첨단산업기술유출의 방지대책현황과 법적 동향

A Legal Trend and Preventive Measure on the High-Technology Industry Drain

김동복
남부대학교

Kim dong-bok
Nambu Univ.

요약

고도지식정보화사회는 컴퓨터의 보급과 인터넷의 급속한 확대를 재촉하고 있으며, 컴퓨터를 행위의 수단과 목적으로 하는 컴퓨터범죄는 그 형태가 일정하지 않고 매우 복잡다기하며 사이버범죄라고도 부른다. 최근 선박제조 핵심기술적발 등 산업기술유출적발사건으로 올 들어 100조원의 국부유출을 방지한 사건 등을 감안해볼 때 첨단산업기술유출방지방안의 마련이 시급한 실정에 놓여 있다. 본 연구는 핵심산업기술유출의 현황과 방지대책에 관한 법적 검토를 연구의 초점으로 하고자 한다.

Abstract

We live in high level of knowledge and information society spread of computer and rapid expansion of internet. Computer crime is various, complicated and inscrutable. we call it cybercrime. Therefore we should draw up a preventive device of the high-technology industry drain. This study is focused on the legal trend of preventive measure on the high-technology industry drain.

I. 들어가는 말

세계화시대 및 정보화시대에 접어들고 있는 시점에 국가 또는 기업간에도 무한경쟁에서 우위를 점하기 위하여 국가, 기업 및 개인의 산업기술 등 영업비밀을 확보하기 위하여 치열한 산업스파이 활동을 전개하고 있다.

현재의 기업환경에서는 어느 기업도 산업스파이로부터 자유롭지 못하며 외부에서 회사 전산망으로 들어오는 해커를 막는 등 사이버테러방지대책도 중요하지만, 언제 어디서나 내부 지권에 의해 유출될지 모르는 기업정보유출에 대한 방지대책 또한 매우 중요하다.

2007년 5월에는 기아자동차의 한 간부가 자동차 핵심 조립기술을 중국으로 빼돌리려다 붙잡혔는데 유출되었을 경우 22조원의 손실을 입을 것이고, 포스코의 정보기술(IT) 계열사인 포스데이타 전현직 연구원들이 휴대인터넷 와이브로의 원천기술을 미국에 팔아넘기려다 적발된 사건도 있었는데 유출되었을 경우 15조원의 손실을 입었을 것으로 추정된다. 2007년 7월에는 대우조선해양의 퇴직 임원이 핵심 설계도면 15만 장을 중국에 넘기려다 발각되었는데 유출되었을 경우 중국업체는 앞으로 5년간 최소 35조원 규모의 수주를 할 수 있었을 것으로 추산하고 있다. 국가정보원에 따르면 2003년 6건에 머물던 기술 유출사건 검거실적은 2004년 26건, 2005년 29건으로 늘었다. 이 기술이 모두 유출되었을 경우 한국 산업계가 보았을 그 피해액이 82조원으로 추정하고 있다.

가장 최근에는 포스코의 전직 연구원들이 철강 제조의 핵심 신기술을 중국 경쟁사에 팔아넘겼는데, 이번에 유출된 자료는 포스코가 지난 10년간 450억원을 투자해 개발한 것이며 이는 고급 전략 제품의 제조공정 원가를 절감하는 실용기술이어서 향후 추정되는 피해액이 2조 8000억원에 이른다고 한다.

이제 우리도 산업기술 등을 개발하고 발전시키는 것 뿐만 아니라 산업기술의 유출을 막고 이를 보호하는 것이 중대한 과제가 되고 있으므로 산업기술유출방지에 관한 법적, 제도적, 기술적 대책이 절실히 요구되는 시점에 놓여 있다.

본고는 산업기술유출에 관한 방지대책 중 보안관리를 중심으로 검토한 후 산업기술유출관련법안의 문제점과 개선방안을 제시하는 것을 목적으로 한다. 무엇보다도 법적 대응방안에 연구의 초점을 두기로 하며 지면의 한계상 깊이 있는 연구는 이루지지 못한 아쉬움 속에 문제의식을 던지는 정도의 발표로 진행하고자 한다.

