산업보안범죄의 실태 및 대응방안

서봉성* · 임유석**

요 약

현대사회의 무한경쟁시대는 경제적 가치가 매우 큰 최첨단 과학기술을 확보·선점하는 것이 국가의 경쟁력에 상당한 영향력을 미치게 된다. 이러한 국가의 핵심기술이나 기업의 최첨단 기술을 탈취해가는 산업보안범죄는 국가의 경제안보에 위협적인 피해를 줄 수가 있고, 방위산업 분야의 경우 국가안보와 직결되어 있는 심각한 범죄에 해당한다. 한번 유출된 국가의 핵심기술과 기업의 영업비밀은 회수가 불가능하기 때문에 엄격한 처벌과 대책으로 산업보안 침해범죄를 미연에 방지해야 한다. 일부 선진외국에서도 국가의 경제 및 국가안보와 직결된 산업보안범죄에 대해서는 국가차원에서 관리 가능하도록 법과 제도들이 운영되고 있다. 최근 들어 국내에서도 국가핵심기술이 침해되는 사례가 급증하고 있으며, 아울러 기업의 핵심적인 산업기술을 유출시키는 방법도 과거 저장된 문서를 단순하게 복사하거나 출력해 나가는 수단이 아니라, 최첨단 IT기술 발달로 인해 그 유형과 행태도 다양해졌다. 따라서 국가의 핵심기술과 기업의 영업비밀을 침해하는 산업보안범죄에 대한 피해는 상당히 위협적이기 때문에 산업보안을 단순히 기술유출방지라는 시야가 아닌 산업과 관련된 모든 손실방지와 지적재산보호라는 넓은 범주에서 파악하는 것이 필요하다.

Industrial Security Crime's Realities and Counter-Measure

Seo, Bong Sung* · Lim,You Seok**

ABSTRACT

Modern society is to have an significant impact on the competitiveness of the country in which the economic value is very high occupancy and ensure a state-of-the-art science and technology. The country's core technology or industry security crimes going seized state-of-the-art technology firms can threat of damage to the country's economic security. In particular, the defense industry serious crime that is directly related to national security. The company's core technology and trade secrets leaked once the industrial countries must prevent security breaches and offenses of strict punishment measures because it is impossible to recover. Also, some advanced countries directly has been operating industrial security crime for the country's economy and national security. In recent years, Nation core technology infringement cases are rapidly increasing in the country. In addition, industrial security crime threat to national security. Therefore, the industry security crimes damage to the national security that infringe on the business secrets of core technologies and businesses. It is necessary to identify that industry security crime associated with the visibility of the broad scope of intellectual property protection.

Key words : Industrial Security, Economy Security, Trade Secret, National Core Technology, Scientific Technology

접수일(2015년 10월 1일), 수정일(1차: 2015년 10월 7일, 2차: 2015년 10월 15일), 게재확정일(2015년 10월 28일)

* 현대직업전문학교 경찰행정학과
** 동국대학교 사회과학연구원

1. 서 론

최근 국내의 최첨단 산업기술이 다양한 형태로 해외로 유출되는 사례가 발생하고 있다. 이는 경제안보 분야에 심각한 피해를 줄뿐만 아니라 국가안보와 직결되어 있는 중대한 범죄에 해당한다. 더욱이 산업보안 침해 범죄로 인한 최첨단 산업기술 유출은 적시에 필요한 인지와 대응이 이루어지지 않기 때문에 사후에 범죄에 대한 행위자를 처벌할 수 있을지는 몰라도 이미 유출된 첨단기술은 회수가 불가능하게 된다. 그래서 산업보안범죄는 사전예방이 더욱더 중요한 영역이다. 아울러 산업기밀에 대한 보호는 개별 기업을 넘어 국가산업 전체를 좌우하는 중대한 사안이므로 기업 단위의 대응은 물론 국가 차원의 다양한 대책을 마련할 필요가 있다.

