

국제법상 산업스파이에 관한 연구*

문 규 석**

I. 서론	3. 규제의 내용
II. 산업스파이에 관한 일반적 고찰	4. 평가
1. 의의	IV. 산업스파이의 이중적 지위에 따른 처벌 문제
2. 성격	1. 서언
3. 실태	2. 이중적 지위
4. 평가	3. 정치범의 관련성 여부
III. 산업스파이의 규제에 관한 법적 근거 및 그의 내용	4. 평가
1. 서언	V. 결론
2. 법적 근거	

I. 서론

냉전시대에서 국제관계의 초점은 국가안보라는 측면에서 군사 및 정치적 협력관계의 구축이 우선적 지위를 차지하였다. 이것은 자본주의와 사회주의라는 두 축의 대립으로 인하여 대규모의 국제전쟁 또는 핵전쟁의 위협이 고조된 상태였다고 볼 수 있다. 그런데 1980년대 후반을 기점으로 냉전체제가 무너진 이후에 대규모 국제전쟁의 위협이 감소하게 되었다. 이와 동시에 경제문제가 차지하는 무게중심은 점차 확대되었다. 따라서 자본주의와 사회주의를 지향하는 국가들간의 대규모 군사적 충돌은 감

* 이 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2002-075-B00024).

** 전 한국외국어대학교 학술연구교수, 현 한국외국어대학교 강사.

소한 반면에 자국에게 괄목할만한 경제적 이익을 가져다 줄 수 있는 새로운 유형의 전쟁이 나타났다. 그것은 각종 첨단산업기술정보를 수집하기 위하여 산업스파이를 활용하는 경제전쟁이다.

이러한 예는 국내 및 국제적인 측면에서 찾아볼 수 있다. 먼저 국내적인 측면에서, 6세대 초박막 트랜지스터 액정표시장치(TFT-LCD) 컬러필터의 공정기술을 빼내 대만 A반도체사에 입사하려 한 혐의로 관련자를 체포한 사건,¹⁾ 국내 휴대폰 제조업체 A사 연구원들을 매수해 기술을 빼낸 혐의로 관련자를 구속기소한 사건이 있다.²⁾ 국제적 측면에서 미국 인텔사의 펜티엄 프로세서의 설계도를 인텔사 직원이 훔쳐서 경쟁사에 전송하려다가 체포된 사건,³⁾ 미국인이 소위 별들의 전쟁이라고 불리는 미국의 전략방위구상(SDI)에 관한 비밀기술을 제공한 대가로 일본의 미쓰비시 등 4개 회사로부터 60만 달러 이상을 받은 사건,⁴⁾ 스웨덴 정부가 자국 기업 에릭슨의 핵심 기술자료 유출혐의로 스웨덴 주재 러 대사관 외교관 2명을 추방 조치한 사건이 있다.⁵⁾ 게다가 미국은 영국의 잉글랜드 지방에 설치한 Echelon 스파이 시스템을 사용하여 유럽의 재산정보를 가로채어 그 정보를 미국 회사에게 제공하고 있고, 프랑스도 외국의 경제자료를 수집하기 위하여 스파이위성을 운영하고 있다.⁶⁾

국제법상 무력충돌시에 타방 교전자의 병력, 무장의 정도, 전략과 전술의 파악 및 군사작전이 수행되는 지형지물의 탐색에 관한 정보를 습득하기 위하여 스파이(간첩)를 활용하는 것은 국제법상 허용되어 있다.⁷⁾ 문제는 평시에 군사 및 정치에 관한 정

1) 동아일보, 2004. 12. 6(제45판), p.A31.

2) 국가정보원, 『언론보도자료집(2002. 1 - 2004. 6): 산업스파이 사건 재조명』, 2004. 7, p.83; 국내의 기술이 해외로 유출되는 사건 및 국내 업체간 기술유출 사건에 관한 수사 사례는 남상봉, “산업스파이 수사사례 분석 및 대응방안”, 국가정보원, 『산업보안 연구논총』, 창간호, 2004. 11, pp.62-70 참조.

3) Robert C. Van Arnam, “Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection”, North Carolina Journal of International Law & Commercial Regulation, vol.27, Fall 2001, p.95.

4) 박인환, “산업스파이 수사상의 문제점과 대처방안”, 『검사세미나 연수자료집: 국제화시대의 검찰 수사력 제고방안』, 법무연수원, 1995, p.197.

