

국제기술이전계약에서의 산업보안에 관한 연구*

서 정 두**

-
- I. 서 언
 - II. 기술이전계약과 산업보안
 - III. 기술이전계약의 법적보호와 문제점
 - IV. 기술유출 방지대책과 모델계약
 - V. 결 언
-

주제어 : 기술이전계약, 산업보안, 영업비밀, 기술보호, 기술유출

I. 서 언

우리나라는 근대화 시대의 기술도입단계에서 제4차 산업혁명 시대의 기술수출 관심국가로 발전하는 과정에 산업현장의 핵심기술이 해외로 유출되어 국가경쟁력의 약화와 당사자간의 무역분쟁 등 심각한 사회문제로 대두되고 있다.

여기서 “기술”(technology)이라 함은 제품의 생산이나 생산공정의 사용 또는 서비스의 제공에 필요한 기술적인 모든 지식으로서, 구체적으로는 과학적인 지식의 응용을 통하여 자연력이나 자연물을 가공, 개량 또는 변경함으로써 이를 인간생활에 이용할 수 있게 하는 발명이나 그 결과물을 비롯하여 바이오 생명공학, 첨단과학산업의 노하우, 영업비밀 등 신지식 분야도 포괄하는 의미로 사용된다.)

* 이 논문은 2017학년도 호원대학교 교내학술연구조성비의 지원으로 연구된 것임.

** 호원대학교 무역경영학부 교수, E-Mail : set01@howon.ac.kr

2 무역상무연구 제76권 (2017. 12)

기술은 그 일부 또는 전부를 재산적 가치가 있는 지식재산권으로 승화시킬 수 있는데, 이렇게 재산권화된 기술을 국경을 넘어 이전하거나 또는 사용자에게 라이선스를 부여하는 것을 “국제기술이전”이라고 하며, 산업현장에서 기술의 소유자와 사용자가 사적으로 특허실시권, 상표사용권 또는 노하우 등의 라이선스계약을 체결하거나, 턴키베이스의 플랜트 건설계약이나 프랜차이즈 계약 등의 일부로 포함시켜 당해 기술이 사용될 공장의 건설이나 상대방 기술인력의 훈련 등을 목적으로 하는 모든 형태의 약정을 “기술이전계약”(technology transfer agreement)이라고 한다.

문제는 정부가 기술이전시의 보안 관련 법률을 제정하고 국가정보원에서 ‘산업기밀보호센터’를 설립하는 등 기술유출방지를 위한 노력을 하고 있으나, 불법적인 기술유출 외에 합법적인 계약에서도 첨단기술이 유출되는 사례가 있고 이를 색출하기 위한 산업보안 전문인력은 물론 국민적 관심도 부족하고 산업현장에서 기술이전계약서를 어떻게 작성할 것인가에서부터 기술이전기간 및 임직원의 퇴사 후 관리까지 어떻게 대응하여야 하는지에 대한 체계적인 연구검토가 부족한 실정이다.²⁾

따라서 본고에서는 다양한 형태로 이루어지는 기술이전계약의 유형과 기술유출의 실태 등 산업보안의 중요성에 관하여 정리하고, 우리나라 및 주요국의 기술이전계약에 관한 법적보호와 문제점을 지적한 후, 국가와 개인차원의 기술유출 방지대책과 구제방법 및 기술보호 모델계약조항을 제시하고자 하는데 연구의 목적을 둔다.

II. 기술이전계약과 산업보안

1. 기술이전계약의 유형

국제적으로 기술이전은 다양한 경로와 방법으로 이루어진다. 예컨대 기계설비, 플랜트 등의 수출을 통한 기술이전, 해외직접투자에 의한 기술이전, 라이선스계약에 의한 기술이전, OEM 수출에 따른 기술이전 등이 있으며, 기술이전계약도 기술창출형, 기술양도형, 기술대여형 등 다양한 형태로 체결되고 있다.³⁾

1) 서정두, “국제기술이전계약상의 불공정조항에 관한 연구”, 무역상무연구 제12권, 한국무역상무학회, 1999. 2, pp. 107~108; 서정두, 국제무역계약, 삼영사, 2007, pp. 293~294.

2) 선행연구로는 박지형, “첨단기술유출 예방을 위한 제도적 발전방안에 관한 연구”, 박사학위 청구논문, 경기대학교 대학원, 2011; 임성환, “해외진출 중소기업의 산업기술보호”, 석사학위 청구논문, 성균관대학교 대학원, 2009; 김웅일, “산업기술의 법적 보호에 관한 연구”, 석사학위 청구논문, 고려대학교 대학원, 2011. 등이 있다.

① 기술창출형계약은 당사자간에 신기술의 창출을 목적으로 하는 계약으로서, 신기술의 개발 관련 내용, 장래 개발된 신기술의 실시허락 등에 관한 내용이 주를 이룬다. 기술개발은 공동연구개발계약이나 위탁연구개발계약으로 이루어지는데, 전자의 경우 당사자 쌍방은 신기술의 공동연구를 위한 주요 의무사항과 연구개발의 성과에 관하여 명확하게 약정하여야 한다. 연구 성과에 관하여는 각자 개발한 것은 단독소유로 하고 공동 개발한 것은 공동소유로 하는 것이 원칙이다. 또 후자의 경우는 당사자간에 소정의 수수료와 약간의 정보·자료를 제공하고 신기술의 연구개발을 위탁하는 계약으로서, 이들 모두 비밀유지조항을 필수로 한다.

② 기술양도형계약은 당사자간에 기술의 소유권 이전을 목적으로 하는 계약으로서, 특허권이나 특허출원, 저작권, 노하우 등이 계약대상이 될 수 있다.⁴⁾ 기술양도의 방법은 당사자간에 기술의 소유권 이전만을 규정하는 기술양도계약이나 당사자 쌍방의 기업합병계약 등에 의하여 이루어지는 것이 일반적이다.

③ 기술대여형계약은 기술의 소유권을 제외하고 사용권만을 상대방에게 허락하는 계약으로서, 여기에는 라이선스계약, 재라이선스계약, 상호라이선스계약, 패키지 라이선스계약 등이 있다. “라이선스계약”(license)이라 함은 기술을 상대방에게 독점적 또는 비독점적으로 실시허락하는 계약을 말하며⁵⁾, 실시권자가 이를 제3자에게 다시 실시허락하는 경우 “재라이선스계약”(sublicense), 당사자 쌍방이 기술을 상호 부여하는 경우 “상호라이선스계약”(cross license), 수개의 기술을 하나의 계약에 묶어 허락하는 경우 “패키지 라이선스계약”(package license)이라고 한다.

2. 산업보안의 의의와 중요성

최근 세계 각국은 첨단기술 확보를 위해 소리 없는 전쟁을 벌이고 있다.⁶⁾ 우리나라는 1990년대 이후 정보통신기술의 발달에 따라 IT 관련 산업이 발전하고, 모바일·디스플레이·로봇·바이오 등 신성장동력 산업을 중심으로 산업구조가 급변하고 있다. 특히 우리나라는 모바일·디스플레이·반도체 산업 등을 필두로 세계 시장에서 첨단기술로 인정받는 분야가 늘어나면서, 국내외 산업스파이들의 표적이 되고 있다. 따라서 산업기술의 해외유출로 인한 경제적 손실을 방지하고 국가경쟁

3) 野口良光, 國內實施契約の實務, 發明協會, 1985, p. 70; 윤선희·조용순, 기술이전계약론, 법문사, 2013, pp. 30~37.

4) V. Korah, *Technology Transfer Agreements and the EC Competition Rules*, Oxford, 1996, p. 123.

5) V. Irish, *Intellectual Property Rights for Engineers*, Inst. of Electrical Engineers, 1994, p. 166.

