한국경호경비학회 – 제38호(2014): 57–82
투고일 2014. 01. 29, 심사일 2014. 02. 18, 게재확정일 2014. 03. 03

# 독일의 산업보안 정책과 시사점

이 성 용

# 독일의 산업보안 정책과 시사점*

이 성 용**


## 〈요 약〉

본 연구에서는 국내 산업기술보호 제도와 정책의 발전을 위한 기초자료로서 독일의 산업보호제도를 살펴보고 시사점을 찾아보았다. 독일은 고도로 발달된 경제와 산업기술로 인해 이미 오래전부터 산업스파이 활동의 주요 무대가 되었으며 따라서 산업기술보호에 대한 지대한 관심을 가져왔다. 특히 국가의 개입이 요구될 뿐만 아니라 적극적인 선제적 역할이 강조되는 경제스파이(Wirtschaftsspionage)분야와 일반 산업스파이(Industrie-spionage) 분야를 구분하여 전자의 경우 국가기관의 활동의 주된 영역으로서 정부차원의 대응이 두드러지는 반면 후자에 있어서는 상공회의소를 중심으로 하는 민간조직 차원의 활동이 주를 이루고 있다. 경제스파이에 미치지 못하는 경쟁스파이 행위라 할지라도, 당연히 부정경쟁방지법상의 범죄행위에 해당하게 되고, 이 경우 형사사법기관인 경찰에 의한 수사와 처벌이라는 법집행은 진행될 것이나, 우리나라와는 달리 독일의 부정경쟁방지법은 이러한 산업스파이 행위를 특별한 공공의 이익이 존재하지 않는 한, 친고죄로 보아 형사사법기관의 개입을 제한하고 있다. 민관협력은 기실 대등한 당사자를 전제로 하는 것이다. 산업보안의 영역에서 민간이 대등한 당사자로서 국가와 협력하고 이른바 협조적 법치국가로 발전하기 위해서는 독일에서 보듯이 국가의 영역과 민간의 영역을 원칙적으로 구분한 이후에 민간차원에서 주도적으로 산업보안을 위한 이익집단을 구성하고 국가와 협력하는 방식으로 나아가야 한다. 또한 자국의 이익 확대라는 이름으로 정보기관이 외국의 산업기술에 대한 적극적 수집을 하는 것이 어디까지 허용될 수 있을지를 국가윤리의 차원에서 고민해야 한다.


**주제어 : 산업보안, 경제스파이, 경쟁스파이, 민관협력, 국가윤리**

* 이 논문은 2013.6.28. 한국경호경비학회 상반기 정기세미나에서 발표한 글을 수정·보완한 것임
** 계명대학교 경찰행정학과 교수(주저자)

목 차



# Ⅰ. 서 론

타인이나 특정기관의 기밀을 탐지하는 활동은 테러집단이나 적국의 비밀정보기관에 의해서 오래전부터 시도되었다. 세계의 모든 국가들은 자국의 중요한 정보유출을 방지하기 위해서 방첩기관들을 설치하고 정보방어활동을 하고 있다. 그러나 동서지역의 냉전이 종식되고 정치적 대립이 약화됨에 따라 이러한 정보탐지의 주된 관심은 경제분야로 이동하게 되었고 그 대상도 종전의 국가기관에서 주요 산업기술을 보유하고 있는 사기업으로 변화되고 있다.

산업활동에서 중요한 회사기밀들이 유출되는 것은 해당기업의 경제적 손실뿐만 아니라 국부의 유출로도 연결된다. 그럼에도 이러한 산업보안의 유출이 발생하는 경우 가해자 측은 물론이거니와 피해기업 측에서도 기업이미지 추락 등을 우려해 피해사실과 공식적인 대응을 피하려는 속성이 있어 문제의 심각성은 외부로 좀처럼 표출되기 어렵다(신성균, 박상진, 2009:

산업보안의 문제는 오랜 역사를 가지고 있다고 알려진다. 5세기에서 6세기 중국에서는 비단생산의 기밀을 자국에서만 보유하고 독점생산을 계속하고 있었으나 산업스파이 활동으로 인해 이러한 생산기밀이 유럽으로 유출되었고, 이로 인해 당시 중국경제는 심각한 타격을 입게 되었다(Meissinger, 2005). 산업보안의 심각성을 인식한

우리나라에서도 2007년 4월 '산업기술유출방지 및 보호에 관한 법률'을 제정•시행하고 있고, 동법 제16조에 따라 산업기술의 유출방지 및 보호에 관한 시책을 효율적으로 추진하기 위하여 산업통상자원부장관의 인가를 받아 산업기술보호협회를 설립하여 운영하고 있다.

산업기술보호의 문제는 비단 우리나라의 문제만이 아니라 범세계적인 문제이고, 특히 산업기술이 발전한 국가일수록 그 심각성도 비례할 수밖에 없다. 미국의 경우는 민간시큐리티 전문기관인 미국 보안산업협회(ASIS: American Society of Industrial Security)가 보안산업 분야의 대표적 단체로서 자리매김하고 있으며, 관련한 많은 선행연구가 국내에서 진행되었다(최진혁, 2010: 최선태, 유형창, 2010). 한편 세계경제의 또 다른 축을 형성하고 있는 유로시장에 있어서 가장 큰 경제력을 보유하고 있는 독일의 경우는 산업보안에 관한 기본적 법령만이 우리나라에 소개되었을 뿐(하헌주, 2005: 이정덕, 한형구, 2007), 그 시스템에 관한 체계적인 연구가 아직 진행되지 못하였다.

산업기술보호는 특정 국가에 제한된 문제가 아니라 타 국가와 밀접한 관련을 맺고 있으므로 관련 국가들의 기본정책이나 해당 정부조직과 그 활동에 관한 충분한 이해가 필요하다. 이에 본 연구에서는 국내 산업기술보호 제도와 정책의 발전을 위한 기초자료로서 독일의 산업보호제도를 살펴보고 시사점을 찾아보고자 한다.

## Ⅱ. 산업기술정보의 이론적 고찰

### 1. 산업기술보호의 국가관리 필요성 확대

냉전이 종식된 지 수 십년이 지났지만, 아직도 독일은 각 국의 정보기관의 주요한 활동대상이 되고 있다. 다만 그 활동대상이 정치적 정보활동이 아닌 경제적 정보활동으로 바뀌었을 따름이다. 독일통일이후 증대된 정치적 위상과 높은 학문수준과 첨단기술연구의 메카로서 독일은 경제, 지식·기술 정보전의 주요 무대로 등장했다. 외국의 정보기관뿐만 아니라 경쟁적 위치에 있는 각국의 기업들 또한 독일경제의 기술정보(know-how)를 빼내기 위해 혈안이 되었으며 이를 목적으로 독일 국내법인 부정경쟁방지법(UWG)의 규정을 일탈하는 범죄행위들이 발생하고 있다. 독일은 전 세계

신기술 특허시장에서 미국, 일본에 이어 3위를 차지하고 있으며 유럽국가 중 부동의 1위를 고수하고 있는 국가이기 때문이다.[1)]

독일의 대표적 국내정보기관인 연방헌법보호청(BfV)에 따르면 각국의 정보기관들이 자국의 경제발전을 위하여 독일의 첨단 산업정보들을 탐지하고 있는데, 그 중에서도 특히 중국과 러시아의 정보기관들을 대표적으로 열거하고 있다.[2)] 중국의 경우 국가안보성(MSS), 군보안성(MID), 전자첩보성(3VBA)의 3개 정보기관의 직원들이 독일산업정보 유출에 주력하고 있으며, 러시아의 경우 SWR, GRU, FSB의 3대 정보기관의 직원들에게 러시아 경제를 위한 산업기밀탐지를 법적인 의무로 부과하고 있다.[3)] 미국, 영국, 프랑스 등의 서방국가들의 산업기밀 탐지활동 여부와 관련 언론 등을 통한 문제제기가 있기는 하지만, 독일 연방헌법보호청은 아직 자국에 대한 조직적인 산업스파이활동이 존재한다는 사실은 부인하고 있다. 다만 모든 가능성을 열어두고 방첩활동을 하고 있을 따름이다.