II. 첨단산업기술유출행위의 일반론과 방지대책으로서 보안관리

1. 산업기술유출행위의 일반론

1.1 영업비밀 및 산업기술의 의의

영업비밀이란 개념은 단일한 법적 성질로부터 나오는 것이 아니기 때문에 명확하게 정의하기 어렵지만, 부정경쟁방지및

영업비밀보호에관한법률에 의하면(제2조 제2호) “영업비밀이라 함은 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 생산방법・판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다”고 정의되고 있다. 대법원도 영업비밀에 관하여 동법에 따라 정의하면서 “영업비밀의 보유자인 회사가 직원들에게 비밀유지의 의무를 부과하는 등 기술정보를 엄격하게 관리하는 이상, 역설계가 가능하고 그에 의하여 기술정보의 획득이 가능하더라도 그러한 사정만으로 그 기술정보를 영업비밀로 보는 데에 지장이 있다고 볼 수 없다”고 판시한 바 있으며[1], “해외로부터 도입・개량한 제조기술 등의 정보”도 영업비밀로 인정하고 있다. 이러한 영업비밀에 대해서는 기업비밀, 재산적 정보, 트레이드 시크리트(trade secret), 노우하우(know how) 등의 용어로 다양하게 불리우고 있으나 모두 유사한 개념이다.

“산업기술”이란이라 함은 제품 또는 용역의 개발・생산・보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 관계중앙행정기관의 장이 소관 분야의 산업경쟁력 제고 등을 위하여 법령이 규정한 바에 따라 지정 또는 고시·공고하는 기술로서 다음 각 목의 어느 하나에 해당하는 것을 말한다(산업기술의 유출방지 및 보호에 관한 법률 제2조).

가. 국내에서 개발된 독창적인 기술로서 선진국 수준과 동등 또는 우수하고 산업화가 가능한 기술

나. 기존제품의 원가절감이나 성능 또는 품질을 현저하게 개선시킬 수 있는 기술

다. 기술적・경제적 파급효과가 커서 국가기술력 향상과 대외경쟁력 강화에 이바지할 수 있는 기술

라. 가목 내지 다목의 산업기술을 응용 또는 활용하는 기술

"국가핵심기술"이라 함은 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술로서 동법 제9조의 규정에 따라 지정된 산업기술을 말한다. 즉 국가안보적 관점에서 볼 때 국가핵심기술이란 수출이 통제되는 전략물자 관련제품 및 국내에서 연구개발이 진행되고 있는 방산제품에 내재되어 있는 관련 산업기술 등을 포괄하는 헌법상 개념이라고 볼 수 있으며, 국민경제적 관점에서 보게 되면 현재의 위상과 미래의 가능성을 감안할 때, 유출시 국민소득 산업경쟁력 무역수지 고용 등을 감소시켜 국민경제에 중대한 악영향을 줄 수 있는 산업기술을 국가핵심기술로 볼 수 있다. 시장적 관점에서는 현재 세계시장에서 차지하는 점유율이 높은 제품에 내재하는 기술로서 유출시 부메랑 효과가 발생하여 우리나라의 관련 산업에 기술적 파급효과가 큰 산업기술이라고 할 수 있다.

1.2 금지행위의 유형과 처벌규정

1) 금지행위의 유형

산업기술유출방지관련법(이하에서는 부정경쟁방지 및 영업비밀보호에 관한 법률과 산업기술의 유출방지 및 보호에 관한 법률을 산업기술유출방지관련법이라고 한다)에 의하면, 부정취득행위란 절취・기망・협박 그 밖의 부정한 방법으로 산업기술을 취득한 행위 또는 그 취득한 산업기술을 사용하거나 공개하는 행위이다(산업기술의 유출방지 및 보호에 관한 법률 제14조 각 호).

