한다. 또한 '편취'죄는 타인의 하자있는 의사에 의한 처분행위에 의하여 재산을 취득하는 범죄로, 사기죄와 공갈죄가 속한다.[35]

---

32) 이재상, 앞의 책, 307면; 김일수, 형법각론, 2004, 243면 참조.
33) 이재상, 위의 책, 300면; 김일수, 위의 책, 355면 참조.
34) 강도죄와 공갈죄에 있어서 협박개념은, 협박의 '정도'에 따라 성립하는 범죄가 달라지는데, 협박이 상대방의 반항을 억압할 정도일 경우에는 강도죄가 성립하나 공갈죄에서의 공갈행위에 속하는 협박은 사람의 의사결정과 행동의 자유를 제한하는 정도로 충분하다[배종대, 형법각론, 2004, 456면 참조].
35) 김일수, 위의 책, 224면; 정성근·박광민, 형법각론, 2002, 319면 참조.

(2) 소결

산업기술의 유출 및 침해행위에 대한 행위태양으로 절취, 기망 및 협박개념을 동종의 유형으로 규정하는 것은 타당하지 않다고 본다. 각 개념은 첫째, 다른 행위대상에 대하여 하는 행위개념이라는 점과 둘째, 재물과 재산상의 이익에 있어서 서로 다른 보호대상을 갖는다는 점에 비추어 볼 때 동종의 유형으로 규정하는 것도 문제가 있다. 또한 재산죄의 분류에 있어서도 각 개념은 침해방법상 다르다고 할 수 있다. 절취는 탈취죄에 해당하는 행위개념이고, 기망과 협박은 편취죄에 해당하는 행위수단의 개념이기 때문이다. 구체적으로 기망과 협박을 검토해보면, 두 개념도 허위의 의사표시와 해악의 고지라는 것이 행위의 수단으로 사용되었을 경우에 각 범죄의 본질에 차이가 있다고 할 수 있다. 따라서 위의 개념을 동종의 행위태양으로 표현한 것은 법률문언의 명확성에 타당하지 않는 규정이라고 하겠다.

생각건대, 미국의 EEA규정[36]을 참고하여 당해 규정을 '산업기술을 권한 없이 취득하거나 기망·협박 또는 그 밖에 부정한 방법으로 취득하는 행위'의 법문으로 개선하는 것이 죄형법정주의에 부합하는 것이라 본다.

3. 중과실에 의한 침해행위 처벌의 가능성 문제

동법 제14조 제4호는 유출 및 침해행위가 개입된 사실을 '중대한 과실'로 알지 못하고 취득·사용 및 공개하는 행위를 금지하고 있다. 여기서 문제되는 것은 중과실에 의한 유출 및 침해행위 중에서 사용하거나 공개하는 행위를 제외하고 단순히 산업기술을 '취득'하기만 한 경우에도 처벌이 가능한지 검토가 요구된다.

(1) 중과실범의 성립 여부 문제

산업기술의 취득과정에서 사소한 부주의로 기술침해행위를 예견하지 못한 경우 중과실이 성립될 수도 있다. 그러나 주의의무를 위반하여 단순히 산업기술의 내용을 인지하는 '취득'의 경우에 형법의 적용대상으로 처벌할 수 있는 중과실범이 성립할 수 있느냐 하는 것이다. 이를 판단하기 위해서는 과실범의 구성요건을 검토하여야 한다.

1) 과실범의 개념

과실(Fahrlässigkeit)이란 정상의 주의를 태만히 함으로 인하여 죄의 성립요소인 사실을 인식하지 못하는 것을 말한다. 즉 사회생활에서 요구되는 주의의무를 위반함으로써 구성요건적 결과가 발생하는 경우에 형벌이 과하여지는 범죄가 바로 과실범이다. 과실에는 일반인에게 통상적으로 요구되는 주의의무에 위반하는 보통의 과실과 구분하여 중대한 과실을 가중처벌하고 있는데, 이를 '중과실'이라고 한다. 중과실이란 주의의무를 현저히 태만히 하는

36) 미국은 EEA 제1831조 (a) (1)에서 '기업비밀을 절취하거나… 기망 또는 속임수로 기업비밀을 취득하는 행위…'라고 하여 절취와 기망의 개념을 구분하여 규정하고 있음을 알 수 있다.

것, 즉 극히 근소한 주의만 하였더라면 결과발생을 예견할 수 있었음에도 부주의로 이를 예견하지 못한 경우를 말하는데, 이를 판단하는 기준은 구체적인 경우에 사회통념을 고려하여 결정하여야 한다.[37]

2) 과실범의 구성요건

과실범의 구성요건해당성은 행위반가치와 결과반가치에 의하여 결정되는데,[38] 행위반가치는 주의의무위반 즉 부주의(不注意)에 있고 결과반가치는 결과의 발생과 그에 대한 인과관계라 할 수 있다. 따라서 과실범의 구성요건으로는 주의의무위반, 결과발생 및 결과에 대한 인과관계를 요한다. 여기에서는 행위자의 '취득'행위가 과실범의 주의의무위반과 결과발생의 구성요건에 해당하는지 검토하도록 한다.

먼저 주의의무위반에 관하여 검토하면, '주의의무'의 내용은 구체적인 행위로부터 발생할 수 있는 보호법익에 대한 위험을 인식(예견)하고 구성요건적 결과의 발생을 방지하기 위하여 적절한 방어조치를 취하는 데 있다.[39] 따라서 주의의무위반이라 함은 객관적 주의의무의 침해 또는 사회생활에서 요구되는 주의의 태만을 의미한다. 주의의무위반을 판단하는 기준에 관하여는 견해가 대립되고 있는데, 통설인 객관설에 의하면 주의의무위반은 행위자가 가상의 판단에 의하여 보호의 객체가 위험하다고 인식할 수 있었다면 인정되는 것이다.[40] 따라서 객관적 주의의무위반은 행위자의 위치에 있는 통찰력 있는 사람의 지도형상, 즉 행위자가 소속한 거래범위의 신중하고 사려 깊은 사람의 판단이 기준이 되므로 예컨대, 산업보안회사 등의 '연구원'들은 사소한 주의의무만으로도 기술유출을 방지할 수 있기 때문에 주의의무위반이 인정될 수 있다.

다음으로 취득행위의 경우에 따른 형법상 '결과발생'의 가능성을 살펴보면, 과실범은 구성요건으로서 법익의 침해 또는 위험이라는 구성요건적 결과를 필요로 한다. 여기서 형법상 '결과발생'은 구성요건상의 결과반가치에 해당하는 것으로, 침해란 현실적으로 발생한 법익의 손상으로 보호법익에 대한 직접적인 가치상실을 의미하고, 위험은 보호법익에 대한 침해의 발생이 가능한 상태를 말한다. 따라서 산업기술을 취득하는 행위 중에서 산업기술이 유체물로 화체된 것을 직접 행위자의 점유로 옮기는 경우는 보호법익인 산업기술에 대한 침해의 위험이 인정되므로 형법상 '결과발생'이 인정된다.

---

37) 이재상, 앞의 책, 182면; 박상기, 형법총론, 2005, 277면 참조. 대법원 판례 1980. 10. 14, 79도305 참조.

38) 행위반가치와 결과반가치의 기능을 파악하는 것은 불법론의 가장 중요한 논점인데, 이는 위법성의 문제에 그치는 것이 아니라 불법의 개념에 관한 문제이다. 결과반가치와 행위반가치는 구성요건해당성과 관련되는 문제이며 이에 의하여 무엇이 구성요건요소가 될 수 있는가가 결정된다(이재상, 위의 책, 106면 참조).

39) 이는 예견의무와 결과회피의무를 그 내용으로 하는데, 이에 대한 판단기준으로 구성요건요소로서 객관적으로 결정해야 한다는 견해인 객관설이 통설의 입장이다(이재상, 위의 책, 182-183면; 박상기, 위의 책, 282면 참조).

40) 객관설은 주의의무위반을 「객관적 주의의무의 침해」(Verletzung der objektiven Sorgfaltspflicht) 또는 「사회생활에서 요구되는 주의의 태만」(Vernachlässigung der im Verkehr erforderlichen Sorgfalt)을 의미한다고 한다.

또한 취득행위로써 '내용만 탐지한 행위'의 경우에는 보호법익의 침해나 또는 위험행위 자체로 볼 수 없다. 그러나 보호법익의 침해정도에 따라 형법상 침해범과 위험범[41]으로 구분하여 볼 때, '내용을 인지하여 취득한 행위'는 구성요건이 전제로 하는 보호법익에 대한 위험의 야기로 족한 범죄인 '위험범'에 해당한다고 할 수 있게 된다. 즉, 동 행위는 보호법익인 산업기술에 대한 침해 및 유출을 야기한 것으로 간주할 수 있으므로 형법상 결과발생이 인정된다고 하겠다. 이에 관하여 형법은 보호법익의 침해정도에 따라 침해범과 위험범으로 구분하고 있는데, 내용을 인지하여 취득한 행위는 보호법익인 산업기술에 대한 침해 및 유출의 위험을 야기한 것으로 간주할 수 있으므로 이는 위험범에 해당하여 형법상 결과발생이 인정된다고 하겠다.