이미 전 세계 굴지의 기업들이 전개하고 있는 무한 경쟁은 기술 및 경제적 가치가 매우 큰 국가의 핵심기술을 확보하는 것이 국가 경쟁력에 상당한 영향력을 미치는 시대에 접어들었다. 우리나라의 경우에도 정보통신기술(ICT) 분야나 자동차 등 특정 분야에서 소위 원천기술이라 할 수 있는 핵심기술을 보유하고 있기 때문에 더 이상 기술도입국이 아닌 기술수출국으로서의 위상을 떨치고 있다. 만약 국가의 핵심기술이 해외로 유출된다면 막대한 국부 손실과 함께 국가의 산업 경쟁력을 크게 하락시킬 수 있다는 점에서 핵심기술을 유지하고 확보하는 과정에서 국가와 기업 간의 상호협력적인 대책이 필요하다.[6]

지난해 발생한 산업보안 침해범죄의 적발 실적을 살펴보더라도 국가핵심기술은 2014년 63건으로 매년 증가하는 수치를 보였고, 암수범죄까지 추정한다면 재산적 피해 역시 천문학적인 금액을 나타내고 있으며, 산업보안 침해범죄가 급증하는 원인과 대책에 대해 심각하게 고민해야 할 수준에 이르렀다.

특히 오늘날 초국가적인 산업보안 침해범죄는 과거 냉전 종식 후 전 세계가 경제력과 기술력이 국가안보와 직결되어 있는 상황으로 바뀌었고, 지적재산권 보호시장과는 달리 산업보안 침해범죄에 대한 국제사회의 공조와 법적인 규제가 전무한 실정이다. 따라서 산업보안 침해범죄에 의한 추상적인 피해 리스크를 고려한다면 국내외 유관기관의 적극적인 정보공유와 공조 그리고 협력이 필요한 시점이다.

이 연구에서는 먼저 산업보안범죄와 관련된 국내외의 법적 논의 및 실태를 파악한 후 피해의 심각성에 대해 고찰해보고자 한다. 아울러 최근 빈번하게 발생하는 산업보안 범죄유형을 살펴보고, 국내외의 공조를 위한 효율적인 법과 제도에 대해 논의한 후 국내의 사정에 적절한 대책에 대해 제언하고자 한다.

2. 산업보안범죄의 법적 논의

2.1 국내의 산업기술보호 관련법

2.1.1 산업기술보호법

산업기술의 유출방지 및 보호에 관한 법률 제9조에 따라 국내·외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장 잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술을 국가핵심기술로 정의하고 있다.

국가핵심기술과 관련해서는 국가안보 및 국민경제에 미치는 파급효과, 관련 제품의 국내외 시장점유율, 해당분야의 연구동향 및 기술 확산과의 조화 등을 종합적으로 고려하고 있다. 이와 관련하여 전기·전자(11개), 자동차(8개), 철강(6개), 조선(7개), 원자력(4개), 정보통신(14개), 우주(2개), 생명공학(3개) 등을 국가에서 지정·관리함으로써[9] 국가안보 및 경제안보와 직결된 국가핵심기술에 대해서는 기업의 협력을 유도하여 집중적인 관리와 지원을 해주는 실정이다.

2.1.2 영업비밀법

부정경쟁방지 및 영업비밀보호에 관한 법률 제2조 제항에 의하면, 영업비밀이란 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것을 의미하며,

기업의 합리적인 노력에 의해 비밀로 유지된 생산 및 판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다. 최근 2014년 1월 31일 이후 영업비밀의 보유주체를 기업에서 영업비밀 보유자로 확대하여 시행하고 있으며, 부정한 이익을 얻거나 손해를 가할 목적이라는 위법성을 규정하고 있다. 아울러 영업비밀 침해행위를 국내외로 규정하고 엄격히 처벌하고 있다.[7]

한편, 영업비밀의 부정한 취득행위라 함은 영업비밀을 자신의 수중에 두는 행위를 의미하는데 영업비밀에 해당하는 정보를 입수 또는 확보하는 것으로서 비밀이 화체된 문서, 기타 매체 그 자체에 대한 점유의 취득뿐만 아니라 영업비밀을 기억하는 등의 방법으로 당해 정보를 확보하는 일체의 행위를 말한다.[1] 이러한 영업비밀에 대한 정보를 정당한 수단으로 취득하여 부정취득행위에 속하지 않는 요건으로는 1985년 미국 통일영업비밀법(UTSA) 제1조에서는 독립적으로 개발한 취득(discovery by independent invention), 역분석(reverse engineering), 영업비밀보유자의 허가를 얻은 취득, 공개 사용 또는 전시물에 대한 관찰을 통한 취득, 공개된 출판물을 통한 영업비밀의 취득행위를 들고 있다.[5]

또한 본 법에서는 영업비밀 침해유형을 제시하고 있는 바, 영업비밀을 부정 취득・사용・공개하는 행위, 부정취득된 영업비밀을 악의 또는 중과실로 취득・사용・공개하는 행위, 선의취득 후 악의 또는 중과실에 의한 사용・공개행위, 영업비밀을 부정공개 또는 사용하는 행위, 부정 공개된 영업비밀을 악의 또는 중과실로 취득・사용・공개하는 행위, 선의취득 후 악의 또는 중과실에 의해 사용・공개하는 행위로 구분하여 처벌하고 있다.