6) 윤선희·조용순, 전게서, pp. 25~29.

4 무역상무연구 제76권 (2017. 12)

력의 제고를 위하여는 산업보안에 관한 각계의 철저한 대응전략이 필요하다.

“산업보안”이라 함은 광의로는 산업 전반을 모든 형태의 범죄로부터 보호하기 위한 노력으로서, 구체적으로는 범죄로부터 유·무형의 모든 산업자산을 지키는 자산보호와 피해를 막는 손실방지의 활동을 말한다.⁷⁾ 그러나 현실적인 개념으로서 산업보안이란 “산업 활동에 유용한 기술·경영상의 모든 정보나 인원, 문서, 시설, 자재 등이 산업스파이, 경쟁관계자나 기타의 자에게 누설 또는 침해당하지 아니하도록 보호 관리하기 위한 모든 대응방안이나 활동” 또는 “산업체나 연구소에서 보유하고 있는 기술·경영상의 정보 및 이와 관련된 인원, 문서, 시설, 통신 등을 해외의 경쟁 국가나 업체의 산업스파이, 전·현직 임직원, 외국인 유치과학자 등 각종 위해요소로부터 침해당하지 아니하도록 보호하는 활동”으로 정의된다.⁸⁾

우리나라는 2006년에 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지하기 위하여 「산업기술의 유출방지 및 보호에 관한 법률」(이하 “산업기술유출방지법”)을 제정하였다. 이 법은 산업기술⁹⁾과 국가핵심기술 등에 관하여 정의하고, 국가핵심기술의 지정, 국가핵심기술의 수출 등에 대한 승인·신고, 산업기술의 유출과 침해행위의 금지 및 신고, 산업기술보호위원회와 분쟁조정위원회의 설치, 비밀유지의무, 산업기술 유출행위 등에 대한 처벌조항 등을 담고 있다.

3. 우리나라의 기술유출 실태

우리나라는 기업의 글로벌화와 과학기술이 발달하면서 국내 첨단기술을 노리는 산업스파이¹⁰⁾의 활동도 더욱 기승을 부리고 있으며, 최근에는 컴퓨터 등 정보통신

7) 한국산업보안연구학회, 산업보안학, 박영사, 2011, p. 6.

8) 국가정보원, 산업보안실무, 국가정보대학원, 1999, p. 1; 상계서, pp. 6-7.

9) “산업기술”이라 함은 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 행정기관의 장(해당 업무가 위임 또는 위탁된 경우에는 그 위임 또는 위탁받은 기관이나 법인·단체의 장을 말한다)이 산업경쟁력 제고나 유출방지 등을 위하여 이 법 또는 다른 법률이나 이 법 또는 다른 법률에서 위임한 명령(대통령령·총리령·부령에 한정한다. 이하 이 조에서 같다)에 따라 지정·고시·공고·인증하는 다음 각 목의 어느 하나에 해당하는 기술을 말한다. 가. 제9조에 따라 고시된 국가핵심기술, 나. 「산업발전법」 제5조에 따라 고시된 첨단기술의 범위에 속하는 기술, 다. 「산업기술혁신 촉진법」 제15조의2에 따라 인증된 신기술, 라. 「전력기술관리법」 제6조의2에 따라 지정·고시된 새로운 전력기술, 마. 「환경기술 및 환경산업 지원법」 제7조에 따라 인증된 신기술, 바. 「건설기술진흥법」 제14조에 따라 지정·고시된 새로운 건설기술, 사. 「보건의료기술진흥법」 제8조에 따라 인증된 보건신기술, 아. 「뿌리산업 진흥과 첨단화에 관한 법률」 제14조에 따라 지정된 핵심 뿌리기술, 자. 그 밖의 법률 또는 해당 법률에서 위임한 명령에 따라 지정·고시·공고·인증하는 기술 중 산업통상자원부장관이 관보에 고시하는 기술(산업기술유출방지법 제2조 제1호).

기기의 발달로 기술유출 사건은 매우 은밀하게 진행될 뿐만 아니라 그 수법도 첨단화·지능화되고 있다. 산업기술이 유출되는 기업들은 주로 중소기업이고, 임직원의 보안의식과 보안시스템의 부실 등 보안관리가 취약한 것이 특징이다.

국가정보원의 최근 통계자료(2006~2010)에 의하면, 우리나라의 주력업종인 전자, 정보통신 등 첨단산업 분야의 기술유출이 전체의 60%를 차지하고, 대부분의 피해가 산업보안 관련 시스템이 부족한 중소기업에 몰려 있으며, 또 기술유출의 주체는 전·현직 임직원, 협력업체의 임직원, 유치과학자 등 내부인으로 분류되는 인력에 의한 기술유출이 전체의 94%를 차지하여 절대적으로 나타났다.¹¹⁾ 이는 전·현직 임직원이 현재보다 더 나은 조건의 업체를 찾아 중요기술을 유출하는데서 기인한 것으로 해석된다. 따라서 피해예방을 위하여는 각 기업이 임직원의 근로조건 개선, 직무보상 등에 최선을 다해야 하겠으나 이는 결코 쉽지 않은 일이므로 국가나 사회적 합의에 의한 개선대책도 함께 모색해 나가야 한다.

기업 현장에서 발생하는 기술유출의 유형과 실태를 크게 보면, i) 임직원 등 내부인력에 의한 기술유출, ii) 협력업체 등의 계약위반에 의한 기술유출, iii) 경쟁업체나 국가의 산업스파이에 의한 기술유출 등 3가지로 구분할 수 있다.¹²⁾

① 임직원 등 내부인력에 의한 기술유출은 가장 대표적인 현상이다. 경쟁사에서 고액연봉과 인센티브, 개인적인 취약점 등을 이용하여 전·현직 임직원을 유인하거나 핵심인력을 스카우트하여 기술을 유출하는 경우, 대외무역법 등의 수출금지규정을 위반하여 해외의 현지생산에 필요한 기술을 유출하는 경우, 해외 진출국의 법과 제도에 미숙하여 당국의 인·허가과정에서 핵심기술도면을 유출하는 경우, 해외에 파견된 임직원이 개인적인 욕심이나 기업에 대한 불만 등으로 기술을 유출하는 경우, 국내의 외국인 직원이나 현지의 고용인이 경쟁사로 전직하거나 현지에서 직접 창업하여 기술을 유출하는 경우 등이 일반적으로 나타나고 있다.

대표적인 사례로서, 2005년 7월 서울중앙지검 첨단범죄수사부와 국가정보원 산업기술보호센터는 하이닉스 반도체사의 낸드플래시 메모리 웨이퍼 제조기술을 중국으로 유출하려던 동사의 전직 생산기술부장 등 7명을 적발하여 기소한 사건을 들 수 있다.¹³⁾ 이 사건은 과거 임직원 등이 해외로 전직하면서 빼낸 기술을 외국 기업에 넘겨주던 유출 사례와는 달리 해외에 직접 반도체 법인과 공장을 설립하고 현지의 정부기관으로부터 자금지원까지 받으려 시도한 사건이다. 이들 모의가 성

10) “산업스파이”란 경쟁국이나 기업의 산업정보를 부정한 목적과 수단으로 정탐하고 유출하는 일체의 행위를 하는 사람을 말한다(국가정보원 산업기밀보호센터. <http://service4.nis.go.kr>).

11) 국가정보원 산업기밀보호센터(2011. 5). <http://service4.nis.go.kr> 참조.

12) 박지형, 전계논문, pp. 24~28; 임성환, 전계논문, pp. 45~51.

13) 서울중앙지법 2005.9.22, 2005고단3969(하이닉스반도체 웨이퍼 제조기술 유출 사건).