(2) 소결

동 규정에서 문제되는 중과실에 의한 산업기술의 취득은 법익에 대한 침해의 결과를 인정하기는 어렵지만, 법익에 대한 위험의 발생은 인정할 수 있을 것이다. 형법상 결과발생은 법익의 침해 또는 위험이라는 구성요건적 결과를 의미하므로, 주의의무위반으로 인하여 법익에 대한 위험이 발생하는 경우에도 과실범이 성립할 수 있게 된다. 따라서 본인의 사소한 주의의무위반으로 산업기술을 취득하는 경우는 산업기술유출의 위험이 발생하는 경우에 해당하므로, 중과실에 의해 산업기술을 취득하는 행위는 처벌할 수 있을 것이다.[42] 다만, 객관설에 의해 과실 즉 주의의무위반은 고의와 마찬가지로 구성요건요소와 책임요소로서의 2중의 기능을 가지고 있으므로 주관적 주의의무는 책임문제로 고려되어야 한다고 본다.

4. 미수범의 처벌 가능성 문제

동법 제36조 제6항은 산업기술의 국내·외 유출 및 침해행위에 대한 미수범처벌을 규정하고 있는데, 그 내용으로 금지행위 중에서 '취득'만 하거나 '유출'만 한 행위가 포함된다. 여기서 문제로 제기되는 것은 '취득'만 하거나 '유출'만 한 행위에 대한 미수범처벌의 성립여부, 즉 산업기술을 '취득'하거나 '유출'하는 행위가 기수가 되는 경우에 미수범이 성립하는지 검토가 요구된다.

(1) 미수범의 성립 여부

41) 위험범(Gefährdungsdelikte)이라 함은 구성요건이 전제로 하는 보호법익에 대한 위험의 야기로 족한 범죄를 말한다. 이는 다시 구체적 위험범과 추상적 위험범으로 나누어지며, 법익침해의 구체적 위험인 실체적 위험의 발생을 요건으로 하는 범죄를 구체적 위험범(konkrete Gefährdungsdelikte)이라고 한다(이재상, 앞의 책, 70면 참조).

42) 다만, 이러한 경우에 중과실의 범위는 사회통념을 고려하여 그 주의의무의 범위를 명확히 확정할 수 있어야 할 것인데, 형법의 해석상 객관적 주의의무위반은 일반적으로 인정된 기술이나 과학상 규정 또는 경험칙에 의하여 판단될 수 있는 것이라고 할 수 있겠다.

형법 제25조 제1항에 의하면, 미수범(Versuch)이란 범죄의 실행에 착수하여 행위를 종료하지 못하였거나 결과가 발생하지 아니한 때를 말한다. 미수범은 범죄 실행에 착수하였다는 점에서 예비와 구별되며, 미수와 예비의 구별은 행위의 가벌성을 결정하는 데 중요한 의의가 있다.[43] 따라서 미수가 되기 위해서는 「범죄 실행의 개시(Anfang der Ausführung)」를 의미하는 실행의 착수(der Beginn der Ausführung)가 있어야 한다.[44]

미수범이 성립하기 위해서는 실행에 착수하여 행위를 종료하지 못하였거나 결과가 발생하지 아니할 것을 요한다. 그러나 미수범에 있어서도 고의, 즉 구성요건실현의 결의가 있어야 한다. 따라서 미수범의 구성요건으로는 주관적 구성요건으로서의 고의와 객관적 구성요건으로서 실행의 착수 및 범죄의 미완성이라는 세 가지 요건이 필요하다고 할 수 있다. 여기서는 객관적 구성요건인 실행의 착수와 관련하여 검토하도록 한다.

1) 실행의 착수에 관한 학설 및 판례의 입장 검토

실행의 착수시기에 관하여 대립하고 있는 견해들[45] 중에서 절충설, 즉 주관적 객관설(subjektiv-objektive Theorie)에 의하면, 실행의 착수가 있느냐에 대한 본질적인 기준은 보호되는 행위의 객체 또는 구성요건의 실현에 대한 직접적 위험이지만 여기에 해당하느냐의 여부는 주관적 표준, 즉 개별적 행위계획에 의하여 결정되어야 한다는 것이다. 따라서 이를 개별적 객관설(individuell-objektive Theorie)[46]이라고도 한다. 이는 독일의 통설일 뿐 아니라 우리 형법의 해석에 있어서도 타당한 견해라 할 수 있다.[47]

그러나 판례의 원칙적 입장은 실질적 객관설, 특히 밀접행위설을 따르는 것으로 평가된다. 실질적 객관설은 구성요건해당 행위라는 엄격한 법률적 형식이 아니라 다른 실질적 관점에서 판단하려는 견해를 말하는데, 이에 대법원은 “법익침해에 밀접한 행위가 있으면 실행의 착수가 있다”고 한다.[48] 이러한 판례의 견해에 의할 때 산업기술을 취득하기 위한 특정한 목적, 즉 부정한 목적도 표명되지 않은 상태에서 부정한 수단에 의한 기술취득에 밀접한 행위의 범위를 명확하게 한정하는 것이 쉽지는 않다. 더욱이 본 죄에 대한 예비·음모에 대해서까지 처벌해야 한다면 취득 이전의 밀접한 행위가 예비행위, 즉 기술취득을 위한 준비행위인지 혹은 실행의 착수에 해당하는 행위인지 구별하기가 쉽지 않다. 예컨대 기술을

43) 이재상, 앞의 책, 343면; 배종대, 형법총론, 2005, 506면 참조.
44) 이재상, 위의 책, 348면 참조.
45) 그 외에도 객관설(objektive Theorie)이란 실행행위의 개념을 객관적 기준에 의하여 정해야 한다는 견해이다. 형법은 구성요건에 규정된 행위를 실행하는 것을 처벌하므로 실행의 착수에 대한 기준은 「구성요건에 해당하는 실행행위」여야 한다는 이론으로, 법률에 기술해 놓은 구성요건에 해당하는 정형적인 행위 또는 적어도 정형적인 행위의 일부를 개시한 때에 인정해야 한다는 견해인 형식적 객관설과 실질적 객관설이 있다. 주관설(subjektive Theorie)은 범죄의사의 수행성 또는 확실성이라는 주관적 기준을 가지고 이를 명백하게 인정할 수 있는 외부적 행위가 있을 때에 이를 인정하려는 견해이다(손동권, 형법총론, 2005, 400면 참조).
46) 독일 형법 제22조는 「그의 의사에 의하여 직접 구성요건이 실현되는 행위를 개시한 자는 미수이다」라고 규정하여 명문으로 주관적 객관설의 입장을 명백히 하고 있다(이재상, 앞의 책, 350-351면 참조).
47) 김일수, 앞의 책, 421면; 배종대, 앞의 책, 428면 참조.
48) 대법원 1983. 3. 8, 선고 82도2944 판결; 1999. 9. 17, 선고 98도3077 판결 등 참조. 「‘절도죄 등 죄’에서 실행의 착수시기에 대해, 야간이 아닌 주간에 절도의 목적으로 다른 사람의 주거에 침입하여 절취할 재물의 물색행위를 시작하는 등 그에 대한 ‘사실상의 지배를 침해하는 데에 **밀접한 행위**를 개시’하면 절도죄의 실행에 착수한 것으로 보아야 한다.」

위해 기망하는 행위를 시작하였을 경우, 이러한 기망행위를 취득을 위한 예비행위로 볼 것인가 혹은 취득에 밀접한 실행의 착수로 볼 것인가가 명확하지 않다.

2) 실행의 착수시기의 판단기준 검토

주관적 객관설에 의하면 실행의 착수가 있다고 하기 위하여 반드시 구성요건에 해당하는 행위를 개시할 것을 요하는 것은 아니다. 그러나 행위자의 주관적 범죄계획에 따라 그대로 진행되는 경우에는 직접 구성요건이 실현될 수 있는 구성요건에 해당하는 실행행위와 밀접한 행위가 있으면 실행의 착수가 있다는 일반적 기준이 제시될 수 있다. 이러한 일반적 기준을 구체화하는 것이 각칙상의 개별적인 구성요건의 실행행위에 대한 해석의 문제이다.