2.1.3 기타 관련법

산업보안 침해범죄에 대한 처벌은 영업비밀법, 산업기술법 이외에도 국가R&D보안관계법, 지식재산기본법, 중소기업기술보호지원에 관한 법률, 특허법, 상표법, 식물신품종보호법, 디자인보호법, 저작권법, 반도체 직접회로의 배치설계에 관한 법률, 군사기밀보호법, 공공기록물관리에 관한 법률, 대외무역법, 방위사업법, 형법 등 약 20개의 법에 의해 규제대상의 요건과 처벌을 규정하고 있다.

2.2 국외의 산업기술보호 관련법

2.2.1 미국

최근 미국의 경우 특허등록 된 옥수수 종자 절도사건에 대해 해외정보감시법(FISA)을 적용하였는바, 식품종자 산업스파이 사건에 대테러법을 적용할 만큼 경제안보와 산업스파이의 위험성을 경고하고 있다.[10] 미국은 판례법 국가임에도 불구하고, 영업비밀 보호에 관한 성문법도 상당히 발달해 있는 특징이 있다.[4] 일반적으로 산업스파이에 대해서는 영업비밀 침해 시 민사적 구제와 형사적 구제 가능하다. 민사적 구제는 통일영업비밀보호법(UTSA: Uniform Trade Secrets Act)을 근간으로 각 주(州)에서 제정한 영업비밀보호법에 의하고, 형사적 구제는 연방경제스파이법(Economic Espionage Act of 1996)에 의해 이루어지고 있다.

첫째, 통일영업비밀보호법(UTSA: Uniform Trade Secrets Act)은 1979년 영업비밀 보호에 관한 각 주의 판례법상 불균형 및 보호수준의 차이를 시정하기 위해 제정하였다. 오늘날 대부분의 주에서 이 법과 동일하거나 유사한 영업비밀법을 채택하여 운영하고 있으며, 이 법을 채택하지 않은 주는 주 법원의 판례법이나 주 형법상 영업비밀 절도죄, 일반 절도죄 등을 통해 영업비밀 보호에 법적 대응을 하고 있다. 또한 영업비밀 유출 피해 시 금지청구권과 손해배상청구권을 인정하고 있는데 특히, 징벌적 손해배상(Punitive Damages)을 채택하여 고의 또는 악의에 의한 침해행위는 손해배상액의 2배까지 청구 가능하도록 규정하고 있다.

둘째, 경제스파이법(Economic Espionage Act of 1996)은 산업스파이 행위를 연방차원의 형사범죄로 규정하여 연방정부의 수사 및 정보기관이 해당사건을 직접 수사할 수 있는 근거를 마련하기 위해 제정하였다. 이 법에 의하면 모든 산업스파이 침해 행위자는 고소

없이 형사처벌이 가능하며, 소송과정상 영업비밀의 기밀성 유지를 위한 법원명령 등이 가능하도록 규정되어 있다. 아울러 보호대상 및 요건 등과 관련하여 모든 형태의 재무・사업・과학기술・공학정보를 기업에게 경제적 가치가 있고 비밀보호 조치를 받고 있는 것으로 규정하여 형사처벌하고 있으며, 외국정부나 기관 등과 연계된 영업비밀의 유출행위에 대해서는 산업스파이죄로 가중 처벌하지만, 외국이 관여되지 않은 영업비밀 침해행위에 대해서는 영업비밀절도죄를 적용하고 있다.