산업기밀유출의 유형은 행위국의 산업기술수준에 따라 크게 두 가지 유형으로 구분될 수 있다. 우선 미국, 프랑스, 영국 등과 같이 기술수준이 고도로 발달한 국가들은 주로 정보수집 부분에 집중적인 관심을 가지고 있는 바, 기업전략이나 기업의 협력 및 입찰이나 정책결정의 내정사항 등에 관한 것들이 주된 내용이 된다. 일반적으로 위에 언급한 국가들은 독일에 상응하는 기술수준(Know-how)을 보유하고 있으나 시장전략에서 보다 유리한 위치를 점하기 위함이다. 대표적인 사례가 우리나라에서 구매했던 고속열차에 관한 것으로 당시 프랑스의 정보기관이 경쟁 대상이었던

1) "특허 출원 건수에 따른 주요 국가들의 순위는 미국이 4만4천855건으로 1위를 고수한 가운데 일본(3만2천156건), 독일(1만7천171건), 중국(1만2천337건)이 뒤를 이었다. 우리나라는 9천686건으로 5위를 차지해 프랑스와 영국에 앞섰다." 연합뉴스 2011.2.10.

2) 마찬가지로 미국의 경우도 중국과 러시아의 정보활동에 대해 동일한 비판을 공개적으로 하고 있다. "미국 정보 당국이 중국 정부를 '가장 위험한 사이버 공격자'로 지목했다. 다른 나라의 스파이 활동을 감시하는 미 방첩(防諜) 집행관실은 3일 의회에 제출한 보고서 '외국의 첩보원들이 사이버 공간에서 미국 경제 기밀을 훔친다.'에서 "중국은 정부 차원의 사이버 공격으로 미국 경제에 결정적 영향을 끼치는 많은 정보를 수년 동안 빼갔다"고 했다. AP는 미 정부가 중국 정부를 사이버 범죄의 주범이라고 구체적으로 지목해 비난한 것은 이번이 처음이라고 보도했다. 2년마다 한 번씩 발행되는 '방첩보고서'는 미 정부 산하 14개 정보 관련 기관이 수집한 자료를 중심으로 만들어진다. 보고서에 사이버 스파이 수행국으로 언급된 나라는 중국과 러시아 두 곳뿐이었다. 러시아에 대해서는 "1위(중국)와 격차가 큰 2위"라면서도 "모스크바의 정보 당국은 사이버 공격 등 다양한 방법을 통해 미국의 경제 관련 정보와 기술을 빼내고 있다"고 전했다. 조선일보 인터넷판, 2011.11.05, http://news.chosun.com/site/data/html_dir/2011/11/05/2011110500107.html.

3) http://www.verfassungsschutz.de/de/publikationen/spionageabwehr_geheimschutz/broschuere_4_0806_wirtschaftsspionage/

독일의 지멘스사의 공급계약에 관련한 정보를 입수하여 결국 독일이 아닌 프랑스 방식의 고속열차가 선정된 것으로 알려져 있다(Nathusius, 2001).

한편 산업기술면에서 독일보다 우위에 있지 못한 중국이나 러시아는 또 다른 동기와 목적에서 산업스파이 활동에 관여하게 된다. 이들 국가의 주된 관심은 자국이 아직 보유하고 있지 않거나 산업화할 수 없는 단계의 산업기술을 탐지하여, 독일 기업의 라이선스 수익을 침해하거나 독일에서 고비용으로 생산되는 기술집약적 제품을 보다 생산비가 저렴한 국가에서 가격경쟁력을 갖춘 자국제품으로 생산토록 하는 것이다. 일반적으로 이러한 국가들은 자국기업에 이익을 가져올 수 있는 산업적으로 중요한 정보에 관하여 무차별적으로 탐지하고자 시도한다. 중국, 러시아뿐만 아니라 북한도 여기에 해당하는 대표적인 국가이다(Meissinger, 2005).

## 2. 산업스파이의 유형

독일에서는 산업유출과 관련하여 일반적으로 '경제스파이(Wirtschafts- spionage)'와 '산업스파이(Industriespionage)'를 구분하고 있다. 전자는 국가정보기관의 개입을 정당화시키는 사안으로서 '국가에 의해서 조정되고 지원되는 외국 정보기관이 관여하는 기업이나 영업에 대한 탐지행위'로 정의할 수 있다. 반면 산업스파이는 경쟁스파이(Konkurrenzspionage, Wettbewerbsspionage)라고도 불리는데, '특정 사기업에 의한 다른 기업에 대한 탐지행위'로 정의할 수 있다. 경제스파이나 산업스파이는 그 탐지방식에 있어서 큰 차이가 있는 것은 아니지만 그 위험의 방지에 관한 영역에 있어서 국가가 적극적으로 개입하고 대처할 것인가(전자의 경우), 아니면 사경제의 영역으로서 사기업의 위험방지 활동이 우선적으로 수행되고, 형사범죄에 해당하는 경우에 국가의 개입이 소극적으로 사후에 진행되는 시스템인가에 따라 구분될 수 있겠다.

이외에도 일반적인 경제스파이와는 구분되는 개념으로서, 기술정보 스파이활동의 대상인 대량살상무기의 확산(Proliferation)이 문제된다. 고도로 발달된 산업기술로 인해 독일은 핵무기를 비롯하여, 대량살상무기에 관한 정보기관들의 정보수집활동의 주요 무대가 되고 있다. 그러나 본 연구는 민간산업보다는 정부의 주된 관심이 되는 대량살상무기 관련 산업기술정보나 군수산업기술정보의 문제는 논의에서 제외하기로 한다.

## 3. 유출방식에 따른 구분

기업에 있어서 정보와 지식은 존속과 번영의 중요한 요소가 된다. 그 다양한 형태를 고려할 때 지식은 크게 외표적 지식과 내재적 지식으로 구분할 수 있다. 전자는 문자나 언어 또는 임의적인 형태로 전달이 가능하고 파악할 수 있다. 또한 물질의 형태로 이동도 가능하다(Lack, 2004).

이러한 지식은 최근 증가하고 있는 컴퓨터의 발전을 통해서 기존의 종이매체에 의한 전달로부터 탈피되고 있다. 더군다나 USB와 같은 간편한 매체를 통해 대량의 정보이동이 가능하게 되었다. 따라서 외표적 지식의 탐지를 위해 종전처럼 방대한 분량의 서류를 복사하거나 빼내오는 것은 더 이상 의미가 없게 되었다.

한편 내재적 지식은 외표적 지식이 창조적이고 지적인 행위나 현장의 경험을 통해 체화되는 것으로 특정한 사무를 해결함에 있어서 적합하다. 정리자면 외표적 지식은 생산품서류, 방식설명서 등과 같이 저장된 지식을 말하는 반면, 내재적 지식은 기업 구성원의 기억 속에 존재하거나 본래의 형태로 저장될 수 없는 지식을 의미한다.

산업기술의 유출과 관련, 일반적으로는 타 회사의 외표적 지식이 탐지의 대상이 된다. 내재적 지식은 단지 이러한 지식이 체화되어 있는 해당기업 구성원의 조력을 통하거나 직원의 위장투입 또는 경쟁업체에서 직원의 스카우트 등을 통해서만 가능하다.