따라서 실행의 착수는 구성요건에 해당하는 행위 또는 직접 구성요건의 실현을 위한 행위가 개시되면 인정되는 것이다. 구성요건의 일부가 실현되어 이미 구성요건적 행위가 개시된 때에는 문제가 없으나 구성요건적 행위가 개시되지 아니한 때에도 직접 구성요건의 실현을 위한 행위가 있으면 실행의 착수가 있다고 할 수 있다. 다만 그 행위는 구성요건의 실현을 위한 직접적인 행위임을 요하며 이러한 직접성은 구성요건적 행위와 시간적·장소적으로 접근한 경우에 인정할 수 있다.[49]

(2) 소결

미수범의 실행의 착수시기에 대한 학설 중에서, 절충설은 미수범의 처벌범위를 확보하면서도 미수범의 지나친 확장을 방지할 뿐 아니라 실행의 착수의 인정기준이 보다 명백하다고 볼 수 있으므로 이에 관한 일반기준으로서는 절충설이 타당하다고 본다. 다만, 여기서 '직접적인 행위의 개시'란 구성요건실현과 '시간적·장소적으로 근접'해 있기 때문에 다른 '중간행위의 개입 없이'도 구성요건에 이르러 갈 수 있는 행위의 개시를 의미하는 바, 이러한 행위가 개시되었는가는 중립적인 관찰자가 객관적으로 관찰하는 것이 아니라 행위자의 전체적인 범행계획에 의해 결정되어야 한다.[50] 즉 예비·음모, 미수는 모두 범의의 표현이라는 것을 전제로 하기 때문에 어느 단계까지를 준비행위로 볼 것인가에 대한 기준을 제시하지 않는다면, 미수의 처벌범위가 부당하게 확대될 수 있게 된다. 이는 형법의 보충성 원칙에 반하는 법적용이 될 것이다.

따라서 미수범을 처벌하고자 하는 경우에는 취득의 경우를 제외하고, 취득하여 사용하거나 제3자에게 누설한 경우에 한하여 미수범을 처벌하는 것이 타당할 것이다.

---

49) 또한 실행의 착수가 있는가, 즉 직접 구성요건의 실현을 위한 행위가 있는가는 행위자의 범죄의사 내지 범죄계획에 의하여 결정해야 한다. 다시 말하면 범죄자의 의사에 의하여 공격수단이 공격객체와 실재적 연관에 놓여 직접적인 위험범위에 들어가게 된 행위가 있으면 실행의 착수를 인정해야 한다(이재상, 앞의 책, 351-353면 참조).

50) 이재상, 위의 책, 361면 참조.

Ⅳ. 첨단기술 유출방지 관련법규의 개선방안

첨단기술의 유출방지를 위한 관련법규의 개선방안으로 형사적 처벌 관련 규정과 형사소송 관련규정에 관하여 고찰하도록 한다. 먼저 형사적 처벌과 관련하여서는 벌금형 확정의 조정방안과 양벌규정의 법정형 차등 방안, 벌금형병과제도의 개선방안을 살펴본다.

다음으로 형사소송과 관련하여서는 소송절차 관련규정의 개선방안으로 친고죄규정의 폐지에 따른 문제점을 개선하기 위한 방안인 재판공재제한 및 소송기록열람 제한 규정을 신설하는 문제를 논의하고, 수사실무 관련규정의 개선방안으로 기술유출범죄 수사의 효율성을 위한 통신제한조치의 대상범죄로 당해 범죄를 추가하는 방안과 소프트웨어 불법복제수사에 강제수사인 감청 및 압수·수색의 허용, 산업스파이행위의 규제를 위한 개선방안으로 함정수사제도의 도입과 역외관할권 규정의 신설을 살펴본다.

1. 형사적 처벌 관련규정의 개선방안

(1) 벌금형 확정의 조정방안

기업의 산업기밀 유출사건의 범죄자 대부분은 연구원 및 직원 등과 같이 개인이다. 이에 반하여 산업기밀의 가치는 수십억 이상인 경우가 많아, 실제 법 집행단계에서는 경제적으로 벌금을 감당하기 어려운 개인에게 수십억이나 수백억의 벌금형을 선고하기 곤란하다는 점에서 벌금형의 실효성에 문제시되고 있다. 또한 수사 및 재판실무상 '재산상 이득액'에 대한 금전적 가치의 확정이 곤란한 점도 있다.[51] 개정 후, 벌금형을 받은 산업스파이들이 한 명도 없다는 데에 큰 문제점이 나타나는 것이다.[52]

이처럼 가중벌금제도를 도입한 영업비밀보호법 제18조에 대하여 벌금이 비현실적으로 과다하게 부과되는 등 실효성에 문제가 있다며 2005. 6. 1. 영업비밀보호법 개정안이 발의된 바 있다.[53] 개정안에서는 벌금형의 타당성과 범죄예방의 실효성 확보를 위해 첨단기술 유출범죄에 대한 벌금형을 국내·외 유출사건에 대해 모두 5억원 이하의 확정금액으로 규정하였다.[54]

---

51) 이러한 비현실적 규정으로 2005년부터 2006년 2월까지 선고가 난 54명 중 벌금형을 받은 사람은 단 1명에 불과하다(한국경제신문, 2006년 3월 23일자 참조).

52) 실제로 6세대 LCD기술 유출사건과 LG-팬텍계열 간 휴대전화 관련 기술 유출분쟁에서 피해추정액이 4천억원, 60억원으로 산정되어 사실상 벌금형을 내리기란 어려운 문제이다. 이 사건에서 벌금형을 내릴 경우, 1백여원에서 4조원이라는 천문학적인 단위에 달하기 때문이다. 이러한 이유로 결과적으로 낮은 형량이 선고되고 있으며, 나아가 이러한 천문학적인 벌금형을 피하기 위하여 선고된 집행유예나 사회봉사명령, 무죄판결 등이 자칫 미세한 규정결함으로 인해 빚어진 역효과로 연결될 수 있다는 점이다.

53) 한나라당 안상수 의원 등은 기술유출 행위로 부당하게 얻은 재산상 이익의 2배이상 10배이하의 벌금형에 처하도록 규정하고 있는 현행 형벌규정이 '재산상 이익'을 명확하게 계산할 수 없는 등 불명확한 점이 있으며, 첨단기술 유출로 부당하게 얻은 이익은 수십억에서 수백억에 이를 수 있는데 그 10배를 벌금으로 부과하는 것은 그 실효성이 현저히 부족한 것으로 판단하고 있다(산업자원위원회 전문위원 구희권, 부정경쟁방지 및 영업비밀보호에 관한 법률중개정법률안 검토보고서, 정부제출안, 2003, 18-20면 참조).

생각건대, 벌금형을 합법적으로 마련하는 것은 범죄예방의 실효성을 확보하는 차원에서 강하게 요구된다고 할 수 있다. 따라서 벌금액을 확정액으로 조정하여 실효성을 확보하는 것이 타당하다고 판단된다.[55] 또한 벌금형을 규정함에 있어서 수사 및 재판실무상 '재산상 이득액'에 대한 금전적 가치의 확정이 곤란하다는 점도 고려되어야 한다. 산업스파이로 인하여 기업이 막대한 이익을 얻었고, 피고인과 법인의 경제능력평가가 정확하게 이루어질 수 있다면 일수벌금제도(Tagessatzsystem)의 도입[56]도 고려해야 할 것이다. 일수벌금제도의 가장 큰 장점은 기업에 벌금액을 인상할 수 있다는 것인데, 기업에게는 자유형을 부과할 수 없으므로 일수벌금제도에 따라 일수를 정한다면 이것이 자유형의 일수계산과 일맥상통하므로 자유형을 대체하는 방안으로 모색될 수도 있겠다.[57]

(2) 양벌규정의 법정형 차등 방안

양벌규정이라 함은 행위자뿐만 아니라 동시에 단체나 고용주에게도 책임을 물어 처벌하는 것을 말한다. 형법은 책임원칙을 기본원칙으로 하고 있기 때문에, 범죄행위를 한 당사자인 개인만이 행위에 책임이 있으며 이에 의해 처벌을 받는다. 그러나 이러한 개인이 일정한 단체의 구성원이나 또는 타인의 사용인으로서 그 단체나 고용주의 임무를 수행하는 과정에서 기술유출범죄를 행하는 경우, 이 행위는 결국 개인이 속한 단체나 고용주의 행위로 평가되는 측면이 강하다고 할 수 있다. 그 이유는 동 행위의 효과 및 이익의 귀속이 행위자 개인이 속한 단체 또는 고용주에게 귀결되는 경우가 많기 때문이다.[58]

종래 양벌규정은 위반행위자에 과해지는 형벌 중 법정벌금형의 한도 내에서 벌금형을 가하고 있다. 그런데 법인, 즉 기업에 대한 형벌로서의 벌금형은 실제로 별로 큰 액수가 아니므로 양벌규정의 적용으로 법인이 응징을 받는다는 효과를 사실상 기대하기 어렵다. 여기서 법인 등에 대한 벌금형을 행위자에 대한 형벌과 분리하여 대폭 강화하려는 움직임이 나타나고 있다.[59]

---

54) 국가정보원, 첨단 산업기술 보호동향, 2005. 3 제3호, 22면 참조.

55) 이에 참고하여 EEA를 살펴보면, 국외유출목적의 범죄를 행한 조직이나 단체에 대해서 국내유출범죄보다 가중처벌하고 있다는 데에 특이점을 발견할 수 있다. 또한 미수와 음모에 대해서도 법정형의 처벌규정을 두고 기수와 동일하게 처벌하고 있는 점도 눈여겨 볼만하다(윤해성, 앞의 논문, 31-32면 참조).