한편, 2013년 1월 외국과 연계된 경제스파이범죄 대상을 최대 벌금으로 증액하여 처벌을 강화하는 내용의 경제스파이법 개정안(Foreign and Economic Espionage Penalty Enhancement Act of 2012, EEPE)이 만장일치로 상원을 통과하였다. 이 법에 의하면 개인에 대해 국외 산업스파이죄에 대해서는 15년 이하 징역 또는 500만불 벌금, 국내 영업비밀절도죄에 대해서는 10년이하 징역 또는 벌금에 처하도록 규정하고 있다.[2]

2.2.2 독일

독일은 산업스파이 처벌을 직접 규정한 단행법은 없으며, 영업비밀보호 차원에서 부정경쟁방지법(UWG: Gesetz gegen den unlauteren Wettbewerb)을 통해 규율하고 있다. 부정경쟁방지법은 1909년 제정된 이래 영업비밀보호와 관련하여 지속적으로 처벌의 확대 및 강화의 방향으로 법개정이 이루어져왔다.[7]

부정경쟁방지법(UWG)에 의하면, 친고죄를 원칙으로 하고 공공의 이익을 위해 필요하다고 인정되는 경우에만 피해자의 고소 없이 기소 가능하며, 미수범은 인정되지만, 예비・음모는 처벌할 수 없다. 또한 이법에 의하면, 영업비밀 침해 시 3년 이하 징역 또는 벌금 부과가 가능하며, 외국으로 유출 시 5년 이하의 징역에 처하도록 규정하고 있다.[7,8] 이와 같이 독일은 산업스파이에 대한 처벌은 기본적으로 기업의 영업비밀 보호차원에서 민사절차에 의해 해결하려고 하며, 예외적인 경우에만 형사범죄로 취급하는 국가와 기업 간의 협력 및 지원체계로 이루어져 있다.

2.2.3 일본

일본은 산업기술 유출방지를 위한 부정경쟁방지법을 개정하여 기업의 영업비밀을 누설 또는 교사・방조한 자도 정범으로 처벌하고, 공무원이 외국공관원 접촉할 경우 사전승인 및 사후보고를 하도록 시스템을 제도화하였다. 아울러 경제산업성 등 다양한 부처와 사안별로 기술유출방지지침 및 지식재산취득관리지침 등을 제정하여 의도하지 않은 기술유출에 대한 방지대책을 강화하고 있으며, 최근에는 특허의 경우도 국가안보와 관련된 내용은 공개하지 않는 방안을 추진하고 있다. 또한 산업스파이 활동을 하다 검거되면 부정경쟁방지법과 형법상 절도죄, 사기죄, 횡령죄, 장물죄, 배임죄 등 각종 재산죄와 비밀누설죄, 주거침입죄 등으로 처벌이 가능하며, 영업비밀 침해죄는 공소제기에 피해자 등의 고소를 필요로 하는 친고죄로 처벌이 가능하도록 규정하고 있다.[7,12]

먼저, 일본은 기업의 영업비밀 처벌과 관련해서는 대표적으로 부정경쟁방지법을 통해 보호하고 있으며, 영업비밀의 보호요건, 침해 행태, 민사적 구제수단 등에 내용은 우리 법과 유사 첨단기술 유출에 대한 심각성을 인지하고 한국, 미국, 독일 등 외국의 영업비밀보호 강화 추세에 흐름을 같이 하고 있다. 2005년 6월 부정경쟁방지법을 개정하여 2005년 11월부터 영업비밀 침해 범죄와 산업스파이에 대한 형사처벌을 강화하였고, 영업비밀 국외사용 및 공개행위 처벌, 퇴직자에 의한 영업비밀의 사용・공개행위 처벌, 법인도 처벌 가능하도록 규정하고 있다.

둘째, 경제산업성은 2003년 3월 해외에서 활동하는 기업들의 의도하지 않은 기술유출을 방지하기 위하여 기업이 실무적으로 활용할 수 있는 기술유출방지지침을 제정하였다. 이 지침의 주요내용으로는 의도하지 않은 기술 유출이 발생하는 주요 유형을 설명하고, 선진기업의 대응사례를 통해 기업이 참고할만한 기술유출 방지대책을 제시하고 있으며, 해외 진출 시 기술이전 전략, 사내 조직체제, 사업 활동, 사내 교육, 사후관

리 등 경영 전반적인 내용으로 구성되어 있다.

2.2.4 중국

중국의 영업비밀 규정은 중화인민공화국반부정당경쟁법에 영업비밀의 정의, 침해유형, 민사책임에 대하여 비교적 간단하게 규정하고 있고, 행정법규로는 영업비밀침해행위에 관한 규정이 있으며, 이 외에도 형법, 민법통칙, 계약법, 회사법, 노동법 등의 규정이 있다. 영업비밀과 관련해서는 공중(公衆)이 모르고 권리자에게 경제이익을 가져다주며 실용성을 구비하여 권리자가 비밀조치를 취한 기술정보와 경영정보를 규정하고 있다.