불법유출행위란 산업기술의 유출방지 및 보호에 관한 법률 제34조의 규정 또는 대상기관과의 계약에 따라 산업기술에 개한 비밀유지의무가 있는 자가 그 산업기술을 절취・기망・협박 그 밖의 부정한 방법으로 유출하는 행위 또는 그 유출한 산업기술을 사용하거나 공개하거나 제3자가 상용하게 하는 행위를 말한다.

악의 취득행위란 부정취득행위 또는 부정유출행위가 개입된 사실을 알고 그 산업기술을 취득・사용 및 공개하는 행위를 말한다. 부정취득행위에 대하여만 적용하는 민법상의 불법행위와 달리 사후 관여자에 대한 처벌이 가능하다.

선의취득 후 악의 사용행위란 부정취득행위 또는 부정유출행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득・사용 및 공개하는 행위를 말한다. 산업기술은 특허 등과 달리 등록에 의한 공시성를 갖지 않음으로 경과실까지 불이익을 둔다면 기술거래를 부당하게 제한할 우려가 있다.

승인없이 국가핵심기술을 수출하는 행위란 산업자원장관의 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술의 수출을 추진하는 행위를 말한다.

명령 불이행 행위란 국가핵심기술에 관한 산업자원부장관의 수출중지・수출금지・원상회복 등의 명령에 위반하는 행위를 말한다.

2) 처벌규정

산업기술의 유출방지 및 보호에 관한 법률에 의하면, 산업기술을 외국에서 사용하거나 사용되게 할 목적으로 산업기술을 유출하거나 침해하는 행위를 한 자는 7년 이하의 징역 또는 7억원 이하의 벌금에 처하고, 동법 제14조 각 호에 해당하는 행위를 한 자에 대해서는 5년 이하의 벌금에 처한다(제36조). 이와 같은 범행의 예비 또는 미수범을 처벌하며(제37조 제1항), 위와 같은 범행의 예비 또는 음모한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고(동조 제2항), 양벌규정을 두어 법인 등도 처벌하고 있다(제38조).

또한 부정취득행위 또는 부정유출행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개한 경우에는 3년 이하의 징역 또는 5억원 이하의 벌금에 처한다. 비밀유지의무가 있는 자가 비밀을 누설한 경우에는 5년 이하의 징역이나 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

2. 산업기술유출행위의 방지대책으로서 보안관리

2.1 서언

산업기술유출행위을 방지하려면 외부에서 회사 전산망으로 들어오는 해커를 막는 등 사이버테러방지대책도 중요하지만, 언제 어디서나 내부 직원에 의해 유출될지 모르는 기업정보유출에 대한 방지대책 또한 매우 중요하다. 즉 정부기관이나 기업의 내부직원에 의해 핵심기술이 새어나가고 있으므로 이제는 이에 대한 효율적인 방어대책의 수립이 시급한 실정이다.

일반적으로 정보자산을 효과적으로 보호하고 기업비밀의 유출방지를 위해서는 보안정책이나 제도, 보안 솔루션, 또는 종업원에 대한 교육 등이 있는 바, IT환경에 변화에 따라 지속적인 개혁이 이루어져야 한다.

산업스파이로부터 산업기술을 방지하려면 보안관리가 보안인프라 중 가장 중요한 핵심요소로 간주해야 한다. 즉 채택한 정책이나 제도, 솔루션들이 지속적으로 활성화될 수 있도록 하는 수단이 보안관리이기 때문이다. 여기서는 보안관리에 대한 개괄적 검토에 그치기로 한다.

2.2 정보보안의 개별적 요소

정보보안의 개별적 인프라에는 정보보안정책, 정보보안전략, 정보보안조직, 기술적 측면의 정보유출방지, 정보보안관리절차 등이 있다.