56) 독일과 오스트리아 형법에 도입된 일수벌금형제도는 벌금형을 일수(Zahl der Tagessätze)와 일수정액(Höhe eines Tagessatzes)으로 분리하여 일수는 일반적 양형규정에 따라 행위자의 불법과 책임을 표시하여 대체자유형의 문제를 자동적으로 해결하게 하며, 일수정액은 피고인의 경제적 사정을 고려하여 결정하게 함으로써 합리적이고 정당한 벌금형을 정할 수 있게 하는 제도라고 할 수 있다[이재상, 앞의 책, 538-539면 참조].

57) 박광민·윤해성, 부정경쟁방지법상 영업비밀 개념의 검토, 성균관법학 제18권 제1호, 2006. 6, 430-431면 참조.

58) 이러한 양벌규정은 지식재산권 관련법제 대부분에서 규정하고 있는데, 특허법 제230조, 실용신안법 제53조, 의장법 제87조, 저작권법 제103조에서 법인의 대표자, 법인 또는 개인의 대리인, 사용인 기타 종업원이 그 법인 또는 개인의 업무에 관하여 권리침해행위를 한 경우, 행위자를 벌하는 외에 그 법인 또는 개인에 대해서도 동시에 벌금형을 부과하고 있다. 또한 신지식재산권 관련법제에서도 그대로 적용되는데, 영업비밀보호법 제19조, 산업기술유출방지법 제38조, 반도체법 제49조, 컴퓨터프로그램보호법 제50조 등에서도 이를 내용으로 하고 있다(홍승희, 앞의 글, 163면 참조).

59) 이에 관하여 영·미 법계에서는 일반적으로 법인의 범죄능력을 인정하고 있는데 비하여, 대륙법계의 독일에서

따라서 법인의 범죄능력 여하에도 행정형벌의 취지 및 특히 지식재산권 관련범죄가 행위자에 대한 윤리적 비난보다는 이득 침해에 대한 징벌적인 의미에 중점을 두고 있음을 고려하여, 법인 등에 대한 벌금형을 대폭 강화하는 것이 효과적일 것이다.[60]

(3) 벌금형병과제도의 개선방안

현행법에서는 징역형과 벌금형을 동시에 처벌하는 병과규정이 있다. 이는 현행법상 범죄수익몰수제도의 기능을 갖는 것으로 볼 것인지에 대하여 논의되고 있는 제도로서,[61] 사실 현행법상 벌금형병과가 과연 어떠한 기능을 염두에 둔 규정인지 다시 말하면 본래의 입법취지는 분명하지 않다고 할 수 있다.[62] 이러한 병과규정은 범인으로부터 일정한 재산을 박탈하는 것을 내용으로 하는 재산형인 벌금형을 자유형에 병과 하는 형태를 현행법상 활용하고 있는데, 이는 형법 및 형사특별법에서 채택되어 있으나 일반적인 규정은 없고 개별적으로 형법각칙이나 특별형법에서 병과규정을 둔 경우에 벌금형을 병과 하도록 되어 있다.[63]

1) 현행 병과제도의 문제점

벌금형이 병과 되면 벌금형의 형량만큼 자유형의 형량이 삭감되어야 하는데, 총액벌금형제도를 취하고 있는 현행법상 벌금형과 자유형을 상호 환산하는 기준이 명확하지 않다. 따라서 어느 정도의 벌금형 액수가 어느 정도의 자유형에 해당하는지 계산할 수 없다는 문제점이 있다. 결국 자유형에 병과 되는 벌금형은 사실상 법관의 판단에 의해서 정해질 수밖에 없는데, 이 경우 형법상 책임원칙에 상응하는 벌금형을 정하는 것이 사실상 어려울 수 있다.

그 다음으로 벌금형병과제도 하에서는 벌금형을 납부하지 못하는 행위자는 선고된 벌금형만큼 대체자유형이 집행되어야 하는데, 그렇다면 더욱이 병과제도 또한 책임원칙에 부합해

는 법인에 대하여 윤리적 비난을 가할 수 없다는 이유로 범죄능력을 부인하고 있다. 또한 일본에서는 학설상 긍정설·부정설이 있으나 법인의 범죄능력을 긍정하는 입장에서도 행정법규에 한하여 이를 긍정하며, 형법상 범죄에 있어서는 이를 부정하는 것이 일반이다.

60) 한편 기업 활동의 현장에서는 양벌규정의 적용을 받는 일선의 행위자와 법인 이외에, 기업의 의사를 결정하는 이사회, 기타 임원의 존재가 실제로 중요한 역할을 수행하고 있음에도, 이들은 위법행위의 책임을 하급의 특정행위자와 아무런 감정도 없는 법인에 전가하고 자신들은 처벌을 면하는 경우가 많다. 따라서 법인의 처벌 이외에 법인의 의사결정기관에 대하여도 감독책임을 물어 행위자, 의사결정기관, 법인의 3자를 처벌하는 이른바 삼벌주의를 도입하여 불균형을 시정하는 방법도 생각해 볼만하다(홍승환, 지적재산권의 권리침해와 보호제도에 관한 연구, 경희대학교 대학원 석사학위논문, 2006. 2, 65면 참조.).

61) 학설상으로 그다지 문제되지 않는 것과는 달리 헌법재판소 판례에서는 특정범죄가중처벌법 제8조의 위헌여부와 관련하여 벌금형병과제도에 대하여 법리적 관점에서 그 적정성여하가 문제된 바 있다[헌법재판소 1998. 5. 28, 97헌바68 특정범죄가중처벌등에관한법률 제8조 제1항 등 위헌소원결정 참조].

62) 박미숙, 현행법상 벌금형병과제도의 문제점과 개선방안, 형사정책연구소식 제81호, 2004년 1/2월호, 2면 참조.

63) 현행법상 벌금형병과제도는 다른 입법례에서는 찾아보기 어려운 제도이다. 병과의 행위유형은 그 보호법익은 달리하되, 궁극적으로는 그 행위가 재산적 이익을 노리고 행해지는 경우가 많다는 점과 나아가 중대한 범죄유형이라는 점을 알 수 있다. 즉 벌금형병과를 통해서 일정한 이득을 박탈할 수 있도록 함으로써 벌금형병과제도가 사실상 범죄수익에 대한 몰수의 기능을 수행하고 있을 뿐만 아니라, 가중형벌적 성격을 갖고 있다는 점이다(박미숙, 위의 글, 2-3면 참조).

야 할 것이다. 그러나 과연 벌금형병과에 있어서 자유형과 벌금형의 산정이 책임원칙에 부합하여 이뤄지는지 의문이다.[64]

2) 소결

적어도 자유형의 법정형을 재조정하여 적정한 형벌을 보장하고, 형사정책적인 의미가 없는 벌금형병과규정은 가능한 한 형법에서 삭제하도록 함이 타당하다. 또한 형법상 벌금형병과규정이 범죄수익몰수기능을 하기에 적정한 제도인지도 의문이다. 범죄수익몰수제도는 약물 및 조직범죄와의 대응을 위해 발전되어 온 제도인데, 벌금형병과제도는 이러한 기능을 하도록 만들어진 것은 아니기 때문이다. 따라서 범죄로부터 생긴 불법수익을 박탈하는 것은 몰수제도의 기능 자체에서 찾아야 하며 이는 몰수제도의 정비를 통해서 가능하도록 함이 타당하다.[65]

3) 개선방안으로 몰수제도 정비의 검토

몰수제도(Einziehung)는 범죄반복의 방지나 범죄에 의한 이득의 금지를 목적으로 범죄행위와 관련된 재산을 박탈하는 것을 내용으로 하는 재산형으로, 경제적 이득을 목적으로 하는 범죄에 대하여는 그 경제적 동기를 제거하고 계속적 범죄활동의 수행을 불가능하도록 이들 범죄의 근원인 범죄수익을 박탈하며 그 보유·운용을 용이하게 하는 일체의 행위를 처벌하는 등 범죄수익을 철저히 규제할 필요성이 매우 크다고 하지 않을 수 없다.[66]

그러나 아직 우리나라의 경우 형법상 몰수제도가 물건을 그 대상으로 하는데 그치고 있고, 일부 공무원범죄나 마약류범죄 등 범죄수익몰수제도가 도입되어 있기는 하지만 그 법규정해석이나 운용측면에서 미비점이 적지 않게 드러나고 있다. 따라서 기술유출범죄로 취득한 범죄수익을 몰수할 수 있는 제도를 도입할 필요가 있다.[67]

생각건대, 범죄수익은닉의규제및처벌등에관한법률은 특정범죄와 관련된 범죄수익 등을 가장·은닉하는 행위를 규제하고, 범죄수익 등의 몰수 및 추징에 관한 특례를 규정함으로써 특