### 1) HUMINT (Human Source Intelligence)

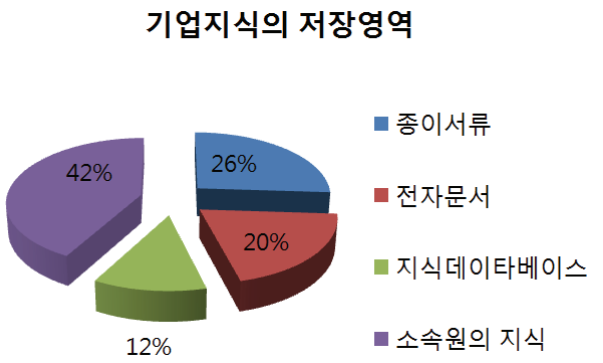
'휴먼(human)'과 '인텔리전스(intelligence)'의 합성어로서 우리말로는 '인적 정보(人的情報)' 또는 '대인 정보(對人情報)'로 번역할 수 있다. 대인(對人) 접촉, 곧 정보원이나 내부 협조자 등 인적 네트워크를 활용하여 얻은 정보를 말하며, 스파이를 활용하는 정보활동이 휴민트의 전형이라고 할 수 있다(한희원, 2011).

기술이 고도화되고 있는 현대사회에서도 인간은 여전히 경쟁상대로부터 정보를 획득하는 가장 중요한 방식이 된다. 물론 인간은 획득한 정보의 저장과정 등에서 기술적 보조물을 통해 지원되지만, 그 활동의 중심에 인간이 기능하게 되면 휴민트로 분류될 수 있다. 휴민트를 통한 정보유출방식은 소속원들의 내재적 지식을 탐지하거나 경쟁사로부터 소속원이 접근 가능한 외표적 정보들을 빼내오는 방식이다. 휴민트를 통한 산업기술유출에서는 자사직원들을 불법적으로 은밀하게 타사에 잠입토록 하

여 정보를 탐지하는 방식이 보편적이나, 산업시설의 시찰이나 개방행사를 통해 합법적인 접근도 가능하다. 산업기술정보취득을 위해 경쟁사의 산업시설에 무단 침입하여 기술을 절취하는 방식도 있겠으나 이 경우는 휴민트에 해당한다고 보기는 어렵다. 왜냐하면 휴민트의 경우는 대체로 비노출 방식에 의한 스파이행위로서 피해자가 인식하지 못하거나 상당한 시간이 경과된 후 인식하는 유형을 의미하기 때문이다.

기업의 외표적 지식보다는 휴민트 형식의 정보가 산업기술유출에서 큰 비중을 차지한다. 기업의 소속원들은 내재적 지식을 그 머릿속에 저장하고 있는 산업기술의 저장소가 되기 때문이다. 최근의 산업사회에서 지식사회로의 전환은 산업기술로서의 휴민트의 비중을 더욱 크게 강화하고 있다. 표면적인 정보를 넘어서는 산업기술의 주요 부분은 관련된 인적자원의 지원을 통해서만 취득이 가능해지고 있다.

### 2) TECHINT(Technical Intelligence)




출처: Schildbauer, Braun & Schultze, 2003.

〈그림 1〉

산업기술 정보탐지에 있어서 휴민트 다음으로 중요한 정보의 형태는 기술정보를 의미하는 테킨트로서 기술적 수단을 투입하여 실행되는 모든 스파이행위가 해당된다. 기술의 발달에 따라 경제스파이 분야에서도 테킨트의 비중은 점차 커지고 있으며 앞으로도 더욱 확대될 것으로 전망된다. 특히 외국과 관련한 정보기관요원은 국가적 예산지원과 기술지원을 통해 산업기술 정보취득에 충분한 테킨트를 활용할 수 있다(Lux & Peske, 2002). 최근에는 관련 장비의 구입경로나 가격의 하락으로 인해 경쟁기업이나 사정보업체의 경우도 이러한 기술활용이 어렵지 않은 상황이다.

테킨트의 취득을 위해서는 목표기업에 접근하는 것이 가장 문제되므로 실질적인 테킨트의 취득에 있어서는 휴민트를 통한 지원을 필요로 한다. 예를 들어 도청을 위해서는 도청장비를 도청지점까지 은밀히 설치하는 휴민트의 활동이 필수적이다. 테킨트는 다시금 첨단장비를 사용하여 신호를 포착하는 시진트(SIGINT: signal intelligence)[4]와 항공기나 위성에 의한 화상정보를 수집하는 이민트(IMINT: Imagery Intelligence), 계측기기를 이용하여 신호가 아닌 방사선, 적외선, 열 등을 측정하여 수집하는 정보인 매신트(MASINT : Measurement and signature intelligence) 등으로 구분된다.

미국이 뉴질랜드, 영국, 캐나다, 호주와 협력을 맺고 통신감청용으로 사용하고 있는 에셜론(Echelon)이 대표적인 사례이다. 이를 규명하기 위해 2000년 유럽의회에서는 비상설 조사위원회를 구성하고 2004년 보고서를 통해 전 세계의 모든 위성통신의 감청이 가능하다고 확인한 바 있다(Schmid, 2004). 동 시스템을 활용하여 특히 국제무대에서 활동하고 있는 기업들이 위성을 통한 의사결정이나 화상회의가 진행되는 경우 포착이 가능해 진다. 또한 위원회의 결과보고서에서는 이 시스템이 사경제영역에서의 통신감청에 사용되고 있음을 확인한 바 있다.

### 3) COMPINT (Computer Intelligence)

컴핀트의 목적은 컴퓨터망에서 데이터와 정보를 탐지하는 것이다. 자사의 직원을 대상기업에 투입하거나 외부에서 전산망에 접근하는 방식 또는 전자기기를 통한 전송을 탐지하는 방식 등이 사용된다. 따라서 컴핀트에서는 휴민트와 테킨트의 방식이 결합되어 활용되고 기존의 이분법적 분류방식에 위치시키기 어려워진다. 이러한 연유에서 휴민트 및 테킨트와 구분되는 컴핀트를 새로운 정보획득의 유형으로 분류하고 있다(Meissinger, 2005). 최근 컴퓨터 사용이 경제부문에서 필수불가결한 요소로 자리 잡게 됨에 따라 이러한 컴핀트의 중요성은 더욱 높아지고 있다. 전자적으로 저장되는 정보 또한 지속적으로 증가하고 있으며, 물리적 도난이 흔적을 남기는 점에 반해 컴핀트는 탐지의 흔적을 남기지 않는다는 장점도 존재한다.

4) SIGINT는 다시금 레이더 능력과 특성을 파악하는 전자정보수집(ELINT: Electronic Intelligence)과 통신의 내용을 파악하는 통신정보 수집(COMINT: Communication Intelligence)으로 분류할 수 있다.

#### 4) OSINT (Open Source Intelligence)

오신트는 공개된 출처에서 얻는 정보로서 공개정보, 공개소스정보, 오픈소스정보 등으로 불리고 있다. 민간에서 특히 오신트의 분석기관으로 유명한 것은 언론사와 대학 등이며 위키피디아도 대표적인 오신트에 해당한다.

오신트 자료는 사용자의 측면에서 보안이 요구되지 않는다는 것이 특징인데 합법적인 방식으로 다량의 기초정보의 수집이 가능하다. 이러한 방대한 자료들의 분석과 접목을 통해 가치가 부가되는 고급정보의 생산이 가능하다. 오신트의 큰 장점은 정보취득을 위한 고가의 탐지장비들을 필요로 하지 않는 것이다.