6 무역상무연구 제76권 (2017. 12)

공하여 반도체 첨단기술이 중국으로 유출되었더라면, 국내에서 투입된 직접개발비용을 포함하여 당시 약 12조원에 달하는 경제적 피해가 예상되었고, 우리나라의 반도체산업 발전과 국가경쟁력에 치명타를 입을 수 있었던 순간이었다.

② 협력업체 등의 계약위반에 의한 기술유출도 다양하게 나타나고 있다. 국내의 협력업체가 공동 개발된 핵심부품·장비를 무단으로 수출하거나 위·수탁계약에 의한 해외의 첨단제품 생산과정이나 영업활동을 위해 국내의 기술정보를 수집·제공하여 유출하는 경우, 해외의 하청업체에 생산시설과 제품생산에 필요한 부품과 자재, 공정과정의 노출 등 관리 소홀로 인해 기술이 유출되는 경우, 라이선스계약으로 기술을 이전받은 해외업체가 무단으로 기술을 양허하거나 해외에 합작회사를 설립하여 기술만 빼가고 계약을 파기하는 경우, 외국기업이 국내기업과 합법적인 M&A 계약을 통해 유출하는 경우¹⁴⁾ 등이 파악되고 있다.

대표적인 사례로서, 삼성전자의 협력업체인 미국 어플라이드머티리얼스(AMAT)의 한국지사 AMK의 직원이 2005년 3월부터 6년여간 삼성반도체 공장을 출입하면서 D램, 낸드플래시 메모리 제조공정 등 국가핵심기술을 포함해 총 95건을 유출하고 이중에 13건을 하이닉스 반도체에 넘긴 사건이다.¹⁵⁾ AMK는 삼성전자에 독점적으로 장비를 공급하면서 반도체 공장을 손쉽게 출입하면서 친분 있는 삼성전자 직원을 통해 정보수집, 비밀자료를 빼내는 수법을 사용하였다. 2010년 2월 검찰수사과정에서 삼성전자의 직접적인 피해액은 수천억 원으로 추정되었고, 후발주자와의 기술격차가 좁혀지는 등 간접적인 피해규모는 수조 원에 이를 것으로 추정되었다. 결국 AMAT사는 삼성전자와 화해계약을 통해 부당한 방법으로 기술정보를 획득, 유용했다는 사실을 시인하고 인센티브 방식의 배상합의로 종결되었다.

③ 산업스파이에 의한 기술유출도 최근 들어 급증하는 추세이다. 동일 업종에 경쟁관계에 있는 국가나 업체가 특정기업의 내부 및 협력업체의 인력 매수, 위장취업, 해킹이나 절취 등 불법행위에 의해 기술이 유출되는 경우, 해외의 전시회나 제품설명회 등에 출품한 신제품이 분실되어 핵심기술이 유출되는 경우 등이다.

예컨대 2000년 2월 LG전자의 60인치 PDP TV가 독일 하노바에서 개최된 세계 첨단전자제품 박람회에 전시된 후 뉴델리로 이송 중 분실된 사건, 2001년 4월 삼성전자의 63인치 PDP TV가 미국 라스베이거스의 방송장비쇼에 전시하고자 이송 중 도난된 사건, 국내 K사가 2년간 연구 개발하여 전자제품 등에 사용되는 발포체의 신제품을 중국 저장성에서 생산하던 중 현지 경쟁업체인 J사가 K사의 중국 지사장을 매수하여 기술정보를 절취한 사건은 모두 불법적인 기술유출 사례이다.¹⁶⁾

14) 중국 상하이자동차의 쌍용자동차 인수가 M&A의 대표적인 기술유출 사례이다(임영모, “핵심 기술 해외유출의 실태와 대책”, CEO Information 제472호, 삼성경제연구소, 2004, p. 8).

15) 서울경제, “삼성반도체 핵심기술 美장비업체가 빼돌려”, 2010. 2. 4.

III. 기술이전계약의 법적보호와 문제점

1. 산업기술 보호 관련 해외규범

① 국제조약 : 국제적인 지식재산권, 영업비밀 및 미공개정보의 보호를 규정한 대표적인 국제조약에는 파리협약, WTO/TRIPS 협정, NAFTA 협정 등이 있다.¹⁷⁾

첫째, 파리협약¹⁸⁾은 1883년 산업재산권의 보호를 위해 제정된 최초의 국제조약이지만, 산업스파이 등을 직접 규제하는 조항은 없다. 다만 파리협약은 특허권, 실용신안권, 상표권 등 산업재산권의 보호를 주목적으로 하고 있으나, 그 범위를 확대하여 부정경쟁행위의 방지도 적용범위에 포함하고(제2조 제2항), 또 ‘정직한 산업 또는 상업적 관행에 어긋나는 경쟁행위’를 부정경쟁행위로 규정하고 있는 바(제10b조 제2항), 산업기술의 유출행위를 규제할 수 있는 근거가 충분하다.

둘째, 1995년 WTO/TRIPS 협정¹⁹⁾은 제2장 제7절에서 ‘미공개정보의 보호’라는 제목하에 영업비밀 보호에 관하여 정보가 자신의 동의 없이 건전한 상업적 관행에 반하는 방법²⁰⁾으로 타인에게 공개되거나 획득되거나 또는 사용되는 것을 금지할 수 있도록 하고(제39조 제2항), 정부기관에 제출된 정보보호에 관하여 회원국은 신규 의약품이나 화학물질을 이용한 농약품의 제조허가 요건으로 상당한 노력이 소요된 미공개 테스트나 기타 데이터를 부정한 영업적 사용으로부터 보호할 것이며, 또 그러한 데이터가 공개되는 것을 금지하도록 규정하고 있다(동조 제3항).

셋째, 1994년 NAFTA 협정²¹⁾은 회원국의 영업비밀(trade secrets)에 관하여 국제적으로 특별한 보호를 규정하고(제1711조 제1항), 그러한 영업비밀은 대중에게 비밀로 존속하는 한 영구적으로 보호되어야 함을 강조하고 있다(동조 제3항).

② 미국법 : 미국은 영업비밀 보호와 산업기술의 침해에 관하여 민사적·형사적 구제법 체계를 모두 갖추고 있다.²²⁾ 즉, 영업비밀의 침해행위에 대한 민사적인 구제

16) 중소기업청, 중소기업 기술유출 대응 매뉴얼, 2007, pp. 190~193.

17) 박장혁, “산업기술관련 법체계 정비에 관한 연구”, 석사학위 청구논문, 단국대학교 대학원, 2013, p. 28.

18) 산업재산권 보호를 위한 파리협약(Paris Convention for the Protection of Industrial Property).

19) 무역관련 지식재산권협정(Agreement on Trade-Related Aspects of Intellectual Property Rights).

20) “건전한 상업적 관행에 반하는 방법”이라 함은 최소한의 계약위반, 신뢰위반 또는 그러한 위반을 유도하는 것을 의미한다(서정두, 국제통상법, 삼영사, 2001, pp. 460~461).

21) 북미자유무역협정(North American Free Trade Agreement).

를 위해 1979년 「통일영업비밀보호법」(UTSA), 영업비밀의 불법유출행위에 대한 형사적인 보호를 위해 1996년 「경제스파이법」(EEA)을 제정하였다.²³⁾ 기타 외국인의 투자와 같은 합법적인 접근을 통한 기술유출을 제재하기 위해 2007년에 「엑스-플로리오법」(Exon-Florio Act)을 개정한 「외국인투자 및 국가안보법」(Foreign Investment & National Security Act : FINSA) 등을 제정하였다.