64) 서보학, 형법상 범죄수익몰수의 필요성과 법치국가적 한계, 고려대학교 법학 제5호, 1997, 89-91면 참조.
65) 박미숙, 앞의 글, 9면 참조.
66) 세계 각국에서는 막대한 경제적 수익을 목적으로 하는 범죄에 대한 효과적인 대처방안으로 각광받고 있다(현대호, 미국의 영업비밀 보호에 대한 입법동향, 법령정보 Newsletter, 한국법제연구원, 2006. 5, 79-81면 참조). 미국의 RICO법상 형사몰수제도 하에서는 유죄의 선고에는 자백 기타 증거조사에 관한 모든 실정법 규정 및 헌법상 보장된 적법절차를 준수할 것이 요구되고 이를 통해 피고인의 유죄가 합리적 의심이 없을 정도로 확인되어야 한다(이규호, 영업비밀보호를 위한 미국 민사소송법제, 연세법학연구 제6집 제2권, 연세법학회, 1999, 125면 참조). 독일은 몰수제도를 일원화하여 형법전에 물건에 대한 몰수와 범죄수익에 대한 몰수로 나누어 규정하고 형법 각칙의 개별범죄에 관한 규정에서 이를 지시하는 방식의 입법을 채택하고 있다. 이 방식의 장점은 몰수의 대상을 물건에서 범죄수익 또는 불법재산으로 확대하는 문제를 용이하게 해결할 수 있고, 조직범죄 및 경제범죄 등과 같이 경제적 수익을 목적으로 하는 범죄를 법 정책적인 측면에서 합리적으로 선별할 수 있다는 점이다(심재한, 독일의 개정 부정경쟁방지법 고찰, 경영법률 제16집 제1호, 한국경영법률학회, 2005. 10, 26면 참조).
67) 한편 여기서 주목할 점은 지식재산권 관련법에서는 여전히 몰수규정이 그대로 존재하고 있으나, 현대사회에서 새로이 등장한 신지식재산권 관련 보호법제에서는 이러한 몰수규정이 없다는 점이다. 따라서 이 점은 입법불비가 아니라, 바람직한 합리적인 입법으로서 장차 기존의 지식재산권 법률에서도 몰수규정에 대한 재정비가 이뤄져야 할 것으로 판단된다(홍승희, 앞의 글, 162-163면 참조).

정범죄를 조장하는 경제적 요인을 근원적으로 제거하기 위해 제정되었으나 기술유출범죄는 위 특정범죄의 목록에서 빠져 있다.[68] 동 법률을 개정하여 기술유출범죄를 특정범죄로 규정하여 기술유출범죄를 환수 대상으로 추가할 필요가 있다.[69] 또한 영업비밀보호법에도 산업기술유출방지법상 필요적 몰수·추징 규정을 마련함이 타당하다고 본다.[70]

2. 형사소송 관련규정의 개선방안

(1) 소송절차 관련규정의 개선방안

1) 재판공개제한의 규정 마련

우리 사회에서 재판공개의 요구가 점점 강해지고 있지만, 첨단기술이 재판에 의하여 공개되는 것은 그 보호를 위하여 바람직하지 않으며 재판을 공개하면서 기술보유자의 권익을 보호한다는 것은 기술유출을 방지하기 위한 관련법규의 제정취지를 무색케 하는 것이다.[71] 민사소송이 대부분인 당해소송에 있어서 공개재판은 개인의 이익을 해할 가능성이 많고, 분쟁의 적정·신속한 해결을 저해할 우려도 높다. 또한 기술의 비밀성이 상실될 가능성은 민사소송에서 상대적으로 더 크지만, 형사소송이라고 하여 달리 볼 것은 아니다. 공소장은 청구원인 중 피고인의 침해행위가 피해자의 기술을 침해하는 것이라는 주장을 기재해야 하기 때문에 역시 누설될 위험이 있는 것이다.[72]

따라서 기술유출에 관련된 재판을 요함에 있어서 재판을 비공개로 할 수 있는 절차와 요건을 명확히 규정하는 것이 요구된다. 생각건대, 재판공개제한의 규정[73]을 기술유출관련법규와 법원조직법 및 형사소송법을 개정하여 수용하여야 할 것이다.[74]

2) 소송기록열람 제한 규정 도입

재판공개제도로 인한 피해를 막을 수 있는 유용한 방법은 소송기록 공개의 제한이다. 우리나라의 재판진행과정은 구두진술보다는 서면진술로 진행되기 때문에 소송기록열람의 제한

---

68) 법무부, 범죄수익은닉의규제및처벌등에관한법률해석, 70면 참조.
69) 이윤제, 미국 경제스파이법 연구, 법제, 2007. 1, 168면 참조.
70) 2005년 6월 1일 안상수의원 등 14인으로부터 발의되어, 2일 산업자원위원회에 회부된 부정경쟁방지및영업비밀보호에관한법률 일부개정법률발의안 참조.
71) 숭실대 오철호 교수는 공개재판의 규정의 경우 미국이나 일본처럼 소송과정에서 영업비밀의 비밀성을 유지하기 위한 조치를 취하도록 의무화할 필요가 있다고 주장하였다(중앙일보, 2004년 10월 31일자 참조).
72) 이와 같은 점 때문에 UTSA 제5조는 소송 전 증거공개제도(Discovert Proceeding)와 공개 청구에 의한 보호명령(Protective Oder), 비밀심리(camera Hearing) 및 소송기록의 봉인 등의 규정을 두고 있다. EEA 제1835조도 "… 법원은 영업비밀을 유지하기 위하여 필요하고도 적절한 명령, 기타 조치"를 취하여야 한다고 규정하고 있다. 이처럼 미국의 영업비밀침해에 대한 구제방법이 대부분 민사소송절차로 이루어질 수 있는 배경은 재판 시 비밀유지가 잘 되어 있기 때문이다(최병규, 미국에서의 영업비밀보호에 관한 연구, 창작과 권리 통권5호, 1996년 겨울호, 194면 참조).
73) 구체적으로는 현행 영업비밀보호법에 '성폭력범죄의처벌및피해자보호에관한법률' 제22조 제1항에 유사한 규정을 두는 것을 고려할 수 있다.
성폭력범죄의처벌및피해자보호에관한법률 제22조 (심리의 비공개) ① 성폭력에 대한 심리는 그 피해자의 사생활을 보유하기 위하여 결정으로 이를 공개하지 아니할 수 있다.
74) 윤해성, 앞의 논문, 228-230면 참조.

을 통하여 재판공개의 원칙에 의한 폐해를 어느 정도 제거시킬 수 있다. 미국의 경우 증거개시제도를 도입[75]하여 자료의 열람을 엄격히 제한하고 있는 것과 유사하게 우리나라에서도 소송의 심리보다는 소송의 기록에 의해 첨단기술이 외부에 유출될 위험성이 더 높다는 것을 인식하여 소송기록의 열람을 제한해야 한다는 논의가 있었고, 그 동안의 논의를 수용하여 2002년 개정 민사소송법[76]에서는 기술유출방지를 위한 열람제한 규정을 두었다.[77]

따라서 첨단기술의 경우에도 원칙적으로 소송당사자에 한정하여 소송기록의 열람을 허용하는 등 입법적인 개선이 필요하다. 이외에 법원의 사전승인 없이는 문제된 첨단기술의 공개금지명령 등과 같이 공개심리주의에 관한 특례를 두어야 하며 정식재판이 아닌 중재나 약식재판에 의한 해결방법을 강구할 필요도 있다. 그러므로 형사소송절차에도 이와 유사한 규정을 제정하고 아울러 이러한 열람제한규정을 위반한 행위에 대하여 처벌규정을 마련할 필요가 있다. 또한 민사적 구제뿐만 아니라 형사적 처벌의 실효성을 확보하기 위해서라도 법률에 기술유출방지를 위한 재판공개와 소송기록열람의 제한을 명시하여야 할 것이다.[78]

(2) 수사실무 관련규정의 개선방안

1) 기술유출범죄 수사의 효율성을 위한 개선방안

기술유출범죄와 관련한 수사의 효율성을 제고하기 위한 방안으로, 이에 관한 정보수집이나 특히 필요한 경우에 허용되는 '통신제한조치'에 당해 범죄를 대상범죄에 추가하는 방안과 강제수사관련 압수·수색 및 감청의 허용에 관하여 검토한다.