오신트는 정보기관의 정보분석에 있어서도 중요한 소스가 되고 있는데, 독일 바덴뷔르템베르트 주 헌법보호청에 따르면 오신트에 기반을 둔 정보기관의 정보생산이 90%에 달한다고 한다(Lux & Peske, 2002). 아직 독일에서도 사경제영역에서 오신트에 정보 점유비중이 어느 정도인지는 구체적으로 연구된 바가 없으나, 정보기관의 비중보다 더 높을 것으로 추정하고 있다. 가장 보편적인 방식은 인터넷을 활용하는 것이다. 거의 모든 기업들이 인터넷에서 잠재적인 고객들에게 기업에 관한 정보를 제공하고 있다. 기업정보의 탐색은 이러한 인터넷상의 기본정보에서 시작되고 검색기능을 통해 확산된다.

## Ⅲ. 산업기밀보호 관련 법제

기업이 보유하고 있는 정보나 기술이 국가의 중요한 자산으로 인식되어 보호되어야 한다는 점에는 전 세계의 모든 국가들이 공감하고 있으나 이에 대응하는 법제도는 크게 두 가지로 구분된다. 새로운 법적 장치로의 대응을 적극적으로 모색하는 국가로 경제스파이법을 제정하여 시행하고 있는 미국, '산업기술의 유출방지 및 보호에 관한 법률'을 통해 적극적으로 대응하고 있는 우리나라 등을 들 수 있고, 반면에 독일과 같은 국가는 부정경쟁방지법이나 형법과 같은 기존의 법규범의 보완을 통해 대응하고 있다고 볼 수 있다.

독일에서는 산업기밀의 보호에 관련한 법적 근거로 부정경쟁방지법(UWG)[5]을 들

5) "Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. M rz 2010 (BGBl. I S. 254)"

수 있다. 동법 제1조에서는 이 법이 경쟁자와 소비자, 그 밖에 시장참여자들을 부정한 영업행위로부터 보호하기 위함을 그 목적으로 정하고 있다. 동시에 왜곡되지 않은 경쟁에 따른 일반의 이익을 보호하고 있다.[6] 동법은 영업비밀관련 처벌규정을 마련하여 산업스파이로부터 산업기밀을 보호하고 형사적 대응이 가능하도록 한다. 물론 동법 제정 이전에 형법이나 기본 법제를 통해 이에 대한 대응이 불가능한 것은 아니었으나, 그 대응이 한계 이르자 영업비밀보호를 부정경쟁방지법에 도입하기에 이른 것이다. 우리나라에서 시행되고 있는 "부정경쟁방지 및 영업비밀보호에 관한 법률" 또한 독일의 부정경쟁방지법을 그 모태로 하고 있다고 볼 수 있는데(하헌주, 2005), 독일의 법도그마를 따라 우리나라에서도 영업비밀의 침해를 부정경쟁의 법리로 이해하고 있다는 의미이다.

부정경쟁방지법에 도입된 1996년 당시, 고객명단과 같은 영업상의 정보를 포함하지 않는 기술적 지식을 중심으로 한 개념인 노하우(Know-how)의 보호에서 시작되었으나, 이후 개정이 이루어지면서 보호범위를 점차 넓혀 현재는 영업상의 비밀까지 이르고 있다(이정덕, 한형구, 2007).

또한 형법(SGBG)에서는 타국을 위해서 독일의 기밀을 유출하는 행위를 처벌하고 있는바, 이 또한 산업기밀보호, 특히 국가적 개입과 보호의 법적인 근거가 된다고 할 수 있다.

## 1. 부정경쟁방지법(UWG)

부정경쟁방지법이 도입되기 이전, 독일에서는 상표법 내지 상법에 근거하여 충분히 부정경쟁 행위가 규제될 수 있을 것이라 보고 민법상의 불법행위 규정만을 두고 무제한의 영업자유를 인정하였으나, 산업스파이 등 부정경쟁 현상이 심각해지자 1896년 기만적 광고와 같은 특별한 형식의 불법경쟁행위를 금지시키는 부정경쟁방지법을 제정하기에 이른다(한국특허기술연구원, 2010).

부정경쟁방지법에서 영업비밀의 보호는 제17조에서 규정하고 있는데, 영업비밀의 침해행위는 기본적으로 공정한 경쟁을 해치는 행위로써 선량한 풍속에 반하는 것으

6) "Dieses Gesetz dient dem Schutz der Mitbewerber, der Verbraucherinnen und Verbraucher sowie der sonstigen Marktteilnehmer vor unlauteren gesch aftlichen Handlungen. Es sch utzt zugleich das Interesse der Allgemeinheit an einem unverf alschten Wettbewerb."

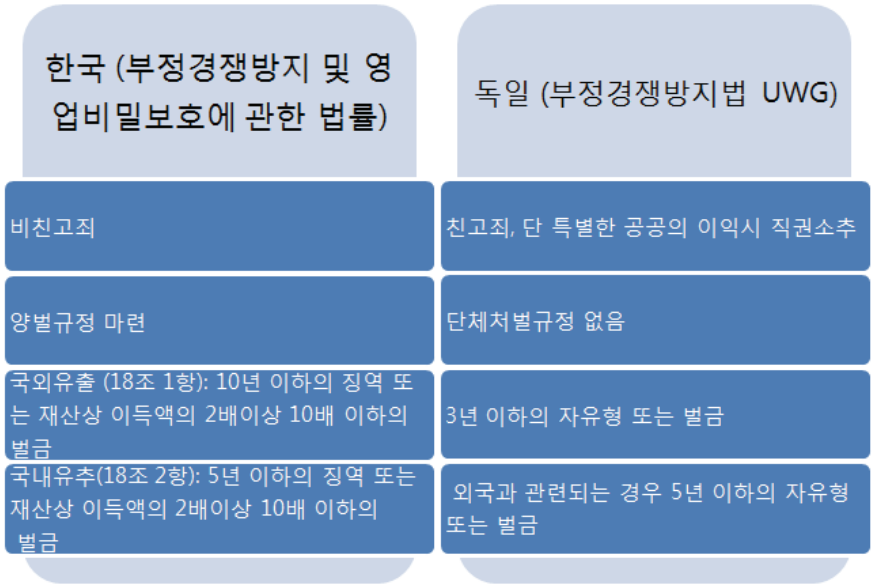
로 본다.

동조에 따르면, 기업의 종업원, 근로자 또는 견습공으로서 근로관계에 의해 위탁받거나 접근 가능한 산업기밀 또는 영업기밀을 고용기간 동안에 경업(競業)목적, 자신의 이익, 제3자의 이익을 위하여 또는 사기업에 손해를 가할 목적으로, 권한 없이 누군가에게 전달한 자는 3년 이하의 자유형 또는 벌금에 처해지며, 이를 친고죄로 규정하고 있다. 동조에서의 행위자는 고용관계가 계속되는 자로서 기업에 소속된 모든 구성원이 해당된다고 하겠다. 또한 '권한 없이'의 의미는 영업비밀 소유자에 대하여 피용자가 부담하고 있는 신뢰의무에 반한다는 의미이다.

산업기밀과 영업기밀에 대한 지식은 영업관련성(Betriebsbezogenheit), 비공개성(Nichtoffenkundigkeit), 기밀유지의 의사(Geheimhaltungswille), 기밀유지의 이익(Geheimhaltungsinteresse)이라는 네 가지 구성요소를 필요로 한다.