첫째, UTSA는 총 11개 조문으로 구성되어 있는데, 제2조에 영업비밀의 침해행위에 대한 법원명령제도(금지청구권), 제3조에 통상적인 손해배상 및 부당이득 반환청구권을 포함한 넓은 의미의 손해배상청구권을 각각 규정하고 있다.²⁴⁾

둘째, EEA는 외국의 정부, 정부기관 또는 정부관리를 이롭게 할 목적으로 영업비밀을 절취, 복사, 수령하는 등 외국정부나 외국기관과 연계된 고의적인 유출행위에 대해 경제스파이죄로 처벌하도록 규정하고 있다(제1831조).

③ 유럽 주요국법 : 유럽의 독일, 프랑스, 영국 등은 우리나라처럼 국가핵심기술에 대한 산업스파이(espionage)의 처벌을 직접적으로 규정한 단행법이 없다.²⁵⁾

첫째, 독일은 「부정경쟁방지법」(Gesetz gegen den unlauteren Wettbewerb : UWG)에 영업비밀의 보호에 관한 규정을 도입하여 산업스파이에 대한 처벌을 규율하고, 기타 민법, 형법, 대외무역법 등에도 영업비밀의 보호를 위한 민사적·형사적 규정을 두고 있다. 특히 1909년 제정된 부정경쟁방지법은 영업비밀에 대한 피용자의 누설행위와 산업스파이 행위를 부정경쟁행위로 처벌하되(제17조 제1항), 행위자가 영업비밀의 누설시 해당 비밀이 외국에서 사용된다는 사실을 알고 있거나 행위자 스스로 외국에서 사용한 경우에는 가중처벌을 규정하고 있다(동조 제4항).

둘째, 프랑스는 영업비밀의 보호에 관한 별도의 법제를 두지 않고, 기존의 민법, 상법, 형법 등으로 규율하고 있다. 즉, 프랑스 민법은 타인에게 손해를 유발한 행위를 한 자는 자신의 과실로 인한 손해배상을 원칙으로 하며(제1382조), 또 형법은 회사의 임직원에 의한 영업비밀의 누설행위에 대한 처벌규정을 두고 있는데, 외국인에게 누설하는 경우에는 특별히 가중 처벌하도록 하고 있다(제418조).

셋째, 영국은 영업비밀의 보호에 관한 성문법이 존재하지 않으나 영업비밀의 부정사용, 부정공개 등 부정유출행위를 금지하는 다수의 판례법 체계에 의하여 이를

22) Daniel W. Park, "Trade Secrets, the First Amendment, and Patent Law : A Collision on the Information Superhighway", *10 Stan. J. L. Bus. & Fin.*, 2004, pp. 46~61.

23) 「통일영업비밀보호법」(Uniform Trade Secret Act of 1997), 「경제스파이법」(Economic Espionage Act of 1996). 특히 경제스파이법은 이후 2012년 및 2013년에 영업비밀의 보호대상범위를 확대하고 외국 및 경제스파이에 대한 처벌수준을 강화하여 「외국경제스파이처벌강화법」(Foreign & Economic Espionage Penalty Enhancement Act : EEPE)으로 개정되었다.

24) Allison Coleman, *The Legal Protection of Trade Secrets*, Sweet & Maxwell, 1992, pp. 22~26.

25) 손승우, 수탁 중소기업의 기술보호를 위한 개선방안 연구, 중소기업청, 2011, p. 179.

보호하고 있다.²⁶⁾ 즉, 영국에서는 회사의 임직원 등 신뢰관계가 인정되는 당사자가 그 의무를 위반하여 비밀정보를 사용하거나 공개하는 경우 형사상의 절도죄를 적용하고 있으며, 민사상의 금지청구권과 손해배상청구권도 인정하고 있다.²⁷⁾

④ 일본과 중국법 : 일본은 민법에서 부정경쟁행위를 규정하고(제709조), 부정경쟁방지 등 공정한 거래질서와 국제적인 무역규범을 준수한다는 취지에서 1934년 「부정경쟁방지법」을 제정하고, 이외에도 「영업비밀관리지침」, 「기술유출방지지침」등 영업비밀 보호관련 각종 지침을 통해 산업기술을 보호하고 있다.

한편 중국은 자국의 첨단기술과 국가기밀의 누설에 대해 강력한 처벌규정을 두고 있다. 즉, 산업기술의 해외유출 방지를 위해 1993년 「반부당경쟁법」을 제정하고, 기타 「대외무역법」, 「기술수출입관리조례」등을 시행하고 있으며, 특히 산업기밀의 누설행위는 형법 외에 「국가안전법」, 「인터넷관련기밀보호법」등에 의거하여 벌금, 간첩죄, 국가기밀 불법취득죄 등 중형으로 규제하고 있다.²⁸⁾

2. 산업기술 보호 관련 국내규범

우리나라의 산업기술 보호에 관한 대표적인 법률은 「산업기술유출방지법」과 「부정경쟁방지법」(부정경쟁방지 및 영업비밀보호에 관한 법률)이고, 기타 「지식재산기본법」, 「방위사업법」, 「대외무역법」, 「형법」등이 시행되고 있다.

① 산업기술유출방지법 : 본법은 2006년 10월 국가차원에서 산업기술의 유출방지와 보호정책 수립, 산업기술의 유출방지와 관리, 산업기술 보호의 기반구축 및 산업보안 기술의 개발 등을 골격으로 제정되었다.²⁹⁾ 적용범위는 본법의 적용을 받는 대상기관을 기업뿐만 아니라 산업기술을 보유한 대학과 연구기관, 전문기관 등으로 넓히고 대상기술도 영업비밀을 포함한 산업기술 전반으로 확대하였다.

특히 국가연구개발자금이 투입된 국가핵심기술³⁰⁾을 보유한 대상기관에 대하여는 엄격한 정부승인의 의무를 부과하고, 대상기관의 산업기술을 침해하면 형사처벌을 받도록 하며, 대상기관에게도 산업기술의 보호조치, 국가핵심기술의 수출통제, 산업기술 침해의 신고의무 등을 부과하고 있다. 국가핵심기술의 지정·변경·

26) 황의창·황광연, 부정경쟁방지 및 영업비밀보호법, 세창출판사, 2011, pp. 146~147.

27) Allison Coleman, *op. cit.*, pp. 96~100.

28) 정덕배, “중국의 영업비밀 보호제도 고찰”, 지식재산21, 특허청, 2002. 7, pp. 153~155.

29) 현대호·이호용, 산업기술보호법, 법문사, 2013, pp. 65~69.

30) 산업기술유출방지법은 다른 법률에 특별한 규정이 없는 한 이 법이 정하는 바에 우선적으로 따르도록 규정하고 있다(제4조); 김응일, 전계논문, pp. 93~94.

해제는 산업통상자원부장관이 관계중앙행정기관의 장으로부터 대상기술을 통보 받아 산업기술보호위원회의 심의를 거쳐 시행하도록 하고 있다(제9조 제1항).

본법은 불법적인 기술유출(예, 임직원의 퇴사후 불법유출, 산업스파이, 외국정부의 인·허가시 기술유출 등)뿐만 아니라, 합법적인 유출행위(예, 해외매각, 기술이전, 계약, 해외생산 투자, 장비수출, M&A 등)도 예방하고자 한다. 즉, 국가핵심기술의 경우 국가연구개발비를 지원받았으면 수출시 정부의 승인을 받거나 사전신고를 의무화하고 불법적인 수출행위를 금지하며, 기타 국가핵심기술을 보유한 대상기관의 불법적인 해외 M&A, 불법적인 해외 기술이전·매각행위, 정부의 수출금지·금지·원상회복 등의 명령불이행을 금지하도록 규정하고 있다(제11조).