첫째, 보안정책으로는 기업 소속원 개개인에게 정보보안이 비즈니스의 성공요인이라는 정보보안목적을 고취해야 하고 동시에 고객 및 고객의 개인정보보호가 최우선과제라는 전제하에 보안을 추진해야 한다. 이러한 목적을 달성하기 위해 보유하고 있는 모든 정보자산을 대상으로 소유, 책임, 분류, 추적성 네 가지 기본전략을 바탕으로 이에 대한 효과적인 적용을 위한 지속적인 관리사이클을 운영하여야 한다.

둘째, 기업내 침해사고 대응, 정보유출사고 및 예방업무를 상시적으로 수행하기 위해서는 전담 보안팀의 구성이 필수적이며, 보안 전략수립과 보안기술지원, 사고대응, 보안수준평가 등의 업무를 수행해야 한다.

셋째, 정보자산 방지대책을 위하여 기본적으로 선행되어야 할 대표적인 보안기술로서 “문서보안기술”과 “통합인증권한관리(EAM)” 등을 마련하여야 한다. 산업기술유출은 아무리 강력한 방화벽이 설치되어 있더라도 내부자의 산업기술유출은 속수무책이다. 따라서 문서보안은 산업기술유출 경로를 원천적으로 차단하고, 사내 내부 핵심정보와 지식을 안전하게 보호해주는 역할을 한다. 문서보완과 DRM(Digital Rights Management, 디지털저작권관리를 의미한다.)은 기술적으로 흡사하며 두 개념 모두 암복화기술과 사용자권한관리기술을 기반으로 한다. EAM(Extranet Access Management)은 말 그대로 엑스트라넷에 사용자가 접근하는 것을 판단해 인증해주는 솔루션이다. 즉 사용자인증과 데이터 또는 응용프로그램 접근을 관리하는 통합 솔루션이다.

마지막으로 정보보안관리절차인 바, 정보보안에 관한 정책, 제도, 조직, 기술들을 상호 밀접한 연관관계를 가질 수 있도록 연계 또는 결합시켜야 한다[2].

2.3 결어

기업이 존재한 이래 변하지 않고 변할 수도 없는 내용이 바로 보안관리이다. 어떻게 보안수준을 마련하고 직원들이 자발적으로 보안을 인식하고 관심을 쏟게 하는냐가 관건이다.

무엇보다도 외부로부터 침입하는 보안침해 못지 않게 내부로부터 유출되는 산업기술의 보호에 대한 보안관리가 더욱 중요한 시대이다.

Ⅲ. 첨단산업기술유출규제에 관한 현행법상의 문제점과 개선방안

1. 산업기술유출규제에 관한 현행법의 규정

1.1 부정경쟁방지 및 영업비밀보호에 관한 법률

이 법은 국내에 널리 알려진 타인의 상표·상호 등을 부정하게 사용하는 등의 부정경쟁행위와 타인의 영업비밀을 침해하는 행위를 방지하여 건전한 거래질서를 유지함을 목적으로 한다. 종전에는 기업의 전·현직 임직원이 기술상 영업비밀을 제3자에게 누설한 경우만을 형사처벌의 대상으로 삼았고, 양벌규정도 없었으며 친고죄였던 것에 비하여 훨씬 형사책임이 강화된 것이다.

1.2 산업기술의 유출방지 및 보호에 관한 법률

산업기술의 유출방지 및 보호에 관한 법률은 2006. 10. 27. 공포되어 2007. 4. 29.부터 시행되고 있다. 동법은 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지함을 목적으로 한다.

동법은 부정경쟁방지 및 영업비밀보호에 관한 법률이 민간기업비밀누설에만 처벌이 한정되어 있고 각종 법률에 산재하

고 있는 관련 규정으로는 산업기술유출방지 및 근절에 효과를 내지 못하고 있고 국가안보에 직접적인 영향을 미치는 국가핵심기술의 해외유출을 규제하고, 산업기술의 부정한 유출을 방지하기 위한 보안의식 확산 및 제도적 기반의 구축을 통해 국가산업경쟁력을 강화하고 국가의 안전과 국민경제의 안정을 보장하기 위한 것이다.