우선 영업관련성에 있어서 보호되는 기밀은 직접적으로 구체적인 산업이나 영업에 관한 정보라야 한다. 따라서 사적 영역에서의 기밀, 이를테면 기업경영자의 사생활 등과 같은 것은 산업기밀이나 영업기밀에 해당하지 않는다.[7] 비공개성은 상당히 제한된 인원에게만 기밀에 관한 사항이 알려져 있음을 의미한다. 또 기밀을 공유하고 있는 인적구성원들의 범위는 기밀보유자나 정보의 소유자에게 알려져야 한다. 기밀유지의 의사는 정보의 유출차단을 위한 적정한 조치를 통해 구체화된다. 예를 들어 보안표지(vertraulich)나 이와 유사한 표식이 문서에 표시되어야 한다. 기밀유지의 의사는 기밀의 유출을 통해 부정적인 결과가 발생한다는 기밀유지의 이익과 함께 결부되어 고려되어야 할 것이다(Többens, 2000). 행위가 특히 중한 경우는 제4항에 따라 5년 이하의 자유형으로 가중처벌하게 되는데, 비밀이 외국에서 이용되는 것임을 알고 있는 경우, 또는 행위자 스스로 외국에서 이용하는 경우가 여기에 해당되며 미수범도 처벌된다.

7) 물론 이러한 사적인 정보의 수집을 통해 기업임원이나 종사자들에 대한 협박과 회유가 가능하므로 산업스파이들의 주요한 수집대상이 됨은 물론이다.




〈그림 2〉 한국과 독일의 영업비밀관련 규정 비교

## 2. 국가적 법익에 대한 침해

이상에서 살펴본 영업비밀에 관한 사항은 엄밀히 말하자면 사적인 산업기밀에 대한 침해로부터 권한자를 보호하고 불법적인 행위를 처벌하기 위함이고, 경제스파이와 산업스파이를 구분하는 경우 후자를 보호하기 위한 법제라고 볼 수 있다.

반면 경제스파이의 경우는 그 행위자의 배후에 국가가 존재하거나 국가와의 직간접적인 연관성이 존재하는 간첩행위의 일환으로 볼 수 있다. 독일형법 제99조는 타 권력체의 비밀정보활동을 위해 독일연방공화국에 반하는 사실이나 사물, 지식을 전달하는 행위를 하는 경우 5년 이하의 자유형이나 벌금형으로 처벌하고 있는데 경제스파이가 여기에 해당할 수 있겠다.

책임 있는 지위를 남용하거나 행위로 인해 독일연방공화국에 심각한 피해의 위험을 야기하는 경우 10년 이하로 형량이 강화된다. 이 경우 타 정보기관을 위한 행위가 실행되어야만 하는 것이 아니라 그러한 행위의 착수만으로도 처벌이 가능하게 된다.

독일연방공화국에 대한 적대적 비밀정보행위에 해당하려면, 독일의 전체 경제의

이익에 반하는 행위가 존재해야 하는바, 심각한 개별행위나 행위들의 총합을 통해서도 발생할 수 있다. 공공의 이익이 심각하게 관련되는 고용시장에의 영향이나 정부재정에 심각한 피해를 가져오는 행위 등이 그것이다(Jerouschek & Köbel, 2001).

이러한 경제스파이 행위들은 비록 법제도에 의한 원칙적인 처벌이 가능함에도 실제 적용이 그리 쉬운 것은 아니다. 피의자가 외교면책특권을 향유하여 형사사법적 개입이 불가능한 경우가 있기 때문이다. 특히 외교시설이나 상주하는 타국의 군사시설 등과 같은 장소는 독일의 법역에 해당하지 않으므로 경제스파이 행위에 대한 효과적인 대응이 불가하고 따라서 사전단계에서 이를 예방하거나 외교적인 수단으로 항의할 수 있을 뿐이다.

## Ⅳ. 산업기밀보호를 관장하는 국가기관

독일에는 경제영역에서의 기밀보호와 스파이활동을 저지하고 대응하기 위한 많은 국가기관들이 존재한다. 타 국가기관들과의 기본적인 차이점은 독일의 정부기관은 자국의 경제이익을 위한 스파이활동이 법적으로 금지된다는 점이다. 우리나라의 국가정보원법상의 모호한 권한규정과는 달리, 정보기관에 이르기까지 철저한 법치주의를 강조하는 독일에서는 정보기관이나 형사사법기관들의 임무를 명확히 규정하고 있으며, 이에 따라 그들의 임무는 산업기밀보호에 관련한 스파이행위들을 예방하고 추적하는 방어적 임무로만 제한된다. 다만 정보기관의 직무와 그 민감성으로 인해 외국의 경제, 산업스파이 활동들에 관한 구체적인 정보에 대해서는 함구하고 있는 것이 현실이기도 하다(Meissinger, 2005).

### 1. 연방 경제기술부(Bundesministerium für Wirtschaft und Technologie)

산업기술보호와 관련 우리나라 산업통상자원부에서는 '산업기술의 유출방지 및 보호에 관한 법률'을 제정·시행하면서 중앙경제부처에서 적극적인 관심을 가지고 개입하고 있으나, 이와는 달리 독일에서는 부정경쟁방지법 및 형법 등과 같은 소극적인 법제로서 산업기술보호에 대처하고 있으며, 따라서 산업기술의 보호는 원칙적

으로 경제부처의 사무라기보다는 독일의 연방 정보기관인 헌법보호청(BfV)과 연방 수사기관인 연방수사청(BKA)을 총괄하고 있는 연방내무부와 관련된다.

정보기관에 의한 사전적·적극적 국가적 관여 또한 산업기술의 침해가 경쟁스파이(Konkurrenzspionage, Wettbewerbsspionage)가 아닌 경제스파이(Wirtschaftsspionage)에 해당하는 경우라야 한다. 이에 해당하지 않는 기업 간의 경쟁적 기밀탐지와 유출 행위는 고소·고발에 따른 수사가 진행되기 이전에는 민사영역으로서 기업인들의 이익집단이자 공법인인 상공회의소(IHK)의 관심사항이다.

실제 산업기술의 유출방지와 보호를 위한 각종 세미나나 홍보자료 등은 각 주나 연방단위의 상공회의소와 헌법보호청의 협력을 통해 이루어진다.[8] 이러한 점에서 특히 산업기술보호 영역에서의 대등한 민관협력이 이루어지고 있다고 볼 수 있다.

우리의 '부정경쟁방지 및 영업비밀보호에 관한 법률'이 특허청 소관 법률로 분류되고 있는 반면, 독일의 부정경쟁방지법(UWG)은 법무부소관 법률로서, 경제기술부는 부정경쟁방지법이 동 부처의 소관법률이 아님을 천명하고 다만 경제적 영향으로 인해 법무부와 밀접하게 교류하고 있다고 설명한다.[9] 따라서 우리나라 산업통상자원부가 관련법령에 근거하여 적극적인 산업기술보호정책을 펼칠 수 있는 반면에, 독일의 경제관청에서는 이러한 역할이 상당히 제한적이다.

본래 관방학(Kameralismus)에서 시작된 독일의 행정은 적극적 역할보다는 소극적인 현상유지에 지대한 관심을 가지고 있었다. 이러한 관점에서 본다면 산업기술보호는 위험의 방지 내지 보안이라는 공안행정의 영역으로 볼 수 있을 것이다. 따라서 경제적 발전이 아닌 현 산업기술의 소극적 보호의 임무도 공안행정의 영역으로 다루고 있는 것이 독일적 상황이다. 민간경제의 오랜 역사를 가지고 있는 독일에서는 민간산업의 보안은 수익자 부담의 원리에 따라 원칙적으로 당연히 민간의 영역으로서 인식되고 있고, 이에 대한 적극적 역할도 민간경제주체의 연합체인 상공회의소가 하는 것이다.

8) 예를 들어 노르트라인베스트팔렌 주에서 제작된 산업기술보호 관련 브로셔는 모두 상공회의소와 주의 헌법보호사무를 담당하고 있는 주 내무부에서 공동으로 제작하고 있다 (https://bmwi-sicherheitsforum.de/ghb/bibliothek/219, 0, 0, 1, 0.html).