또 본법 제2조에 정의된 산업기술 전반에 대하여도 대상기술의 부정취득·사용·공개행위, 비밀의무가 있는 자의 불법유출행위, 산업기술의 악의취득행위, 선의취득 후 중과실로 알지 못한 악의사용행위 등은 금지하고 있다(제14조).

한편 본법은 산업기술의 유출 및 침해행위에 대한 민사적 구제방법보다 형사처벌에 방점을 두고 있다. 즉, 산업기술을 외국으로 유출 및 침해행위를 한 자에게는 최고 10년 이하의 징역 또는 10억 원 이하의 벌금을 규정함으로써 국내 유출행위보다 가중 처벌하도록 하고 있다(제36조~제39조). 기타 기술유출의 예방차원에서 산업기술 보호의 대상기관은 침해의 행위자를 상대로 법원에 금지·예방 또는 필요한 조치를 청구할 수 있고(제14조의2), 국가핵심기술 및 국가연구개발비로 개발된 산업기술의 경우 대상기관의 장은 즉시 침해사실을 산업통상자원부장관과 정보수사기관장에게 신고하여 필요한 조치를 취하도록 하며(제15조), 다만 본법은 산업기술의 유출 및 침해행위에 따른 분쟁의 신속한 해결을 위해 산업통상자원부 산하에 산업기술분쟁조정위원회를 설치 운용하도록 규정하고 있다(제23조).

② 부정경쟁방지법 : 본법은 1961년 「영업비밀보호법」을 계승하여 1998년 12월 현행 법령으로 확대 개칭하고, 타인의 상표·상호 등을 부정하게 사용하는 등의 부정경쟁행위와 타인의 영업비밀에 대한 침해행위를 방지하여 건전한 거래질서를 유지할 목적으로 전면 개정된 것이다.³¹⁾ 본법에서 “영업비밀”이란 공공연히 알려져 있지 아니하고(비공지성), 독립된 경제적 가치를 가지는 것으로서(경제성), 합리적인 노력에 의하여 비밀로 유지된(비밀유지성), 생산방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상의 정보(정보성)를 말한다(제2조 제2호).

또 본법은 영업비밀에 대한 침해행위도 6가지로 열거하여 규제하고 있다. 즉, i) 영업비밀을 절취·기망·협박 등에 의한 부정취득·사용·공개하는 행위, ii) 부정

31) 윤선희, 지식재산권법, 세창출판사, 2007, p. 520.

취득자로부터 악의취득하는 행위, iii) 선의취득후 악의·중과실에 의한 사용·공개하는 행위, iv) 신의칙을 위반하는 행위, v) 부정공개된 영업비밀을 악의·중과실로 취득·사용·공개하는 행위, vi) 선의취득후 악의·중과실에 의한 사용·공개하는 행위 등을 영업비밀의 침해행위라고 정의하고 있다(제2조 제3호).

한편 본법은 영업비밀의 침해에 대한 민사적·형사적 구제방법을 두고 있다. 즉, 영업비밀의 보유자는 법원에 영업비밀의 부정취득·사용·공개행위에 대한 금지·예방청구권, 폐기·제거 등 청구권, 손해배상청구권, 신용회복조치청구권 등을 행사할 수 있다(제10조~제12조). 또 본법은 영업비밀의 침해에 대한 강력한 처벌조항을 두고 있다. 특히 영업비밀을 외국에서 사용하거나 사용될 것임을 알고서 침해하는 경우 10년 이하의 징역 또는 그 재산상 이득액의 10배 이하의 벌금에 처하도록 함으로써 국내 유출시보다 가중 처벌하도록 규정하고 있다(제18조).

③ 기타 기술보호법제 : 이외에 우리나라는 산업기술 관련하여 i) 지식재산³²⁾의 창출·보호 및 활용을 촉진하고 그 기반 조성을 위한 정부의 기본정책과 추진체계를 마련할 목적으로 2011년 5월 「지식재산기본법」을 제정하고, ii) 전략물자 등 방위산업의 대외경쟁력 강화와 기밀누설을 방지하기 위해 「방위사업법」, 「대외무역법」등을 시행하고 있으며, 또 iii) 영업비밀 등 산업기술의 부정 유출행위에 대하여는 「형법」에 의거 업무상 배임죄³³⁾(제356조), 비밀누설죄(제316조), 장물취득죄(제362조), 증거인멸죄(제155조), 절도죄(제329조) 등으로 규율하고 있다.

3. 산업기술 보호법제의 문제점

WTO 이후 제4차 산업혁명 시대를 맞이하여 기술정보의 중요성이 강조되면서 국내의 기술보호법제도 상당히 개선되었으나 현실적으로 미흡한 점이 많다.

① 현행법상 ‘산업기술’에 관한 정의가 많이 개선되었으나 최근 헌법재판소의 결정문에서 지적하였듯이 아직도 모호한 점이 존재하고, ‘국가핵심기술’의 지정 역시 산업기술의 정의에 해당하는지 불명확하고 애매모호한 점이 있다.³⁴⁾ 또 국가핵심기술의 형사적 구제 관련 ‘외국기업 등’이란 용어를 사용하여 영업중심주의인지

32) “지식재산”이란 인간의 창조적 활동 또는 경험 등에 의하여 창출되거나 발견된 지식·정보·기술, 사상이나 감정의 표현, 영업이나 물건의 표시, 생물의 품종이나 유전자원(遺傳資源), 그 밖에 무형적인 것으로서 재산적 가치가 실현될 수 있는 것을 말한다(법 제3조 제1호).

33) 업무상 타인의 사무를 처리하는 자가 그 임무에 위배하여 재산상의 이익을 취하거나 제3자로 하여금 이를 취득하게 하여 본인에게 손해를 가함으로써 업무상 배임죄를 범한 경우 10년 이하의 징역 또는 3천만 원 이하의 벌금에 처한다(법 제356조).

34) 현재 2013.7.25, 2011헌바39 결정(산업기술유출방지법 제2조 등 위헌소원), pp. 13~15.

설립주의인지 불명확하고 이에 자연인도 포함되는지 언급이 없다(제11조).

② 현행법상 재판의 심리와 판결은 국가안보에 관련이 없는 한, 공개주의를 원칙으로 하기 때문에(헌법 제109조), 영업비밀의 경우 재판과정에서 비공지성의 유지에 어려움이 있다. 또 형사적 구제에서도 영업비밀은 비공지성, 경제성, 비밀유지성을 전제로 하기 때문에, 수사과정에서 중립적인 증거와 진술을 확보하기 어렵고 피의자가 외국인 등과 공모시 수사 지연, 유출된 기술회수 및 처벌이 어려우며, 재판과정에서도 법원은 복합적으로 관대한 처분을 내리는 경향이 있다.³⁵⁾

③ 현행법은 사유재산에 대한 수출제한조치, M&A 통제 등을 취하면서 아무런 보상규정을 두고 있지 않다. 즉, 산업기술유출방지법은 국가핵심기술의 수출뿐만 아니라 대상기관의 해외 M&A 등에 대해 신고의무를 부과하고, 중지·금지·원상회복의 조치를 취할 수 있도록 함으로써 사익보다 국익을 우선하고 있으나, 정당한 보상이나 세금감면 등이 없는 공적제한은 그 자체가 위헌일 수 있으므로³⁶⁾ 이로 인한 법적분쟁이 발생할 수 있고 국가의 보호가 지나쳐 남용될 우려가 있다.