1.3 양 법률의 특징과 상위점

부정경쟁방지 및 영업비밀보호에 관한 법률은 영업비밀 침해행위를 부정경쟁행위방지차원에서 다루고 있으며, 산업기술의 유출방지 및 보호에 관한 법률은 산업기술유출행위를 국익보호차원에서 접근하고 있다. 이러한 제정목적상의 차이로 인하여 부정경쟁방지 및 영업비밀보호에 관한 법률은 침해금지청구권, 손해배상청구권, 신용회복청구권 등과 같은 민사적 구제에 치중하고 있는 반면, 산업기술의 유출방지 및 보호에 관한 법률은 기술유출행위에 대한 강력한 형사적 규제와 기술유출방지정책수립, 산업기술보호위원회설치 등과 같은 보안시스템 확충에 중점을 두고 있다.

2. 양 법률의 문제점

2.1 보호범위의 중복여부

부정경쟁방지 및 영업비밀보호에 관한 법률은 영업비밀침해에 대한 민사적 구제절차와 동시에 형벌을 규정하고 있다. 또한 산업기술의 유출방지 및 보호에 관한 법률도 산업기술의 유출행위에 대하여 형벌을 규정하고 있어 보호범위에 대한 중복가능성이 일어날 문제점이 있다. 부정경쟁방지 및 영업비밀보호에 관한 법률상 “영업비밀”은 고객관리명부, 시장조사정보, 판매지침서와 같은 경영상의 정보를 포함하는 개념인 반면, “산업기술”은 기술상의 정보만을 지칭하는 개념으로써“영업비밀”이“산업기술”에 포함되는 개념으로는 볼 수 없다. 이상에서 살펴본 바와 같이 양 법률의 보호범위는 약간의 차이점이 있다. 그러나 이러한 보호범위상의 차이점에도 불구하고, 최근에 산업기술의 대부분이 부정경쟁방지 및 영업비밀보호에 관한 법률상의 보호대상인 영업비밀에 해당하며, 또한 산업기술의 유출방지 및 보호에 관한 법률상의 보호범위에 해당하는 국가핵심기술도 해당된다는 점에서 향후 양 법률 중 어느 법률의 보호범위에 해당하는지에 대한 혼선이 빚어질 우려가 있다[3].

부정경쟁방지 및 영업비밀보호에 관한 법률은 영업비밀의 성립요건으로 비공지성, 비밀관리성, 경제적 유용성을 들고 있으나 지금까지 산업기술유출 사건 발생시 영업비밀의 성립요건인 비공지성, 비밀관리성, 경제적 유용성에 대한 엄격한 판단으로 인하여 부정경쟁방지 및 영업비밀보호에 관한 법률로 처벌하기 어려운 면이 있었다.

2.2 형사적 규제의 중복여부

부정경쟁방지 및 영업비밀보호에 관한 법률과 산업기술의 유출방지 및 보호에 관한 법률은 각 영업비밀 침해행위, 산업기술침해행위를 규정하고 있다. 양 법률은 국외유출행위에 대해서는 가중처벌규정을 두고 있다는 점, 침해행위의 예비음모죄 및 미수법에 관한 처벌규정을 두고 있으며, 배후자 처벌을 위하여 양벌규정을 두고 있는 점이 공통점이다. 다만 산업기술의 유출방지 및 보호에 관한 법률상에 특별히 규정되는 있는 침해유형으로는 동법 제14조 제5호 국가핵심기술에 대한 해외매각 등의 승인절차 의무를 위반하였거나, 부정한 방법으로 승인을 받아 해외매각 등을 추진하는 행위를 금지하고 있다. 또한 산업자원부장관의 국가핵심기술에 대한 수출중지·금지·원상복귀 등의 명령 등을 이행하지 않는 행위를 산업기술침해행위로 규정하고 있다.