9) http://www.bmwi.de/BMWi/Navigation/Wirtschaft/Wirtschaftspolitik/wettbewerbspolitik, did=162816.html

## 2. 헌법보호청(BfV)

연방 헌법보호청은 쾰른에 소재하고 있는 독일의 대내적 정보활동의 주축기관이다. 헌법보호청은 연방법에 의해서 설립된 정보기관으로 분권화된 연방국가인 독일의 특성상 동법에 따라 16개의 각 주에서는 독자적인 주 헌법보호기관(Landesamt für Verfassungsschutz)을 설치하거나 헌법보호 직무를 주 내무부의 한 부서에서 담당하도록 하고 있다(이성용 외, 2006).

헌법보호청은 산업기밀보호를 극우주의, 극좌주의, 외국인혐오주의, 사이언톨로지 감시 사무와 함께 주요 5대 임무영역으로 규정한다. 유럽의 중심이자 나토회원국으로서의 지정학적 중요성뿐만 아니라 각종 첨단 기술을 보유한 수많은 기업의 소재지인 독일은 외국의 정보기관들의 산업기술탐지의 주요 목표가 되어 왔다. 여기에는 대량살상무기의 불법적인 거래와 기술의 유출도 포함된다. 핵이나 생화학적 무기 또는 그 추진체의 기술을 획득하고자 하는 몇몇 국가들이 독일에서 이를 시도하는 것은 더 이상 비밀이 아니다.

외국정보기관들의 산업스파이 활동은 독일의 기업활동을 침해하고 있고, 이러한 스파이활동의 방지이외에 사전적 예방활동 또한 헌법보호청의 중요 사무이고 이를 위한 다양한 활동들을 수행하고 있다.

전통적인 스파이방식 이외에 최근에는 첨단 정보통신 기술을 활용하는 정보획득이 늘어나고 있다. 외국의 정보기관들은 연방기관이나 정계, 산업분야로 정보통신에 의한 스파이 활동을 하고 있다. 헌법보호청은 이러한 정보통신 스파이활동을 탐지, 분석하고 피해 집단이 이러한 공격으로부터 적절한 방어조치를 취할 수 있도록 지원한다.[10]

또한 생명에 직결되거나 국가방위에 중요한 시설에 불순한 인물이 침투하여 사보타주행위가 발생하는 것을 방지하는 인적 기밀보안에 관련한 신원조사활동을 담당하고 있다.

## 3. 연방수사청(Bundeskriminalamt)

연방수사청에서 산업기술보호에 관련된 사무는 공안부(Abteilung ST: Polizeilicher

10) http://www.verfassungsschutz.de/de/arbeitsfelder/af_spionageabwehr_und_geheimschutz/

Staatsschutz)에서 관장하고 있다. 공안부는 다시 4개의 과로 구분되는데 1과(ST 1)는 정치적 동기에 의한 좌우익사범을, 2과(ST 2)는 국제적 정치동기범죄/간첩행위/불법 핵무기유통/반인류범죄 등을 담당하고 3과(ST 3)는 외국인의 정치동기범죄/ 종교적 동기에 기인한 국제테러범죄를 담당한다. 마지막으로 4과(ST 4)는 중앙사무국의 임무를 수행한다. 이중 산업기술보호와 관련한 사무는 제2과에서 담당하고 있는데, 제2과에 소속된 23계가(Referat 23) 경제스파이 범죄를 전담하고 있다.

연방수사청은 연방수사경찰조직으로서 앞서 살펴본 정보기관과는 달리 정보수집이나 방첩의 업무가 아닌 구체적 위험발생 이후 단계에서의 범죄발생 제지 내지 범죄발생 이후의 형사소추를 위한 범죄수사를 그 임무로 한다. 따라서 연방수사청의 개입을 위해서는 법률의 구성요건을 충족하는 범죄가 발생하거나 이러한 범죄발생의 구체적 개연성이 입증되어야 한다.

한편 산업스파이 행위는 독일형법에서 규정하고 있는 법률용어가 아니라 일반적인 사회적 현상을 의미하는 것이므로, 원칙적으로 연방수사청의 개입은 범죄구성요건의 충족을 전제로 한다. 외국의 정보기관이 개입하게 되는 경제스파이 범죄에는 이미 앞서 살펴본 바와 같이 독일형법 제99조가 적용된다.

반면 기업 간의 불법적인 산업기술유출행위인 이른바 경쟁스파이 행위는 부정경쟁방지법상의 처벌조항과 형법상의 데이터 탐지행위(§ 202a, b. c StGB), 데이터조작 및 컴퓨터 사보타주(§§ 303 a, b StGB), 절도 (§§ 242 ff. StGB) 등에 해당하는 범죄로서 마찬가지로 수사기관의 개입이 가능하나, 범죄의 성격상 특별한 공적 이익이 존재하는 경우를 제외하고는 친고죄로서 신고가 있는 경우에 수사기관의 본격적인 수사가 진행된다. 독일의 형사소추사무도 분권화된 연방제도에 따라 원칙적으로 각 주에서 담당하게 되므로 국익에 관련된 경제스파이 행위를 제외한 사적 경쟁스파이 범죄행위에 대해서는 연방수사청이 아닌 각 주의 경찰수사기관이 개입함이 일반적이다.

산업기술유출에 있어서 형사소추기관인 경찰의 개입영역은 우선 ① 신속한 수사절차를 통한 진행 중인 기술유출행위의 저지, ② 타 기관(정보기관)의 개입요청을 통한 공조, ③ 재범이나 지속적 범죄로부터의 보호 등으로 요약될 수 있다.[11]

11) 이상의 내용은 2011년 2월 15일 베를린에서 개최된 제14차 유럽 경찰회의(14. Europ scher Polizeikongress)에서 연방수사청이 주제 발표한 '경제스파이 수사와 경찰업무'의 내용을 참조하였다.

### 4. 연방정보기술보안청 (BSI: Bundesamt für Sicherheit in der Informationstechnik)

연방정보기술보안청은 1991년 1월 1일 본에서 창설되었는데 연방내무부의 외청으로서 「연방정보기술보안청 설치에 관한 법률(BSI-Errichtungsgesetz)」에 근거한다. 연방정보기술보안청은 IT보안에 관한 모든 사무를 관장하는 독립적, 중립적 기관이다. 동 기관의 주요 임무는 독일사회에서 정보통신기술의 안전화다. 정보기술의 제조자 및 적용자를 주된 대상으로, 그 중에서도 연방과 주 및 산하 지자체의 행정을 대상으로 하지만 사기업도 그 대상범위에 포함된다.

연방정보기술보안청의 직무는 '연방정보기술보안청 설치에 관한 법률'(BSI-Errichtungsgesetz) 제3항에 규정되어 있는데, 정보기술 적용시 보안위험의 조사, IT시스템 보안의 심사 및 평가를 위한 기준과 절차, 도구개발, IT보안의 평가 및 심사, IT 보안시스템 및 구성요소의 허가, IT 보안관할기관의 지원, 경찰이나 형사소추기관·헌법보호기관의 지원, IT보안기술의 제조업자·운영자·적용자에 대한 자문 등을 그 임무로 한다.

최근 IT분야에 대한 관심과 중요성이 높아짐에 따라 그 직무의 중요성도 높아지고 있다. 산업기밀보호와 관련하여 동 기관의 중요성은 특히 중소기업에 대한 정보기술 자문에서 나타난다. 이러한 기업들의 경우 독자적인 정보기술보안 부서를 운영하지 못하게 되므로 기업들에 대한 자문이 산업기술유출방지에 지대한 역할을 담당하기 때문이다.