이 법은 중국에서의 기술유출과 영업비밀보호 등을 위해 1993년 9월 2일 제정하여 1993년 12월부터 시행함으로써 사회주의 시장경제의 건전한 발전과 공평한 경쟁을 보호하고, 부정경쟁행위를 제지하고 경영자와 소비자의 합법적 권익을 보호하기 위하여 제정하였다. 또한 이 법에서는 기술상・경영상의 정보를 보호하고 있으며, 상대방의 영업비밀을 침해한 자에 대해 손해배상책임 및 피침해자가 부정경쟁행위를 조사하기 위해 지불한 비용에 대한 배상책임을 부여하는 민사적 구제, 영업비밀 침해시 감독 조사기관의 위법행위 정지명령 및 사건 정황에 따라 20만 위안까지 벌금을 부과하는 행정적 구제, 영업비밀 권리자에게 중대한 손실을 초래한 경우 그 침해자에 대해 3년 이하의 징역이나 구금을 벌금과 병과하거나 혹은 벌금에 처할 수 있도록 형사적 구제를 규정하고 있다.[7]

3. 산업보안범죄의 실태 및 문제점

3.1 산업보안범죄의 실태

2010년에서 2014년 사이 국내에서 발생한 국가핵심기술의 분야별 유출현황을 살펴보면, 정밀기계 분야가 34건으로 가장 많이 차지하였고, 전기・전자 26건, 기타 16건, 정보통신 14건, 화학 7건, 생명공학 3건으로 나타났다. 이러한 기술유출 피해기업은 중소기업이 64%를 차지하였으며, 기타 대학이나 공공연구기관의 핵심기술이 20%, 대기업에서 16% 피해를 본 것으로 나타났다. 기술유출 사례를 보더라도 과거 바이오환경기술을 비롯하여 최근에는 반도체기술과 의약품까지 다양하게 나타났으며, 방위사업과 관련된 전략물자나 기술까지도 해외에 불법적으로 유출되는 사례가 매년 증가하는 것으로 나타나고 있다.[7]

2014년 한국산업기술보호협회 자료에 의하면, 산업기술유출 예상 피해액은 연평균 약 50조원으로 추정되고 있으며, 이는 2014년 국내총생산(GDP)의 3%에 해당하는 금액으로 나타났다. 또한 산업스파이의 주체는 전직 직원 52.8%, 현직 직원 27.1%, 기타 협력 및 투자업체에 의한 주체가 20.1%를 차지하였으며,[11] 대부분의 국가에서 국가핵심 산업기술이 유출되는 범죄가 기관의 내부 보안사정에 전문적인 지식을 가지고 있는 구성원에 의해 발생하기 때문에 산업기술이 유출되는 경위와 대상 그리고 피해규모를 파악하는 것조차 어려운 실정에 이르렀다.

3.2 산업보안범죄의 문제점

3.2.1 보안의 취약성에 의한 불법적 기술유출

오늘날 기업의 핵심적인 산업기술을 유출시키는 방법은 과거에 저장된 문서를 단순하게 복사하거나 출력해 나가는 것이 아니라 최첨단 정보통신기술(ICT)의 발달로 인해 그 유형과 행태도 다양해졌다.

최근 발생하는 산업기술 유출사건의 특징을 살펴보면, 범죄수법이 최첨단 기술을 통해 지능화되어져 있는 점을 알 수가 있다. 각종 해킹이나 스마트폰 촬영 및 외장하드 등 대용량 저장장치 활용, 사내 보안시스템 우회 유출을 통한 첨단기술 유출사건이 빈번하게 나타나고 있다. 특히 우리 기업이 세계시장에서 점유하고 있는 특정분야의 기술과 지적재산권에 대한 침해가 심각하여 이러한 상품의 위조품이 해외에서 대량생산되어 판매되고, 정품 부품의 불법유출 및 제3국에서의 조립되며, 모조품의 현지 생산과 같이 지식재산 침해가 이루어지고 있다. 나아가 군용 전략물자의 우회

적 불법수출, 전·현직 군인과 해외 방위산업체와 연계된 군사기밀이 유출되는 경우에는 심각한 국가안보 문제하고 직결되어 있다.[7]

특히, 과거와는 달리 오늘날 산업기술이 유출되는 기업은 대기업이 아닌 중소기업에서 이루어지고 있다. 대부분의 중소기업은 보안과 관련된 예산과 비용이 대기업에 비해 상대적으로 저조할 수밖에 없는 보안시스템을 갖추고 있기 때문이다. 따라서 산업기술이 유출된 경로와 피해에 대한 정확한 인지와 대응조차 할 수 없는 실정에 놓여있다.