④ 현행법상 국가핵심기술의 사전신고, 정부승인제도와 부정경쟁방지법의 전직 또는 경업금지청구제도는 헌법에 보장된 직업선택(영업)의 자유를 직접적으로 제한할 뿐만 아니라, 자유로운 경쟁을 저해하여 소비자의 이익을 해칠 우려가 있다. 다만 헌법상 국가안보, 질서유지, 공공복리 등 객관적인 사유가 있는 경우 직업(영업)의 자유를 제한할 수 있고(제37조 제2항), 영업비밀이 존속하는 동안 단기간의 전직금지, 경업금지, 동종업종 취업금지 등의 청구는 위헌이 아니다.³⁷⁾

요컨대 우리나라는 산업기술 및 국가핵심기술에 대한 국부의 유출방지와 창출 및 활용을 촉진한다는 차원에서 전 분야별로 해당 산업기술 관련 법체계를 수립하고 있으나, 최근 지나친 국가 개입에 대한 헌법재판소의 위헌결정이 이어지고 산발적인 입법추진으로 인한 규제의 중복성과 비효율성이 지적되고 있다.

이러한 문제점을 해결하기 위하여는 산업기술 관련 법정 기구를 통할할 컨트롤 타워를 설치하고, 장·단기적인 관점에서 기술보호·창출 및 활용에 관한 현행법들의 적용범위 문제, 구제방법의 현실화 문제, 영업비밀의 비밀성 유지문제, 국가통제의 영역축소 및 보상문제 등 법체계를 조정·지원해 나갈 필요가 있다.

35) 법무부 기술유출사범 통계(1999~2006)에 의하면, 490명 기소중 실형은 14.1%에 불과함.

36) 현재 1998.12.24, 89헌마214 등 병합결정; 김웅일, 전제논문, pp. 100~104.

37) 대법 1997.6.13, 97다8229 판결; 대법 2003.7.16, 2002마4380 판결 등 다수.

IV. 기술유출 방지대책과 모델계약

1. 권리주체의 보호역량 강화

산업기술은 그 개발과정에 따라 권리주체가 개인, 기업 또는 국가일 수 있다.

① 발명·영업비밀 등 지식재산의 창작은 인간의 지적활동에 의한 사실행위이므로 그 창작자·개발자 개인에게 권리가 귀속되는 것이 원칙이다. 그러나 기업, 정부 등 발주기관이 관계법령³⁸⁾, 계약강제 등의 방법으로 그 성과물에 대한 소유권을 일방적으로 제한하거나 귀속시켜 문제가 되는 경우가 많은 데, 이는 국가안보나 공익 등 최소한의 범위 내에서만 국한하는 것이 바람직하다.

② 산업기술이 종업원 등의 직무발명³⁹⁾에 관련된 경우에는 특허권 등을 계약이나 근무규정에 따라 기업에 귀속시킬 수 있다. 다만 종업원은 성과물에 대한 정당한 보상을 받을 권리가 있으며(발명진흥법 제15조), 직무발명 외의 종업원 발명에 대해 기업이 특허권 등을 승계하거나 전용실시권을 설정하도록 하는 계약이나 근무규정은 무효이다(동법 제10조 제3항). 또 영업비밀에 관하여도 권리귀속에 관한 직접규정이 없으나 이와 동일한 기준에서 판단되어야 할 것이다.⁴⁰⁾

③ 산업기술이 국가연구개발사업에 의거한 경우에는 이를 국가안보나 공익의 목적으로 활용할 필요가 있거나, 연구기관 등이 국외에 소재하거나, 기타 연구기관 등이 소유하기에 부적합하다고 인정되는 때에는 관계법령에 따라 국가에 귀속시킬 수 있으며, 또 공무원의 직무발명에 대한 권리는 국가나 지방자치단체, 국·공립학교 교직원의 직무발명은 전담조직이 각각 이를 승계 소유할 수 있다.⁴¹⁾

따라서 산업기술의 보호주체도 개인이나 기업 또는 국가이므로, 이들 주체의 보호역량을 강화하여 기술유출방지를 위한 범국가적인 대응전략이 필요하다.⁴²⁾

38) 국가연구개발사업의 성과는 국가연구개발사업에 참여하는 연구형태와 비중, 연구개발성과의 유형 등을 고려하여 대통령령으로 정하는 바에 따라 연구기관 등의 소유로 한다(과학기술기본법 제11조의3 제1항).

39) “직무발명”이란 종업원, 법인의 임원 또는 공무원(이하 “종업원등”이라 한다)이 그 직무에 관하여 발명한 것이 실질상 사용자·법인 또는 국가나 지방자치단체(이하 “사용자등”이라 한다)의 업무 범위에 속하고 그 발명을 하게 된 행위가 종업원등의 현재 또는 과거의 직무에 속하는 발명을 말한다(발명진흥법 제2조 제2호).

40) 영업비밀의 권리귀속은 영업비밀의 성격, 종업원의 직무범위와 기여도, 사용자의 개발비용 부담정도 등 제반사정에 따라 결정된다(정호열, 부정경쟁방지법, 삼지원, 1993, p. 277).

41) 과학기술기본법 제11조의3 제1항 단서; 발명진흥법 제10조 제2항.

① 국가는 앞서 언급한 바 기술보호의 통합관리를 위한 컨트롤 타워를 설치하고 법체계를 조정 정비하면서, 민·관의 유기적 협의체를 구성하여 기술개발자나 기업, 유관기관 및 단체에 정책자료와 기술자문, 사업지원 등 협력을 극대화하고, 기술유출 사범에 대한 국가간 사범공조와 WTO, FTA 등의 국제무역협상에서 우리 기업에 유리한 방향의 산업기술 보호협정을 확대해 나가야 한다.⁴³⁾ 특히 해외진출 기업에 대하여는 기술보호의 역량 강화를 위한 사전교육, 예산지원 및 법률자문, 상대국에 대한 정보와 사이버 콘텐츠의 제공 등에 주력하여야 한다.

② 개인이나 기업은 자신의 기술정보가 과도하게 해외에 노출되지 않도록 기술이전계약시 해당 기술의 목적외 부당사용 내지 재라이선스 금지, 비밀유지의무 등의 조항을 포함시키고 수시로 의무준수 여부를 점검하여야 한다.

특히 기업의 경우 각 부서를 통괄하는 산업기술 보호체제를 구축하고 기술유출 대응 매뉴얼을 작성하여 보안관리규정과 전담조직, 사내보안 자가진단과 외부감사 등의 상시 모니터링을 통해 기술보호 역량을 강화해 나가야 한다.⁴⁴⁾

2. 기술유출 대응방안과 권리구제

산업기술은 기업의 대외활동 과정에서 자연스럽게 유출될 수도 있고 대부분이 전·현직 임직원이나 현지고용인에 의해 이루어지므로, 기술유출 전의 입사에서 퇴사까지 철저한 윤리교육 및 인사관리, 문서 및 시설관리, 사내정보 시스템 관리는 물론 기술유출 후의 분쟁해결을 위한 구제대책도 강구하여야 한다.⁴⁵⁾

① 기업은 종업원의 근로조건 개선, 직무발명 보상제도 및 철저한 업무분담체계 등을 통하여 기술유출 위험성을 최소화시켜야 한다. 특히 종업원 직무발명 보상제도는 기술유출 예방효과와 함께 자발적인 연구개발을 촉진하는 효과도 있다.

② 종업원의 입사단계에서는 적임자의 선발과 초기교육이 중요하다. 즉, 입사시에는 산업기술 측면에서 검증된 자원을 선발하되 비밀유지의무가 포함된 보안서

42) 국가는 산업기술의 유출방지와 보호에 필요한 종합적인 시책을 수립·추진하고, 관련 기관은 종사자들이 부당한 처우와 선의의 피해를 받지 아니하도록 하고, 산업기술 및 지식의 확산과 활용이 제약되지 아니하도록 노력하고, 모든 국민은 산업기술의 유출방지에 대한 관심과 각자의 직업윤리의식 배양에 노력하여야 한다(산업기술유출방지법 제3조 제1항~제3항).