## Ⅴ. 산업보안에 대한 국가책임과 그 한계: 결론에 갈음하여

### 1. 독일 산업보안의 국가정책

독일은 고도로 발달된 경제와 산업기술로 인해 이미 오래전부터 산업스파이 활동의 주요 무대가 되었으며 따라서 산업기술보호에 대한 지대한 관심을 가져왔다. 특히 국가의 개입이 요구될 뿐만 아니라 적극적인 선제적 역할이 강조되는 경제스파이(Wirtschaftsspionage)분야와 일반 산업스파이(Industrie- spionage) 분야를 구분하여 전

자의 경우 국가기관의 활동의 주된 영역으로서 정부차원의 대응이 두드러지는 반면 후자에 있어서는 상공회의소를 중심으로 하는 민간조직 차원의 활동이 주를 이루고 있다.

1970년 말 RAF테러가 성행하던 시기에 독일상공회의소연합(DIHK)을 중심으로 한 독일 민간경제단체들은 경제보안에 관한 협력체의 조직을 준비하였는데, 정부를 상대로 연방차원에서 경제보안에 관련한 기업들의 이익을 대변하고 동 사안에 관련하여 연방정부에 대응하는 범연방의 대화파트너를 조직하기 위함이었다. 이러한 노력의 결실로 1993년 ASW가 창설되었다. ASW는 "Arbeitgemeinschaft für Sicherheit der Wirtschaft e.V."의 약자로서 "산업보안을 위한 등록법인 협의체" 정도로 번역될 수 있겠다. 동 협의체의 핵심적 임무는 조직의 이름에서 보듯이 산업보안에 관련한 중앙사무를 담당하는 사단법인이다.

국가정보기관의 산업기술보호의 개입은 특정 사기업에 의한 다른 기업에 대한 탐지행위를 의미하는 단순한 경쟁스파이(Konkurrenzspionage, Wettbewerbsspionage)를 넘어서는, 특정 국가에 의해서 조정되고 지원되는 외국 정보기관이 관여하는 기업이나 영업에 대한 탐지라는 경제스파이(Wirtschaftsspionage)의 영역을 다루고 있다는 점에서 그 직무의 영역을 비교적 명확히 제한하기 위한 노력을 하고 있다고 하겠다.

경제스파이에 미치지 못하는 경쟁스파이 행위라 할지라도, 당연히 부정경쟁방지법상의 범죄행위에 해당하게 되고, 이 경우 형사사법기관인 경찰에 의한 수사와 처벌이라는 법집행은 진행될 것이나, 우리나라와는 달리 독일의 부정경쟁방지법은 이러한 산업스파이 행위를 특별한 공공의 이익이 존재하지 않는 한, 친고죄로 보아 형사사법기관의 개입을 제한하고 있다. 더군다나 기 발생한 범죄에 대한 형사소추의 차원이라는 점에서 정보기관의 개입과는 그 의미를 달리한다고 볼 수 있겠다.

독일의 경찰기관은 체포, 구속, 압수, 수색 등과 같은 대인적·대물적 강제권을 가지고 법을 집행할 수 있는 기관으로서 범죄발생 이후의 사후적 대응과 구체적 내지 추상적 위험발생 단계에서 활동하게 된다. 반면 정보기관의 경우는 이러한 추상적 위험이전의 단계에서 위기(Risk)를 관리하는 사전활동에 주력하고 있지만 강제적인 법집행권은 보유하고 있지 않을 뿐만 아니라, 우리나라의 국가정보원과 같은 수사권도 보유하고 있지 못하다는 점에서 양 기관의 권한배분의 균형이 유지되고 있다.

우리나라의 경우 국가의 산업보안정책에 있어서 주무부처가 어디인지조차 불분명한 상황에서 정책적 혼란이 야기될 우려가 있다. 산업보안 예방을 통해 경제이익

을 창출해야하는 경제부처는 여기에 침묵하고 있고, 범죄수사를 담당하는 형사사법기관과 국가보안정보를 담당하는 정보기관 간에도 직무의 구분이 불분명하다. 경찰청에서는 외사국을 중심으로 산업기술유출방지와 관련범죄수사를 주요 직무로 취급하고 있고, 국가정보원에서도 산업기술유출방지를 국가정보원의 핵심기능 중 하나로 분류하고 있다. 「국가정보원법」 제3조 제1항 제1호는 국정원의 직무를 열거하면서 국제범죄조직을 국내 보안정보의 일부로 언급하고 있으나, 사기업에서 유출되는 산업기술은 국가안보나 사회질서에 직접적인 혼란을 야기하는 국내 보안정보라기보다는 국가내 경제활동을 위축시킬 개연성이 있는 국익에 관한 정보로 보아야 할 것이다. 그렇다면 국가의 안위와 무관한 단순한 산업기술정보의 보호가 현행법상 국정원의 직무에 해당하는지, 그 직무범위의 한계도 의문이다.

## 2. 국가개입과 민관협력

치안활동과 마찬가지로 산업보안영역에서도 주된 관심은 위반행위에 대한 처벌보다 그 유출에 대한 사전예방이 될 것이다. 산업보안의 국가사무를 담당하고 있는 국가정보원이나 경찰의 직무는 공히 공공의 안녕에 대한 위험을 방지하는 것이다. 그렇다면 산업기밀유출도 공공의 안녕에 대한 직접적인 침해라고 할 수 있을 것인가. 경찰행정법에서는 형법이나 행정법규범을 위반하는 객관적 법질서 침해를 공공의 안녕의 구성요소로 보고 있으며(서정범, 김연태, 이기춘, 2009), 산업기밀유출이 실정법을 위반하는 범죄라는 점에서는 원칙적으로 공공의 안녕에 대한 위험이며, 국가개입이 정당화될 수 있다고 보인다.

그러나 독일의 입법방식에서 나타나는 것처럼 산업기밀유출이 친고죄로 규정되는 경우 국가가 적극적으로 개입하게 되는 공공의 안녕에 대한 침해로 보기 어렵다. 경우에 따라 산업기밀유출의 피해를 입는 기업들이 기업이미지 실추나 여타 경제적 불이익을 이유로 국가개입을 원하지 않는 경우도 얼마든지 생각할 수 있기 때문이다.

가정의 사생활에 대한 국가개입이 제한되는 것처럼 산업보안의 영역은 원칙적으로 기업의 사적 영역으로서 국가개입이 제한되어야 한다. 국가는 기업이 안전한 경제활동을 할 수 있는 여건을 마련해야 하는 이른바 보장책임(Gewährleistungsverantwortung)[12]을 부담하지만, 그 책임을 어떻게 관철할 것인지는 국가의 정책적 재량사

12) 보장책임은 공공주체가 모든 임무를 스스로 이행할 필요는 없으며, 특정 임무가 누군가에 의해서든

항이 된다. 즉 보안활동의 직접적 수행은 수행책임(Ausübungsverantwortung)으로서 개별 사업자나 그들의 조직으로 위임될 수 있어야 한다(Schuppert, 1998).

그런 의미에서 독일에서 산업보안의 영역을 국가개입이 허용되는 경제스파이와 순수한 기업의 사적 영역인 산업스파이로 구분하는 것은 상당한 의미가 있다. 깊은 학문적 성찰 없이 당위의 영역으로 받아들여지고 있는, 이른바 민관협력(Public Private Partnership: 이성용, 2006)은 기실 대등한 당사자를 전제로 하는 것이다. 산업보안의 영역에서 민간이 대등한 당사자로서 국가와 협력하고 이른바 협조적 법치국가(Wolff, Bachof & Stober, 1994)로 발전하기 위해서는 독일에서 보듯이 국가의 영역과 민간의 영역을 원칙적으로 구분한 이후에 민간차원에서 주도적으로 산업보안을 위한 이익집단을 구성하고 국가와 협력하는 방식으로 나아가야 한다.