3.2.2 합법적 기업인수·합병에 의한 침해

기업에서 발생하는 산업보안범죄의 대표적인 유형은 합법적으로 기업을 인수 또는 합병하는 과정에서 기술을 유출하는 것이 심각하다. 대표적으로 기업이 적대적 M&A를 통해 합법적으로 기술을 유출하는 유형이 있다. 적대적 M&A는 상대기업의 동의 없이 강행하는 기업의 인수와 합병을 뜻하고, 통상 공개매수(Take Over Bid)나 위임장 대결(Proxy Fight)의 형태로 나타난다.

공개매수(Take Over Bid)의 방법은 단기간에 의도한 가격으로 대량의 주식을 공시해 매집하는 것이다. 인수대상 기업도 적극적으로 맞대응하게 되므로 이 과정에서 주가가 상승하면 시세차익을 노려 공개매수가 발생하게 되고, 주식을 매집한 후 대주주를 직간접적으로 협박하며, 이미 매집한 주식을 비싼 값에 되파는 그린메일(Green mail)의 방식을 이용하기도 한다. 이와는 달리 위임장 대결(Proxy Fight)의 방법은 주주총회에서 의결권을 보유하고 있는 위임장을 상대적으로 많이 확보하여 현재 이사진이나 경영진을 교체하는 방법이다.

결국 기업을 합법적으로 인수·합병하는 경영행위 과정에서 기업이 보유한 핵심적인 기술이 암묵적으로 유출되는 경우가 많다. 그렇다고 해서 산업기밀과 관련된 사안에서 당사자가 아닌 국가 또는 제3의 유관기관이 기업의 적법한 경영행위에 적극적으로 개입할 수 없는 한계가 있다.

3.2.3 피해자의 엄격한 손해입증

최근 발생하는 산업보안 침해범죄의 징후를 보면, 타 회사에서 유사제품 생산, 거래선 교체, 제품 A/S 이유 등의 소스코드 요구, 생산제품 주문량 또는 매출액 급감, 공동연구 및 합작투자 등 의향서만 체결 후 본 계약 지연 등의 고도로 지능화 되어 있기 때문에 실제 피해에 대한 인식도 부족할 수밖에 없다.

이러한 행위자에 대해서도 실제 사법부에서는 범죄피해자가 영업상 비밀을 입증해야 하고, 회사가 영업비밀유지를 위해 상당한 노력을 했는지 여부, 실제 손해입증에 대한 인과관계 확정 등을 엄격하게 요구하고 있는바, 실제 피해내용과 규모의 추상성을 구체적으로 입증하기에는 실무적인 어려움이 산재해있다.

3.2.4 범죄의 수준과 처벌의 불균형

대부분의 산업보안 침해범죄자는 관련 조직의 전·현직 구성원이면서 초범자들이 대다수이다. 이러한 경우 범죄에 대한 개전의 정이 현저하거나 생계형 범죄자들은 보통 집행유예나 벌금으로 경미하게 처벌받기 때문에 기술유출이 끊이지 않는 것이다. 이에 범죄자들 역시 범죄를 통해 얻을 수 있는 경제적 이익에 비해 상대적으로 경미한 수준의 처벌은 합리적으로 선택(rational choice)선택하여 범죄로 나아가는 경우가 많다. 그러므로 법과 제도를 통한 보다 강력한 처벌과 사후관리가 필요하다.

3.2.5 유관기관의 공조체제 미비

국가의 핵심적인 산업기술은 국가경제력을 비롯하여 국가안보하고도 직결되어 있기 때문에 각별한 관심과 주의가 필요하다. 오늘날 전 세계에서 동시에 발생하는 산업보안 전쟁은 미국을 비롯하여, 독일, 중국, 대만, 러시아 등 시간과 장소를 초월하여 다양하게 발생한다.

특정 국가의 경제안보가 마비되면, 전 세계의 경제흐름상 예측할 수 없는 피해를 가져올 수가 있고, 상대적으로 경제안보가 취약한 국가에서는 국가부도까지

도 발생할 수 있다는 점을 고려해야 한다. 그럼에도 불구하고 범죄피해산정의 추상성이라는 특징 때문에 구체적인 공조체제를 마련하기에 한계가 있다.