따라서 산업기술유출규제에 관한 현행법상 대표적 법률인 양 법률이 동시에 형사적 규제를 각 규정하고 있다는 것은 법제상 중복이고 효율성이 떨어지는 폐단이 있다.

3. 개선방안

부정경쟁방지 및 영업비밀보호에 관한 법률과 산업기술의 유출방지 및 보호에 관한 법률간의 중복적용문제를 해결하는 방안으로 양 법률간의 조정규정을 두는 방법이 있다. 그러나 현재에도 영업비밀에 대한 요건판단이 어려운 상황에서 조정규정의 신설만으로는 기술유출 발생시 어느 법을 적용할 것인지에 대한 판단이 어려워 법 적용상의 곤란함이 발생할 것이다. 따라서 양 법률의 중복적용문제는 단순히 조정규정으로 해결하는 것이 아니라 양 법률의 개정이 근본적인 해결책이 될 것이다.

그러므로 현행 부정경쟁방지 및 영업비밀보호에 관한 법률과 산업기술의 유출방지 및 보호에 관한 법률을 그대로 유지하도록 하고, 부정경쟁방지 및 영업비밀보호에 관한 법률은 본래 법 목적상의 취지에 맞게 영업비밀 침해행위에 대한 민사적 규제에 관한 사항만을 규정토록하고, 산업기술의 유출방지 및 보호에 관한 법률은 그 동안 국내 법제에 미흡했던 사전보안의식 및 사전보안체제 확립에 대한 근거 법률적 역할과 함께 기술유출에 대한 강력한 형사적 규제를 담당토록 양 법률을 각 개정하여 이원화시키는 방안이 바람직하다고 본다[4].

물론 이와 같은 법체제로 나아갈 경우 양 법률에 대한 대폭적인 개정작업이 이루어져야 하는 번거로움과 복잡함이 예상되지만 양 법률의 충돌을 막고 각 법의 목적에 따른 역할을 강화함으로써 완벽한 산업기술유출방지시스템이 마련될 수 있

다고 본다.

Ⅳ. 맺음말

세계최고의 기술을 자랑하는 국내 자동차 생산관련 핵심기술과 우리나라가 세계최초로 개발한 와이브로 기술, 또한 세계시장 점유율 1위인 국내조선기술 등이 통째로 해외로 유출하려던 사건이 적발되어 우리 사회에 큰 충격과 경종을 울리고 있다.

첨단산업기술유출방지에 관하여 아무리 훌륭한 법과 제도및 보안시스템이 구축되어 있다 하더라도 산업기술을 개발·관리하는 사람들의 보안의식과 윤리의식이 부족하다면 산업기술유출을 막는데 한계가 있다. 따라서 산업기술유출을 방지하려면 먼저 산업기술을 개발·관리하는 사람들의 보안의식과 윤리의식의 고취가 선결되어야 하고 부단한 교육이 필요하다. 동시에 직무발명제도의 적극적인 활용 등 연구원들의 연구성과에 대한 적절한 보상과 인센티브를 부여하고 근무환경을 개선해 줌으로써 애사심과 근무의욕을 고취시키는 등 핵심인력에 대한 기업과 국가차원의 관심과 배려가 요구된다.

또한 산업기술유출방지에 대한 예방대책에 만전을 기해야 하며, 기업과 연구소의 자체적 보안대책과 아울러 국정원의 산업기밀보호센터 운영 등 범정부 차원의 예방대책도 아울러 병행되어야 한다.

▌참 고 문 헌▐

[1] 대법원 1999. 3. 12. 선고 98도4704 판결.
[2] 한국정보통신수출진흥센터, 산업보안과 기술유출, p.125, 2004.
[3] 조용순, 홍영서, “산업기술 유출규제에 관한 법적 고찰”, 산업재산권연구, pp.306-307, 2006.
[4] 조용순, 홍영서, “산업기술 유출규제에 관한 법적 고찰”, 산업재산권연구, p.311, 2006.