43) 민병설, “산업보안체계의 정립에 관한 연구”, 박사학위 청구논문, 경희대학교 대학원, 2002, p. 153.

44) 한국기술거래소, “해외기술이전에 있어서의 기술유출방지 방안”, 산업기술시장 이슈리포트, 한국기술거래소, 2008, pp. 36~37; 임성환, 전계논문, pp. 82~89.

45) 지식재산연구소, 중소기업을 위한 지식재산 관리 매뉴얼, 특허청, 2006, pp. 135~138.

약서를 징구하고, 회사의 윤리지침, 관련법제 및 위반시 법적 제재 등에 관한 윤리 교육뿐만 아니라, 보안업무규정이나 지침, 주변의 보안사고 사례 등 보안교육을 통하여 경각심을 갖게 하고 회사의 보안관리 노력의 증거로도 활용한다.

③ 재직자에게는 정기면담으로 애로사항을 파악하고, 성과급과 신상필벌제도 등을 활용하여 보안서약서를 징구하고 지속적인 보안교육과 점검을 통해 근무기강을 바로잡아야 하며, 퇴직시에는 기술유출 차단을 위해 출입증, 개인 PC, 디스켓, 연구노트 등 지급물품을 회수하고 영업비밀 보유자 등 핵심인력의 퇴직시에는 최소 기간 동안 경업금지 및 경쟁업체 취업제한 서약서를 작성하게 한다.

④ 해외진출기업의 경우 현지시설에 대한 단계별 방호대책을 수립하여야 하고⁴⁶⁾, 문서자료도 비밀분류, 접근제한 장치 등을 통해 등급별 보안관리를 철저히 하여야 하며, 필요시 국가정보원의 ‘테러정보통합센터’가 운영하는 해외진출기업 안전지원단의 도움을 청할 수도 있다. 또 사내 정보 시스템에 대한 보안관리, 예컨대 서버관리, 내부 통신망, 응용프로그램, 개인 PC 방화벽 설치 및 보안프로그램, 임직원의 인터넷, E-메일 등에 대한 모니터링제도를 도입할 필요가 있다.

그럼에도 불구하고 전·현직 임직원 등에 의해 산업기술이 유출된 때에는, 당사자간의 대화, 소송, ADR 등 다양한 방법으로 분쟁해결을 모색하여야 한다.

⑤ 기술유출시 피해자는 가해자와 직접 대화로 해결하는 것이 기술의 비밀성이 사회에 노출되지 않기 때문에 가장 바람직한 방법이다. 산업기술이 침해된 경우 기술보유자는 소송에 앞서 이를 유출한 전·현직 임직원이나 경쟁업체 앞으로 자신의 기술침해에 대한 경고장을 내용증명으로 발송하고 협상에 임한다.

⑥ 기술보유자는 자신의 영업비밀 등 산업기술을 침해하거나 우려가 있는 자에 대해 법원에 침해금지 또는 예방청구의 소송을 제기할 수 있으며(부정경쟁방지법 제10조 제1항), 또 침해행위로 영업상 이익의 손해나 신용이 실추된 때에는 손해배상청구 또는 신용회복조치의 소송도 제기할 수 있다(동법 제11조와 제12조).

⑦ 기술유출 분쟁은 시간과 비용이 많이 소요되고 재판과정에서 비밀성이 노출될 우려가 큰 소송 이외에 전문가에 의한 알선, 중재, 조정 등 “대체적 분쟁해결”(Alternative Dispute Resolution : ADR) 제도를 검토할 수 있다. ADR은 계약서상에 준거조항을 사전 합의하는 것이 원칙이지만 사후합의로도 가능하며, 특히 중재의 경우 여러 면에서 유용하고 확정판결과 동일한 법적 효력을 갖는다.⁴⁷⁾

46) 예컨대 시설보안은 그 중요도에 따라 공용구역·일반구역·제한구역·통제구역 등으로 구분하여 관리할 수 있다(중소기업청, 중소기업 기술유출 대응 매뉴얼, 2007, p. 81).

47) 중재법 제3조 제2호, 제8조 제1항~제4항, 제35조.

3. 기술유출방지를 위한 모델계약

산업기술 관련 당사자간의 비밀유지의무는 별도의 비밀유지계약서, 일반계약서상의 비밀유지조항 또는 비밀유지각서 등 다양한 방법으로 설정할 수 있다.

특히 비밀유지조항(confidentiality)의 내용은 계약의 종류에 따라 다르겠지만, 대체로 다음의 항목을 포함하여야 한다. 즉, (i) 비밀정보는 허용된 목적과 용도 외에는 사용하지 못하도록 하고, (ii) 비밀유지의 대상정보와 제외사항에 관하여 명확히 정의하고, (iii) 비밀자료의 관리상태를 점검·조사할 권한을 명기하고, (iv) 계약종료시 일체의 비밀정보 반환과 사용금지 및 일정기간 비밀유지의무가 계속되도록 하고, (v) 기술개시자의 임직원, 하청업체 등에게도 비밀유지의무를 부과하고, (vi) 비밀유지의무의 위반에 대한 분쟁해결방법과 준거법 등을 합의하여야 한다.⁴⁸⁾

<예시 1> 비밀정보의 사용이 허용된 목적과 용도 등의 적시

1. The Recipient hereby agrees and acknowledges that the Confidential Information shall be an proprietary asset of the Licensor and be held in strict confidence for the exclusive use and benefit of the Recipient and solely for the manufacture, sale, use or other disposal of the Products hereunder. Without the prior written consent of the Licensor, the Recipient may neither use any of the Confidential Information for any purposes other than the performance of its duties under this Agreement nor disclose, sell, assign or divulge in any manner the Confidential Information to any person or legal entity other than those of its employees and sub-contractors.

<예시 2> 비밀정보의 정의범위와 비밀유지의 적용제외 사항

1. For the purpose of this Agreement, "Confidential Information" means any or all technical knowledge, know-how, standard calculations, data, trade secrets and/or other information regarding financial affairs, processes, materials, apparatus, research, yield, specifications, design, manufacture, sale, use or other disposal of the Products, as of the effective date hereof and thereafter, in the possession of the Licensor (developed or otherwise generally used by the Licensor).

2. It is hereby understood and agreed that the provisions of this Article shall not apply to those informations set forth hereafter :

(a) any information which is already in the public domain prior to the effective date of this Agreement;

(b) any information which the Recipient or its subsidiary has independently developed

48) 서정두, 전게서, pp. 164~166; 윤선희·조용순, 전게서, pp. 190~198.

prior to the effective date hereof;
(c) any information which is disclosed, without any restriction, to the Recipient by a third party who has the right thereto.

<예시 3> 비밀자료의 관리상태에 관한 점검·조사권한 명기

1. Copies of documents or parts thereof containing Confidential Information shall be made only where absolutely necessary and their confidentiality shall be protected in the same manner as that of the originals.
2. All original documents and copies thereof containing Confidential Information, which are no longer required to be held by the Recipient for the purposes indicated in this Article, shall be returned to or destroyed upon the instructions by the Licensor.
3. The Licensor shall have the right to conduct periodic audits of the procedure taken by the Recipient to verify compliance with the rules set forth herein.

<예시 4> 계약종료시 비밀정보 반환, 사용금지와 비밀지속의무

1. In the event of the expiration or termination of this Agreement, the Recipient shall make no further use of Confidential Information furnished and licensed by the Licensor hereunder and shall promptly return to the Licensor at the Recipient's costs.
2. The obligations of the Recipient in this Article hereof will survive the expiration or termination of this Agreement and be in effect during the term of this Agreement and for three (3) years thereafter.