4. 산업보안범죄의 대응방안

4.1 기업의 전문적인 보안체제 마련

중소기업은 대기업보다 보안 수준이 낮고 인력관리가 전반적으로 저조하기 때문에 영업비밀과 관련된 산업기술 유출이 심각하고, 피해에 대한 인지 조차도 못하는 경우가 대다수이기 때문에 국가와 기업 간의 협력적인 관계를 통해 산업보안범죄에 대한 사전적 예방활동을 전개해 나가야 한다. 따라서 상대적으로 보안수준이 취약한 중소기업의 경우에는 산업기술유출 대비를 위한 보안과 예방시설이 미비하고 예산도 저렴하기 때문에 중앙정부 차원에서 관리・지원・보호해줘야 할 필요성이 있다.

결국 기업의 보안수준은 보안시스템 설계 예산과 직결되지만, 산업보안범죄 침해로 인해 잃게 되는 손해와 경제적 비용을 적극 고려한다면, 전문적인 보안시스템을 마련하여 산업보안범죄를 사전에 예방하는 비용은 상당히 지엽적인 예산에 불과하다는 인식의 전환도 필요하다.

4.2 기업의 인수・합병에 대한 다자적 대응

기업의 적대적 M&A에 대항하기 위한 방어책은 재무전략이나 회사정관을 이용하여 인수자의 매수자금에 부담을 주는 방법 등 다양한 전략이 가능하다. 그렇기 때문에 기업은 단순히 영업비밀이나 유・무형의 재산을 보호한다는 인식을 넘어 경제안보를 고려하여 적극적인 대응을 위해서라도 유관기관의 협조를 통해 국가의 핵심적인 산업기술을 지켜내야 하는 인식을 공유해야만 한다.

일례로써 2014년 10월 31일 개정된 부정경쟁방지 및 영업비밀보호에 관한 법률상의 영업비밀 원본증명제도는 산업보안 침해범죄를 제재하기 위한 긍정적인 요인으로 평가된다. 원본증명제도를 통해 영업비밀 원본증명기관은 등록된 전자지문과 영업비밀 보유자가 보관하고 있는 전자문서로부터 추출된 전자지문이 같은 경우 그 전자문서가 전자지문으로 등록된 원본임을 증명하는 원본증명서를 발급할 수가 있다. 여기에 국가의 핵심기술과 관련된 기업의 영업비밀 보호는 유관기관의 협력과 지원을 통해 경제안보를 지켜내야 한다.

4.3 피해규모의 입증요건 완화

산업보안 침해로 인한 피해규모의 추상성에도 불구하고, 대법원에서는 기업의 주요 기술에 대해 평소 회사에서 철저하게 비밀로 관리하고, 직원들로부터 보안서약 각서 등을 받는 노력이 있을 때만 기술유출을 인정하고 있다. 이에 산업보안 침해범죄의 입증은 침해한 자가 가장 정확하게 인지하고 있고, 비교적 보안인식이 부족한 피해자들은 추상적인 피해규모를 입증하기에는 어려움이 있을 수밖에 없다.

따라서 사법부는 상대적으로 불리한 산업보안 범죄 피해자의 추상적인 정황과 자료를 재판과정에서 최대한 활용하고, 피해자의 입증요건을 가해자보다 상대적으로 완화하여 산업보안범죄에 대한 실체적인 진실을 밝혀내야 한다. 산업보안을 침해하는 범죄는 일반적인 형사범죄 즉, 재산범죄와는 죄질이 근본적으로 차이가 나기 때문이다.

4.4 산업보안범죄의 수준과 처벌의 균형

국내에서는 일반적인 경제사범에 대한 처벌은 비교적 관대한 편이다. 그러나 국가핵심기술과 관련된 산업보안범죄는 국가의 경제안보와 국가안보와도 연결되기 때문에 범죄수준에서도 질적인 차이가 있다.

미국은 해외정보감시법, 통일영업비밀보호법, 경제스파이법, 독일은 부정경쟁방지법, 일본은 부정경쟁방지법 및 기술유출방지지침, 중국은 중화인민공화국반부정당경쟁법에서 산업보안범죄와 일반적인 영업비밀 유출에 대한 범죄를 차등하여 처벌하고 있다.