① 통신제한조치의 대상범죄 추가방안

통신비밀보호법 제5조는 범죄수사를 위한 통신제한조치의 허가요건을 규정한 것으로 제1항에서 대상범죄를 거시하고 있다.[79] 통신제한조치는 다른 방법으로 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 인정되는 것으로, 압수·수색 영장에서는 요구되지 아니하는 보충적 성격을 나타내는 요건이라 하겠다. 현재 우리나라의 첨단산업발전으로 인하여 기술유출범죄는 관련수사에 있어서 통신제한조치의 필요성이 증가하였다고 할 수 있다. 이러한 인식 하에서 동법은 2001년 12월 개정을 통해 일선 수사기관

75) 미국의 경우 증거개시제도(Discovery)에 의하여 채집된 자료에 대해서는 열람을 엄격히 제한하고 있다. 즉 소송절차를 증거개시제도와 공판(Trial)으로 나누어서 각각에 대하여 공개원칙의 적용이 문제된다. 증거개시제도는 변론준비를 위해 정보를 수집할 수 있는 광범위하고 다양한 수단이 인정되는 제도이다. 그리고 공개제한명령에 의하여 영업비밀 기타 비밀로서 취급되어야 할 조사연구 및 산업상의 정보가 공개되어서는 안 되고 또한 일정한 방법에 의해서만 공개되도록 함으로써 영업비밀누설을 광범위하게 제한하고 있다(최병규, 앞의 글, 195면 참조).

76) 2002. 1. 26. 공포, 법률 제6626호, 2002. 7. 1. 시행.

77) 소송기록 중에 당사자의 첨단기술이 있는 때에는 법원은 당사자의 신청에 따라 결정으로 소송기록 중 비밀이 적혀있는 부분의 열람·복사와 재판서·조서 중 비밀이 적혀있는 부분의 정본·등본의 교부를 당사자에게만 한정하여 할 수 있게 한 것이다[민사소송법 제163조 (비밀보호를 위한 열람 등의 제한) 참조].

78) 윤해성, 앞의 논문, 230-232면 참조.

79) ① 형법 및 군형법에 규정된 일부 범죄, ② 국가보안법, 군사기밀보호법, 군사시설보호법에 규정된 모든 범죄, ③ 마약류 관리에 관한 법률, 단속법에 규정된 일부 범죄, ④ 폭력행위 등 처벌에 관한 법률, 특정범죄가중처벌 등에 관한 법률, 특정경제범죄가중처벌등에 관한 법률 등이 정하는 범죄들이다.

에서 필요성이 있다고 주장된 일부 죄명을 추가하고, 동법의 적용과정에서 필요성이 많지 않다고 인식되어 온 범죄를 대상범죄에서 제외하는 등의 합리적인 조정과정을 거쳤으나, 당시 기술유출범죄는 추가대상범죄로의 필요성이 강하게 요청되고 있음에도 포함되지 않았다.[80] 따라서 기술적 범죄수사의 실효성을 위한 방안의 하나로 기술유출범죄의 통신제한조치의 가능범죄로의 추가문제를 고려해봄직하다.

② 강제수사관련 허용방안

소프트웨어 불법복제 관련강제수사에 해당하는 '압수·수색' 및 '감청'의 허용방안에 관하여 검토하도록 한다.

통신망 또는 인터넷을 이용한 불법복제의 경우에는 우선, 불법복제의 증거와 접속기록을 확보하여 이를 분석·확인하는 절차가 통상적인 증거수집절차 이전에 행해져야 한다. 따라서 수사개시 이후에 이를 해결하기 위해서는 압수·수색과 같은 강제처분이 요구된다. 강제수사는 불법복제로 인한 피해발생을 증명할 수 있는 유일한 수단으로 인정되는 경우에 한하여 허용되어야 하므로, 컴퓨터에 내장된 프로그램에 대하여 형사소송법상 영장주의 적용에 의한 압수·수색이 가능하여야 한다.

우선 압수의 대상에 관하여 현행 형사소송법은 '증거물 또는 몰수물'을 명시하고 있는데, 여기서 증거물 또는 몰수물은 '유체물'을 의미하는 것이므로 '무체정보'인 프로그램, 즉 전자기록 그 자체에 관한 압수가 문제시된다. 물론 원칙적으로는 우리나라의 현행 법체계상 무체정보인 전자기록에 대한 압수를 허용할 수 없겠지만, 형사소송규칙의 '물(物)'의 개념을 유체물에 한정하고 있지 않은 미국 판례의 견해[81]를 도입하여 전자기록에 대한 압수를 허용하는 것이 타당하다고 본다.[82]

다음으로 통신망 또는 인터넷을 이용한 불법복제의 경우 전송되는 정보에 대한 수색에 관해서는, 형사소송법상 강제수사규정의 적용과 별도로 범죄의 증거를 확보하기 위한 통신망 또는 인터넷에 대한 '감청'[83]이 문제된다. 인터넷상 전자우편인 E-mail을 포함하는 컴퓨터통신, 자료나 정보의 전송 등 컴퓨터 이용의 대중화와 더불어 생겨난 새로운 통신수단은 통신비밀보호법상 '전기통신'에 해당한다고 할 수 있다.[84] 또한 「대법원 송무예규 제796호

80) 대검찰청, 통신비밀보호법 해설, 2005, 4-6면 참조.

81) 미국형사소송규칙 제41조(h)항은 "압수의 대상이 되는 물건은 문서, 장부, 서류 기타 유체물을 포함한다"고 규정하고 있다. 이와 관련하여 United States v. New York Telephone Co., 434 U.S. 159, 98 S.Ct. 346, 54 L.Ed.2d 376 (1977)판례는 "형사소송규칙 제41조(h)항에서 물건이라 함은 문서, 장부, 서류 기타 유체물을 포함한다고 정의하고 있으나 이는 한정적 열거가 아니며 대상으로 될 수 있는 物 모두를 열거하고자 한 취지도 아니다. … 동규칙 제41조는 유체물에 한하지 않는 것이다"라고 판시하면서, 제41조는 유체물과 마찬가지로 pen register에 기록된 것과 같은 무체물도 압수할 수 있다고 한다.

82) 또한 Michigan Bell Tel. v. United States, 565 F.2d 385 (6th Cir. 1977)판례도 "기술적으로 무체물은 특정한 기술에 의해 압수할 수 있기 때문에 법원은 형사소송규칙 제41조의 적용범위를 한정할 것은 아니고 오히려 그 목적을 실현하도록 동조를 해석하여야 한다는 것이 일반의 법감정일 것이다."라고 판시하면서, 컴퓨터에 내장된 프로그램 자체도 압수대상으로 인정할 수 있다고 한다.

83) 전기통신의 '감청'은 제3자가 전기통신의 당사자인 송신인과 수신인의 동의를 받지 않고 통신을 채록하는 행위 등을 말한다.

84) 고병민, 미국의 통신비밀보호와 감청관련법규에 대한 고찰, 대검찰청 해외연수검사 연구논문, 2006. 7, 39면 참조.

이메일 등 컴퓨터 통신내용에 대한 강제수사 방법」[85]에서도 컴퓨터통신이 동법상 전기통신에 해당됨을 명백하게 언명하고 있다. 따라서 통신망 혹은 인터넷을 이용하여 행해지는 소프트웨어 불법복제에 대한 수색의 범위로 통신망의 감청이 허용될 수 있을 것이다.[86]

2) 산업스파이행위의 규제를 위한 개선방안

산업스파이행위를 규제하기 위한 수사실무에 있어서의 개선방안으로 함정수사제도의 도입과 역외관할권 규정의 신설을 검토한다.

① 형사소송법상 함정수사제도의 도입방안

함정수사(agent provocateur)라 함은 수사기관 또는 그 하수인이 본래 범의를 가지지 아니한 자에 대하여 사술이나 계략 등을 써서 범죄를 교사한 후 범죄의 실행을 기다려 범인을 체포하는 방법을 말한다.[87] 이러한 점에서 함정수사는 수사의 신의칙에서 정당성이 문제되고 있다.

현행법상 함정수사를 허용하는 규정은 없으므로 함정수사가 강제수사라고 한다면 강제수사법정주의[88]에 의하여 위법하다고 해야 하지만, 함정수사의 유동적인 권리개념을 고려하면 이를 임의수사로 보아 인격적 권리를 침해하거나 위험하게 할 때에는 그 한계를 벗어나기 때문에 위법하다고 해석하는 것이 타당하다.[89] 또한 함정수사의 허용범위에 관하여 우리나라의 통설은 미국 연방법원의 이론[90]에 따라 기회제공형의 함정수사는 적법함에 반하여 범의유발형의 함정수사는 위법하다고 보고 있다.[91]

생각건대 함정수사의 적법성의 한계는 함정수사가 첫째, 범죄를 방지해야 할 국가기관이 범인에게 범죄를 유도했다는 측면과 둘째, 국가가 사술을 사용함으로써 수사의 신의칙에 반하였다는 측면에서 찾아야 할 것이므로, 범죄의 태양과 함정수사의 필요성, 법익의 성질 및 남용의 위험성 등을 종합하여 판단하는 것이 타당하다고 본다. 따라서 산업스파이수사의 효율성을 위한 방안으로써 형사소송법상 함정수사에 대한 근거조항을 입법화하여야 한다고 생각한다.[92]

---

85) 2000년 11월 1일부터 시행된 동 예규에서는 "당사자의 동의 없이 E-mail 등 컴퓨터를 이용한 통신내용을 취득하거나 통신의 송·수신을 방해하는 것은 통신비밀보호법상 '전기통신'에 대한 '감청'에 해당하므로, 위와 같은 경우 통신제한조치허가 사건으로 처리"한다고 규정하고 있다.