<예시 5> 기술개시자의 임직원, 하청업체 등의 비밀유지의무

1. Except as provided hereafter, the Recipient and Recipient's directors, employees, sub-contractors, representatives and agents shall not at any time divulge or disclose to any third party in any manner, directly or indirectly, any information as to Confidential Information furnished at any time to the Recipient by the Licensor.

<예시 6> 당사자간 의무위반시 분쟁해결방법 및 준거법 합의

1. All disputes or controversies between the parties hereto arising out of or in connection with this Agreement, or for breach thereof, shall be finally settled by arbitration in (*Seoul, Korea*) in accordance with (*the Commercial Arbitration Rules of the Korean Commercial Arbitration Board*) and under the laws of (*Korea*). The award rendered by the arbitrator(s) shall be final and binding both parties concerned.⁴⁹⁾

V. 결 언

산업기술은 개시자의 입장에서는 기술도입시 불공정조건이 우려되지만, 제공자의 입장에서는 보안유지가 가장 민감한 과제로 남는다. 우리나라는 앞서 지적한 바와 같이 모바일·디스플레이·반도체 산업 등을 필두로 세계시장에서 첨단기술로 인정받는 분야가 늘어나면서 산업스파이들의 표적이 되고, 산업기술의 해외유출로 인한 막대한 경제적 손실과 국가경쟁력의 약화요인이 되고 있다.

기술유출은 아주 은밀하게 진행되고 수법도 지능화되어 가는데, 주로 종업원의 보안의식과 보안시스템 등 보안관리가 취약한 중소기업의 피해가 크고 유출경로도 전·현직 임직원, 협력업체 등 내부인이 절대적인 것으로 나타났다.

이에 산업기술 관련 국내·외의 보호규범도 점차 강화되고 있다. 즉, 국제적으로 WIPO, WTO, NAFTA 등의 국제조약에서 산업정보에 관한 보호의무를 강조하고, 미국·독일·프랑스·일본 등 기술선진국은 오래 전부터 기술침해에 관한 강력한 민사적·형사적 구제법제를 갖추고 있으며, 특히 해외유출의 경우 가중 처벌하도록 하고 중국은 간첩죄, 국가기밀 불법취득죄 등 중형까지 적용하고 있다.

우리나라는 기술보호를 위해 산업기술유출방지법과 부정경쟁방지법을 제정하고, 기타 지식재산기본법·대외무역법·형법 등을 시행하고 있다. 특히 해외유출의 경우 산업기술유출방지법에서는 10년 이하의 징역과 10억 원 이하의 벌금, 부정경쟁방지법에서는 10년 이하의 징역과 재산 이득액의 10배 이하의 벌금으로 가중 처벌하도록 하며, 형법에서는 업무상 배임죄, 절도죄 등으로 규율하고 있다.

그러나 최근 산업기술에 대한 국가 개입이 지나치다는 헌법재판소의 위헌결정이 이어지고, 정부의 산발적인 입법추진에 대한 중복성과 비효율성이 지적되고 있다. 따라서 정부는 산업기술 관련 각종 기구의 컨트롤 타워를 설치하고 장·단기적으로 기술보호·창출 및 활용에 관한 법체계를 정비하여 개인·기업 및 국가의 보호역량 강화와 기술유출방지를 위한 대책을 선제적으로 마련하여야 한다.

특히 개인이나 기업의 경우 재산권 보호차원에서 스스로 산업기술 보호시스템을 구축하고 온·오프라인 보안관리를 강화하여야 하며, 당사자간의 계약시에도 비밀유지조항을 설정하여 비밀정보의 사용목적과 용도 및 적용제외 등을 명확히 하고, 비밀자료의 정기적인 점검, 계약종료시 비밀정보의 반환 및 비밀지속의무, 계약위반에 대한 구제방법과 준거법 등을 명시적으로 합의해 두어야 한다.

49) 분쟁해결방법과 준거법을 일방적으로 지정하는 계약조항은 불공정행위에 해당할 수 있다.

참 고 문 헌

- 국가정보원, 산업보안실무, 국가정보대학원, 1999.
- 서정두, 국제무역계약, 삼영사, 2007.
- 손승우, 수탁 중소기업의 기술보호를 위한 개선방안 연구, 중소기업청, 2011.
- 윤선희, 지식재산권법, 세창출판사, 2007.
- 윤선희 · 조용순, 기술이전계약론, 법문사, 2013.
- 중소기업청, 중소기업 기술유출 대응 매뉴얼, 2007.
- 지식재산연구소, 중소기업을 위한 지식재산 관리 매뉴얼, 특허청, 2006.
- 한국산업보안연구학회, 산업보안학, 박영사, 2011.
- 현대호 · 이호용, 산업기술보호법, 법문사, 2013.
- 황의창 · 황광연, 부정경쟁방지 및 영업비밀보호법, 세창출판사, 2011.
- 김응일, “산업기술의 법적 보호에 관한 연구”, 석사학위 청구논문, 고려대학교 대학원, 2011. 12.
- 민병설, “산업보안체계의 정립에 관한 연구”, 박사학위 청구논문, 경희대학교 대학원, 2002.
- 박지형, “첨단기술유출 예방을 위한 제도적 발전방안에 관한 연구”, 박사학위 청구논문, 경기대학교 대학원, 2011. 2.
- 서정두, “국제기술이전계약상의 불공정조항에 관한 연구”, 무역상무연구 제12권, 한국무역상무학회, 1999. 2.
- 임성환, “해외진출 중소기업의 산업기술보호”, 석사학위 청구논문, 성균관대학교 대학원, 2009.
- 정덕배, “중국의 영업비밀 보호제도 고찰”, 지식재산21, 특허청, 2002. 7.
- 한국기술거래소, “해외기술이전에 있어서의 기술유출방지 방안”, 산업기술시장 이슈리포트, 한국기술거래소, 2008.
- 野口良光, 國內實施契約の實務, 發明協會, 1985.
- Coleman, A., *The Legal Protection of Trade Secrets*, Sweet & Maxwell, 1992.
- Irish, V., *Intellectual Property Rights for Engineers*, Inst. of Electrical Engineers, 1994.
- Korah, V., *Technology Transfer Agreements and EC Competition Rules*, Oxford, 1996.
- Park, Daniel W., “Trade Secrets, the First Amendment, and Patent Law : A Collision on the Information Superhighway, *10 Stan. J. L. Bus. & Fin.* 46., 2004.

ABSTRACT

The Industrial Security along with the International Transfer of Technology

Jung-Doo SEO

The industrial technology (including trade secrets), which is commonly understood as systematic and applied technical knowledge, can be transferred to third parties by contracting for the transfer of technology or by granting of a licence. The activity of industrial espionage, due to the gradual increase of the economic interests of intellectual property, is displaying intensively in order to gain advanced technology information.

With our outstanding high technology, but compared to the level of the advanced countries, the technical protection systems, the legal protection measures and the systematic management thereof may still be insufficient. Our industrial technology outflow abroad, due to the vulnerability to the security control system in our country, has been increasing since the 2000.

Computer software and SNS, such as smart devices, appear as a rapid change in the technical information environment. In order to minimize the dead zone of a new industrial security, the country's organic activity is being conducted. In 2006, Industrial Technology Outflow Prevention and Protection Law was enacted, which emphasized the responsibilities of the country.

In this paper for the economic entity's efforts to prevent technology leakage overseas, I have looked to how the industrial technology can be protected in terms of national security and economic benefits of our enterprises.

To solve the above-mentioned problems hereof, Korean government should willingly establish a reliable legal system for supporting to enterprise's operations, and Korean companies should autonomously introduce a synthetic technology protection system and incorporate the confidentiality clauses in an international transfer of technology agreement with third parties.

Keywords : Transfer of Technology, Industrial Security, Trade Secrets