## 3. 산업보안과 국가윤리

기존의 연구들은 산업보안정책에 있어서 국가를 방어의 주체로만 인식하였다. 그러나 국가는 산업기술을 보호의 주체일 뿐만 아니라, 나아가 자국의 이익을 위해 외국의 산업기술을 침해하는 침해의 주체가 되기도 한다. 산업보안에 대한 국가개입은 국부나 국익이 부당하게 외국으로 유출되거나, 심각한 기업비밀의 침해로 인한 기업의 경제적 손상을 방지하는 이른바 방어의 영역이 중심이 되어야 한다. 앞서 살펴본 바와 같이 독일의 정보기관들은 산업보안의 영역에 있어서 국가의 역할을 이처럼 소극적 방어로 엄격히 제한하고 있다. 자국의 이익 확대라는 이름으로 정보기관이 외국의 산업기술에 대한 적극적 수집을 하는 것이 어디까지 허용될 수 있을지 고민해야 한다.

2011.2.21자 언론보도에 따르면, 2.16. 국가정보원 직원들이 인도네시아 대통령 특사단의 숙소를 침입하였다. 언론에서 인용한 정부 고위관계자의 말에 따르면 “국정원 직원들이 국익 차원에서 인도네시아 특사단의 협상전략 등을 파악하려 했던 것”이라며 “직원들이 발각된 것은 뜻하지 않은 실수”라고 전했다.[13] 국정원 직원들은 당시 한국을 방문 중이던 인도네시아 특사단 숙소에서 국산 고등훈련기 T-50, 흑표전차, 휴대용 대공미사일 ‘신궁’ 등을 수입하려는 인도네시아의 가격 조건 등 협상전

수행되도록 할 책임만을 부담하는 것을 말한다.

13) http://www.asiatoday.co.kr/news/view.asp?seq=451169

략 관련 정보를 입수하려 했던 것으로 전해졌다. 한편 2013.5.2.자 언론보도에 따르면 호주에서 국가정보원 직원들이 무역협상 정보를 빼내기 위해 호주공무원들을 관리하다가 적발되어 호주 정보기관으로부터 경고를 받기도 했다.[14]

국가정보기관이 국가의 안보를 위해 불가피하게 저지르는 불법행위는 정당화될 수 있다. 그러나 국가의 안보가 아닌 국익의 증진을 위한 비윤리적 행위는 다른 차원이다. 정치철학적 관점에서 본다면 공리주의와 의무론의 논쟁이 될 수 있겠지만, 최소한 국가의 안위를 위태롭게 하는 사안이 아니라면 정당화되기는 어려울 것이다. 공리가 전부라는 도덕이론은 결코 정의에 부합되지 않기 때문이다(레이첼스, 2006).

더군다나 법해석론의 측면에서 볼 때, 현행 국가정보원법은 그 직무범위에 국가이익을 증진을 포함하고 있지 않고, 국가안보만으로 한정하고 있다. 소극적 국가보호가 아닌 국가의 적극적 이익증진을 위한 위법행위가 어느 정도까지 정당화될 수 있겠는가. 국가이익을 위한 절도가 허용된다면, 사회사의 이익을 위한 소속 직원의 기업비밀 절도도 허용될 수 있는가. 애국심으로 정당화될 수 있는 산업스파이 활동이라면 왜 애사심(愛社心)에 근거해서는 허용될 수 없는지 고민해야 한다.

14) 2013.5.2. YTN.

# 참고문헌

김성준, 김우현, 이영석 (2011). 해외 M&A시 산업기술 유출 방지를 위한 법 개선 연구, 한국경호경비학회지, 29, 9-34.

김순석, 신제철 (2010). 산업기술 유출방지를 위한 핵심인력 관리방안에 관한 연구, 한국경호경비학회지, 25, 109-130.

서정범, 김연태, 이기춘 (2009). 경찰법연구, 세창출판사.

신성균, 박상진 (2009). 민간조사원(탐정)을 활용한 기업보안활동의 강화방안: 산업 스파이에 대한 대응방안을 중심으로, 한국경호경비학회지, 20, 199-228.

이성용 (2006). 독일 민간경비의 발전과 Police Private Partnership, 치안정책연구, 160-192.

이성용 외 11인 (2006). 비교경찰론, 수사연구사.

이정덕· 한형구 (2007). 산업스파이범죄에 대한 대응방안에 관한 연구 -미국과 독일 법률의 시사점을 중심으로-, 한·독 사회과학논총, 17(3), 433-466.

제임스 레이첼즈 (2006). 도덕 철학의 기초 (노혜련·김기덕·박소영 역), 나눔의 집.

최선태, 유형창 (2010). 한국 산업보안교육 프로그램의 정립에 관한 연구, 한국경호경비학회지, 25, 185-208.

최진혁 (2010). 산업보안의 제도적 발전방안 연구: 미국 사례를 중심으로, 한국경호경비학회지, 22, 197-230.

하헌주 (2005). 독일경쟁법의 위상과 체계, 비교법학, 16, 69-95.

한국특허기술연구원 (2010). 해외지식 재산권 특허보호 (독일편).

한희원 (2011). 국가정보학 원론, 법률출판사.

Jerouschek, G & Köbel, R. (2001). Souveräne Strafverfolgung, NJW, 22.

Lack, T. (2004). Wissenmanagement. Kremin-Buch, B., Unger, F. & Walz, H.; Wissen- das neue Kapital: Wissenschaft und Praxis.

Lux, C. & Peske, T. (2002). Competitive Intellligence und Wirtschaftsspionage: Gabler.

Meissinger, Jan. (2005). Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland, Hamburg: KOVAC.

Nathusius, I. (2001). Wirtschaftsspionage: Kriminalistik.

Schildbauer, T., Braun, M. & Schultze, M. (2003). Corporate Knowledge: Village.

Schmid. G. (2004). Abhörsystem Echelon, Bericht über die Existenz eines globalen

Abhörsystems für private und wirtschaftliche Kommunikation [On-line] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=DE.

Schuppert, Gunnar Folke (1998). Jenseits von Privatisierung und 'schlankem" Staat: Vorüberlegungen zu einem Konzept von Staatsentlastung durch Verantwortungsteilung. Gusy(Hrsg.), Privatisierung von Staatsaufgaben, Baden-Baden: Nomos Verl.

Többens, W. (2000). Wirtschaftsspionage und Konkurrenzausspähung in Deutschland, Neue Zeitschrift für Strafrecht, 10.

Wolff, Hans. J., Bachof, Otto & Stober, Rolf (1994). Verwaltungsrecht 1. München: C. H. Beck.

【Abstract】

# A Study on the Industrial Security Policies in Germany

Lee, Sung-Yong

The purpose of this paper is to introduce the industrial security policies in Germany and to look for the implication for the development of korean industrial security. Due to highly developed economy and industrial technology, Germany has become the main stage for the industrial espionage for a long time. In Germany industrial espionage is classified into two categories; Economy-espionage and Competition-espionage. While economy-espionage is related to the Espionage of foreign intelligence agencies, Competition-espionage means the act of espionage, that is implemented by the private sector.

When it comes to economy-espionage, prevention of economy-espionage is the duty of the State, because it threat the national interest. Otherwise, the private sector has to take the responsibility of prevention of competition-espionage. It goes without saying that, the state has to investigate the crime, when espionage happens. But Prevention is more important than investigation in this regard.

For the realization of Public-Private-Partnership, the private sector should be the genuine counterpart of the Public through the sharing responsibility of industrial-espionage prevention.

Another talking point this paper suggest, is the national ethic in connection with economy-espionage. The State could be not only a actor of espionage prevention, but also a perpetrator. The economy-espionage for the purpose of national interest would not be justified, unless it has nothing to do with national security.

Key words : Industrial Security, Economy-espionage, Competition-espionage, Public-Private-Partnership, national ethic