86) 김도식, 통신비밀보호법상 통신제한조치의 문제점, 서울대학교 대학원 석사학위논문, 2005. 2, 157-159면 참조.

87) 따라서 범의를 가진 자에 대하여 범행의 기회를 주거나 범행을 용이하게 한 것에 불과한 경우에는 함정수사라고 할 수 없다(대법원 2004. 5. 14, 선고 2004도1065 판결 참조).

88) 형사소송법 제199조 제1항 단서 참조.

89) 이재상, 형사소송법, 2005, 176면 참조.

90) Sorrels v. U.S. 287 U.S. 453; Sherman v. U.S. 356 U.S. 369 참조. 이에 따라 미국에서는 범의를 가지고 있는 자가 함정에 의하여 범죄를 행할 기회를 가진 데 불과한 때에는 형사책임을 면할 수 없지만 범의를 유발한 때에는 형사책임으로부터 해방된다는 이론이 판례상 확립되었다.

91) 대법원 1982. 6. 8. 선고, 82도884; 대법원 1992. 10. 27. 선고, 92도1377 판결 참조.

92) 함정수사를 도입하고 있는 미국의 경우를 살펴보면, 실제로 EEA위반사건의 대다수는 함정수사를 통한 사전 예방활동으로 이루어지고 있다고 한다. 참고로 CCIPS는 홈페이지를 통하여 EEA위반사건들에 대한 보도자료, 공소장 등을 제공하고 있는데, 33개 사건 중 실리콘밸리가 있고 첨단산업이 발달한 캘리포니아 주에서 가장 많은 17개의 사건이 있었다[http://www.usdoj.gov/criminal/cybercrime/eeapub.htm 참조]. 이러한 점을 볼

② 역외관할권 규정의 신설방안

산업스파이의 법적 지위는 산업스파이가 어떠한 신분적 지위를 누리는 상태에서 행위를 하느냐에 따라 다를 수 있다. 즉, 국가가 파견하는 경우와 기업 또는 일반 사인이 파견한 경우가 상이하기 때문에 이중적 지위가 인정되고, 이들의 신분적 지위에 따라 체포 시 처벌의 문제도 달라진다.[93] 따라서 산업스파이수사는 파견자가 누구이고 그 사람이 어떠한 신분적 지위를 누리고 있는지 여부를 근거로 하는 이원적 접근이 바람직하다. 먼저, 산업스파이가 자국민인 경우에는 대부분이 금전적 이익을 목적으로 행위를 한 것으로 추정되므로 추적하여 처벌해야 할 것이고, 외국인(외교관과 비밀요원)인 경우에는 사후적 조치가 사실상 불가능하므로 사전적 예방조치가 최선이라고 할 수 있다.[94] 이러한 문제점을 해결하기 위하여 일반관할규정에 대한 예외인 역외관할권의 입법을 고려해야 할 필요성이 요구되는 것이다.[95]

Ⅴ. 결 론

이상과 같이 본 연구는 국내기업들의 첨단정보기술이 경쟁국가로 유출되어 관련기업과 국가경제에 큰 손실을 주는 첨단기술의 유출을 방지하고 이를 효과적으로 보호하기 위한 관련 법규의 문제점을 형사법적인 측면에서 접근하였다.

우리나라의 첨단기술 유출방지 관련법규인 산업기술유출방지법은 산업기술과 국가핵심기술에 관한 보호를 강화하기 위하여 제정된 특별법으로, 현재 그 개념정의나 처벌규정에 있어 미흡하다고 할 수 있다. 그러나 미국의 EEA는 첨단기술의 유출 및 침해행위에 대한 형사적 처벌의 실효성을 담보하기 위한 선(先) 절차로서 보호대상의 개념이나 처벌행위의 유형을 상세히 규정하고 있으며, 형사적 처벌에 있어서도 기수범과의 미수·음모의 동일형량 처벌조항이나 형사몰수, 역외관할권규정 및 소송절차의 비공개조치까지 규정하고 있음을 알 수 있다. 그러나 이러한 규정에 비해서 우리나라는 아직 입법에 있어서 미비와 불비가 지적되고, 개선되어야 하는 부분에 대한 제시도 요구되고 있는 실정이라 하겠다.

이러한 관점에서 첨단기술 유출방지 관련법규를 재정비하기 위한 방안으로, 첨단기술의 침해에 대한 형사적 처벌의 강화는 외국의 과학자나 기술자를 수입·고용해야 하는 우리의 입장에 비추어 어려움이 있을 수 있다. 반면 국내기업의 휴대전화, LCD, 반도체 관련기술 등 핵심기술을 외국 산업스파이의 공격으로부터 보호해야 하는 실정도 간과할 수 없다. 따

때, 그 중요성을 간과할 수 없다고 할 수 있다.

93) 먼저 외교관이 산업스파이행위를 한 때에는 비엔나협약에 의해서 외교관의 면책특권이 적용되어 추방하거나 소환을 요청할 수 있으므로 이 문제는 정치적으로 해결된다. 그러나 특정국가가 파견한 비밀요원이 일반 사인의 신분인 경우에는 중한 형벌로 처벌되거나 추방될 것이다(강경민, 산업스파이로부터 영업비밀보호에 관한 연구, 성균관대학교 정보통신대학원 석사학위논문, 2004. 4, 180면 참조).

94) 문규석, 국제법에서의 산업스파이에 관한 연구, 성균관법학 제17권 제3호, 2005. 12, 429-430면 참조.

95) 윤해성, 앞의 논문, 222-223면 참조.

라서 외국의 선진기술을 도입하고 있는 우리나라의 실정과 국가경쟁력을 위한 자국의 첨단기술보호를 감안하면서 양자 간의 이중적인 난점을 최대한 유연하게 극복하여 첨단기술에 대한 유출을 방지하기 위한 관련법규의 제도적·법적 장치를 강구하여야 한다고 본다.

< 참 고 문 헌 >

국내문헌

단행본

김일수, 형법각론, 2004
박상기, 형법총론, 2005
배종대, 형법각론, 2004
_____, 형법총론, 2005
손동권, 형법총론, 2005
이재상, 형법각론, 2005
_____, 형법총론, 2006
_____, 형사소송법, 2005
정성근·박광민, 형법각론, 2002

논문

강경민, 산업스파이로부터 영업비밀보호에 관한 연구, 성균관대학교 정보통신대학원 석사학위논문, 2004. 4
김도식, 통신비밀보호법상 통신제한조치의 문제점, 서울대학교 대학원 석사학위논문, 2005. 2
윤해성, 영업비밀보호에 관한 형사법적 연구, 성균관대학교 박사학위논문, 2006
홍승환, 지적재산권의 권리침해와 보호제도에 관한 연구, 경희대학교 테크노경영대학원 석사학위논문, 2006. 2

학술지 및 기관지

강동범, 사이버범죄와 형사법적 대책-제25회 형사정책세미나 자료집, 한국형사정책연구원, 2000
고병민, 미국의 통신비밀보호와 감청관련법규에 대한 고찰, 대검찰청 해외연수검사 연구논문, 2006. 7
국가정보원, 첨단 산업기술 보호동향, 2005. 3 제3호
_____ 산업기밀보호센터, 기술유출현황, 2007. 2
김재봉, 영업비밀의 형사법적 보호방안, 형사정책 제14권 제1호, 2002
곽경직, 영업비밀침해에 대한 형사적 보호, 법조 제47권 9호, 통권 504호, 1998. 9
권오걸, 장물의 성립요건과 범위-컴퓨터등사용사기죄와 배임죄를 중심으로-, 한국비교형사법학회, 비교형사법연구 제8권 제2호, 2006