국내에서도 산업보안범죄 처벌과 관련된 다양한 법률이 있지만, 국가핵심기술과 관련된 산업보안범죄에 조금 더 집중할 필요성이 있다. 최근 영업비밀법이 개정된 바, 종전에 한정적으로 열거된 부정경쟁행위에 보충적 일반조항을 신설·도입해 새로운 유형의 부정경쟁행위에 대한 규제 범위를 확대했다. 개정된 규정으로 인해 영업비밀의 침해에 대해 손해배상뿐만 아니라 금지청구까지 가능해졌다는 점에서 보충적 일반조항은 긍정적으로 작용할 것이라고 해석된다.

그러나 보충적 일반조항은 타인의 상당한 투자나 노력으로 만들어진 성과 등을 공정한 상거래관행이나 경쟁질서에 반하는 방법으로 자신의 영업을 위해 무단으로 사용 또는 타인의 경제적 이익을 침해하는 행위를 제한할 수도 있다. 따라서 구체적인 거래관행이나 경쟁질서의 유형과 기준을 동시에 마련하는 것이 부정경쟁행위에 대한 인식을 각인시켜 줄 수 있다.

4.5 국제사회의 공조체제 확립

산업보안범죄에 대한 국제사회의 통제는 국가들마다 경제안보상황이 다르기 때문에 공통되는 제재시스템은 상당히 미비한 실정이다. 그럼에도 불구하고 산업보안범죄의 수준을 고려한다면, 국내 유관기관과의 초국가적인 공조와 협조를 통해 사전예방과 사후 재발방지가 필요하다. 이에 국내 기업과 유관기관은 국제사회에서 공유할 수 있는 산업보안범죄에 대한 제재와 초국가적인 공조체제를 구축하여 경제안보와 국가안보를 확립하여야 한다.

5. 결론 및 제언

우리나라의 경쟁력 있는 국가핵심기술과 기업의 영업비밀을 침해하는 산업보안범죄는 경제안보 및 국가안보와 직결될 수도 있기 때문에 국익 수호를 위해서라도 기업 스스로의 사전예방과 사후 적극적인 대책이 필요하다. 아울러 국가의 핵심기술과 관련되어 있는 경우에는 기업의 자체적인 산업보안 범죄예방과 유관기관의 협력을 통해 추상적으로 위험한 산업보안 침해범죄를 예방해야만 한다.

국가의 핵심적인 과학기술을 탈취하는 산업보안 침해범죄의 피해에 대한 경제적인 가치는 천문학적 액수에 달하고 궁극적으로 국가경쟁력을 약화시킨다는 점에서 산업보안의 중요성은 아무리 강조해도 지나치지 않다. 또한 산업보안을 단순히 기술유출방지라는 좁은 틀에 국한하지 말고 산업과 관련된 모든 손실방지와 지적재산보호라는 넓은 범주에서 파악하는 것이 필요하다.[3]

따라서 산업보안침해범죄는 단순히 지적재산이 침해당한 절도사건이 아니라 경제안보를 침해하는 범죄에서 나아가 국가안보를 위해서라도 선택과 집중을 통한 예방과 재발방지에 노력해야만 한다.

참고문헌

[1] 김정덕·김성화, “영업비밀보호법의 이해”, 한국학술정보(주), 2011,
[2] 박강우. “산업스파이범죄의 실태와 법적 규제의 문제점”. 형사정책연구. 23권 3호. 2012.
[3] 이창무. “산업보안의 개념적 정의에 관한 고찰”. 산업보안연구학회지 제2권 제1호, 2011.
[4] 정진근. “주요 판례법 국가의 영업비밀 보호와 시사점”. 강원대학교 비교법학연구소. 강원법학 제39권. 2013.
[5] 한국특허기술원, “부정경쟁방지 및 영업비밀보호에 관한 업무편람”, 진한엠앤비, 2010.
[6] 홍영서. “국가핵심기술 보호제도의 문제점 및 개선방안에 관한 고찰”. 산업재산권 제43호. 2014.
[7] 국가정보원 산업기밀보호센터 자료.
[8] 독일 연방법무부 자료.
[9] 산업통상자원부 고시 제2013-120호
[10] 한국경제신문 2015.04.29.
[11] 한국산업기술보호협회 자료 2014.
[12] 일본 전자정부 자료.

[저 자 소 개]

서 봉 성 (Bong-sung Seo)

2006년 2월 학사
2012년 2월 석사
2015년 9월 박사수료

email : sbs502@hanmail.net

임 유 석 (You-seok Lim)

2005년 2월 학사
2007년 2월 석사
2013년 2월 박사

email : camus200@naver.com