노상헌, 일본의 지적 재산권 강화와 근로자의 의무에 관한 법적 쟁점, 기업법연구 제20권 제3호 (통권 제26호), 2005
대검찰청, 통신비밀보호법 해설, 2005
류병운, 경제스파이(Economic Espionage)로부터 영업비밀(Trade Secret)의 법적보호 : 국제법 및 미국법적 제도의 검토를 통한 한국과 국제사회의 대응방향 모색, 외법논집 제17집, 2004. 11
문규석, 국제법상 산업스파이에 관한 연구, 성균관법학 제17권 제3호, 2005. 12
박광민·윤해성, 부정경쟁방지법상 영업비밀 개념의 검토, 성균관법학 제18권 제1호, 2006. 6
박미숙, 현행법상 벌금형병과제도의 문제점과 개선방안, 형사정책연구소식 제81호, 2004년 1/2월호
백성근, 미국의 지적재산권 보호 체계, 법무연수원, 2006. 6
산업자원위원회 전문위원 구희권, 부정경쟁방지 및 영업비밀보호에 관한 법률중개정법률안 검토보고서, 정부제출안, 2003
서보학, 형법상 범죄수익몰수의 필요성과 법치국가적 한계, 고려대학교 법학 제5호, 1997
심재한, 독일의 개정 부정경쟁방지법 고찰, 경영법률 제16집 제1호, 한국경영법률학회, 2005. 10
이규호, 영업비밀보호를 위한 미국 민사소송법제, 연세법학연구 제6집 제2권, 연세법학회, 1999
이윤제, 미국 경제스파이법 연구, 법제, 2007. 1
정덕배, 중국의 영업비밀 보호제도 고찰, 지식재산21, 특허청, 2002
최병규, 미국에서의 영업비밀보호에 관한 연구, 창작과 권리 통권5호, 1996년 겨울호
최호진, 기업의 영업비밀에 대한 형사법적 보호 -부정경쟁방지법및영업비밀보호법을 중심으로-, 형사법연구 제25호, 2006 여름
컴퓨터프로그램심의조정위원회, 주요국의 기술유출방지대책 현황 및 관련법령에 대한 검토, 연구자료, 2005
홍승희, 정보재산권의 형사법적 보호와 한계, 한국형사정책연구원, 연구총서 05-13 사이버범죄연구, 2005
_____, 지식재산권 관련 형벌법규 정비방안, 한국형사정책연구원, 연구총서 06-05, 2006

외국문헌

미국

Kent B. Alexander/Kristian L. Wood, The Economic Espionage Act: Setting the Stage for a New Commercial Code of Conduct, 15 Ga. St. U.L. Rew. 922(1999).

국문초록

본 연구는 국내기업들의 첨단정보기술이 경쟁국가로 유출되어 관련기업과 국가경제에 큰 손실을 주는 첨단기술의 침해를 방지하고 이를 효과적으로 보호하기 위하여 마련되어 있는 관련법규의 문제점에 대하여 형사법적인 측면에서 접근하였다. 우리나라의 현행 첨단기술 유출방지 관련법규에는 일반법인 형법과 특별법인 부정경쟁방지 및 영업비밀보호에 관한 법률, 산업기술의 유출방지 및 보호에 관한 법률, '컴퓨터기술관련보호법률'로 컴퓨터프로그램보호법과 반도체집적회로의 배치설계에 관한 법률, '정보관련보호법률'로 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 통신비밀보호법 등이 있다. 본 연구에서는 특별법 중에서 2006년 제정되어 2007년 4월 시행되고 있는 '산업기술의 유출방지 및 보호에 관한 법률'의 형사법적인 문제점을 검토하고, 첨단기술 유출방지 관련법규 전반에 해당되는 개선방안을 제안하고자 한다.

첨단기술 유출방지 관련법규의 주요내용에서는 주요국과 우리나라의 첨단기술 유출방지 관련법규를 검토하였다. 우선 주요국의 첨단기술 유출방지 관련법규에 관하여는 미국과 독일, 일본 및 중국의 관련법규를 고찰하였는데, 각국은 이를 통해 보호대상에 관한 정의규정과 침해행위의 유형 및 형사적 처벌규정을 구체적으로 마련하고 있었다. 본 연구에서는 미국의 EEA를 중심으로 독일의 UWG과 일본의 부정경쟁방지법, 중국의 국가안전법 및 반부정당경쟁법 등을 검토하였는데, 이를 통해 '첨단기술'에 속하는 정보 등은 그 특성상 일반법보다는 특별법형태의 법률이 그에 대한 유출 및 침해행위에 있어서 효율적인 규제가 가능함을 알 수 있었다. 이를 배경으로 우리나라의 첨단기술 유출방지 관련법규에 있어서 일반법인 형법의 적용가능범죄와 한계를 검토하였고, 특별법들을 중심으로 그 주요내용에 관하여 고찰하였다.

특별법 중에서도 최근 제정·시행되고 있는 '산업기술의 유출방지 및 보호에 관한 법률'은 제정 전부터 보호대상의 개념을 정의한 규정과 유출 및 침해행위의 태양에 관한 규정 및 형사적 처벌조항 등에서 여러 문제들이 제기되어 왔었다. 이에 관하여 수차례의 검토가 이루어졌으나 여전히 형사법적인 관점에서 문제로 제기되는 부분이 남아있다 하겠다. 따라서 본 연구에서는 형사법적인 문제점에 관하여 이미 많은 논의가 이루어진 부정경쟁방지 및 영업비밀보호에 관한 법률 등에 관하여는 개선방안을 제안하는 형태로 언급하도록 하고, 산업기술유출방지법의 '형사법적 문제점 검토' 부분에서는 동 법률에 관한 논의를 중심으로 고찰하였다. 제기되는 문제들로는 먼저 산업기술 등 보호대상의 개념정의규정에 관한 문제와 유출 및 침해행위 태양의 개념에 관한 형법적 타당성 문제, 중과실 및 미수범에 관한 처벌의 가능성 문제가 있다. 먼저 보호대상의 개념정립 문제에서는 '산업기술'과 '국가핵심기술'을 정의한 규정이 형법의 기본개념인 죄형법정주의의 명확성원칙에 위배되는지 여부와 행위대상이 되는 '산업기술'의 재물성 여부를 검토한다. '유출 및 침해행위' 규정에 관한 형법적 타당성 문제에서는 절취 및 기망·협박 개념을 동종의 유형으로 표현하는 것에 관한 법률문언의 명확성원칙 위배여부를 검토한다. 중과실에 의한 침해행위 처벌과 관련하여서는 중과

실범의 성립여부를, 미수범의 처벌 가능성 문제와 관련하여서는 미수범이 성립하기 위한 요건인 실행의 착수를 검토한다.

첨단기술의 유출방지를 위한 현행 관련법규의 개선방안에서는 형사적 처벌 관련규정과 형사소송 관련규정으로 구분하여 논의하였다. 먼저 형사적 처벌 관련규정의 개선방안으로는 '벌금형의 확정액 조정방안'과 '양벌규정의 법정형 차등 방안' 및 벌금형병과제도의 문제점을 개선하기 위한 방안인 '몰수제도의 정비'에 관하여 제안하였다.

형사소송 관련규정의 개선방안으로는 소송절차와 수사실무에서 논의되어야 할 개선방안으로 구분하였다. 먼저 소송절차 관련규정의 개선방안 부분에서는 친고죄의 폐지에 따른 문제점을 해결하기 위한 방안으로 '재판공개제한의 규정' 마련과 '소송기록열람 제한 규정'의 도입을 논의하였다. 다음으로 수사실무 관련규정의 개선방안 부분에서는 기술유출범죄 수사의 효율성을 제고하기 위한 개선방안으로 '통신제한조치의 대상범죄 추가방안'과 '소프트웨어 불법복제 관련강제수사의 허용방안'을 검토하였고, 산업스파이행위의 규제를 위한 개선방안으로 '형사소송법상 함정수사제도의 도입방안'과 '역외관할권 규정의 신설방안'을 제시하였다.

결론에서는 지금까지 논의한 연구내용을 개괄하고 앞으로 첨단기술에 대한 불법적인 유출 및 침해를 방지하면서 이를 효율적으로 보호하기 위한 제안으로 본 연구를 마무리하였다.

[키워드] 첨단기술, 유출방지, 산업기술유출방지법, 형사적 처벌, 형사소송절차, 기술유출범죄수사, 산업스파이

A Study on the relevant Legal regulation's Problems and Improvements from Point of View of Criminal Laws for Preventing Outflow of High-tech Technology

Min-Ji Hong

This research studies problems of certain laws and regulations in a criminal law aspect, which are established to effectively protect high technology and prevent infringement where advanced information and technology of domestic corporations are leaked to competing countries, causing great losses to related corporations and the national economy.

The study examines criminal-law-related problems of a special law, the 'law for leak prevention and protection of industrial technology', which was legislated in 2006 and became effective in April 2007, and provides plans to improve the overall laws and regulations related to high technology leak prevention.

Of all special laws, many questions have been raised regarding the most recently established and enforced 'law for leak prevention and protection of industrial technology' even before the law was established. The questions include provisions defining the concept of subjects of protection, provisions on forms of leaks and infringement acts, and criminal punishment clauses. Although numerous examinations have been made regarding such problems, certain parts are still remaining in the law which may raise issues in a criminal law perspective. Therefore, improvement plans are proposed regarding the laws for prevention of unfair competition and protection of trade secrets where the criminal-law-related issues have been much discussed, whereas the discussion is centered around the industrial technology leak prevention law in the part of 'examination of criminal-law-related problems' of the same law.

The proposed improvement plans for the current laws and regulations related to preventing high technology leaks are discussed in two separate parts – provisions on criminal penalties and provisions on criminal actions. Improvement plans for the provisions on criminal actions are discussed in two parts of legal procedures and investigation practice.

In the conclusion, the overall research discussed is summarized and proposals are provided for prevention of illegal leaks and infringement of high technology and effective protection of high technology.

[Keyword] high technology, leak prevention, industrial technology leak prevention law, criminal penalty, criminal action procedures, technology leak crime investigation, industrial spy