5) 국가정보원, 『산업보안 focus』, 창간호, 2004. 7, pp.56-57.

6) Robert C. Van Arnam, op. cit., pp.130-131; 국가정보원, 전계 자료집, p.166; 조선일보, 1999. 11. 4(제42판), p.9; 동아일보, 2005. 12. 27(제45판), p.A15 참조.

7) 육전의 법규 및 관례에 관한 협약의 동 부속규칙(이하 육전규칙) 제29조-제31조, 1949년 8월 12일자 제네바 제협약에 대한 추가 및 국제적 무력충돌의 희생자 보호에 관한 의정서(제1의정서) 제46조; 김명기, 『국제법(하)』, 박영사, pp.1327-1329 참조; 일반적으로 스파이(간첩)는 특정 국가에

보가 아니라 산업정보(또는 경제정보)를 입수하기 위하여 산업스파이를 특정 국가가 우호국 또는 비우호국으로 파견할 수 있는지 여부이다. 이와 연계해서 제기되는 이슈는 국가가 아니라 특정 회사가 산업스파이를 외국에 파견하여 특정 산업정보를 수집하는 것이 국제법상 허용된 행위인지? 국제법상 산업스파이로부터 보호받을 가치가 있는 정보가 무엇인지? 산업스파이행위를 자행한 이후에 국외로 도피한 경우에 그를 강제로 송환하는 것이 가능한 것인지 등이다.

본 논문은 국제법적인 측면에서 첨단산업기술정보(영업비밀)를 절취하는 산업스파이에 관한 연구이다. 본 연구의 필요성은 첫째, 국내법상 산업스파이는 부정경쟁방지법, 컴퓨터프로그램보호법, 형법 등으로 처벌이 가능하지만 국제법상 산업스파이가 무엇이고 이들의 규제에 관련된 국제조약과 국제관습이 무엇인지 조사할 필요성이 있다는 점이다. 둘째, 산업스파이의 신분이 국가에서 파견된 비밀요원이고, 이들이 활동 중에 체포된 경우 또는 절취한 기술을 전송한 이후에 국외로 도주한 경우에 이들을 어떻게 처리해야 할 것인지에 대하여 검토할 필요성이 있다는 점이다. 셋째, 산업스파이행위에 의해서 영업비밀이 도난을 당한 경우에 국내법상 보호되어야 할 영업비밀의 개념 및 그 범위에 대해서도 알아야 한다는 점이다.

본 연구에서 연구의 범위와 관련하여 제외되는 사항은 다섯 가지가 있다. 첫째, 산업스파이가 절취하고자 하는 정보는 첨단산업기술정보에 한정된다. 즉 기밀인지 여부를 떠나서 군사정보 및 정치관련 정보는 제외된다. 둘째, 산업스파이행위와 관련하여 사람이 직접적으로 개입된 산업정보의 수집이 아니라 예설린, 스파이위성과 같이 첨단과학기술이 접목된 수집 방법도 논의의 대상에서 제외된다. 셋째, 영역적 범위의 측면에서 특정 국가 내에서 기업간에 일어날 수 있는 산업스파이행위는 국내법적인 관점에서 처리될 수 있으므로 제외된다. 넷째, 외국기업이 특정한 능력이 있는 사람을 스카우트하기로 하고 또 그 사람이 특정한 첨단산업기술정보를 그 기업에게 제공하는 경우에 외국기업의 스카우트가 자연인의 직업선택의 자유와 충돌할 수도 있다. 이 문제는 본질적으로 헌법에서 인정된 기본권과 관련된 문제이므로 제외된다. 다섯째, M & A와 관련하여 중요한 산업기술이 외국의 기업에게 이전되는 경우도 국제공법적인 측면에서 다룰 수 있는 문제가 아니므로 제외된다. 따라서 산업스파이는 특정 국가가 자국 국민을 다른 나라에 파견하여 산업스파이행위를 자행하도록 한 경우로

서 군사, 정치, 산업적 가치에 관한 비밀정보를 입수할 목적 또는 다른 비밀스런 목적을 위하여 어느 특정 국가가 다른 특정 국가로 파견한 비밀요원이다. Robert Jennings & Arthur Watts, *Oppenheim's International Law*, 9th ed., vol.I (London : Longman, 1992), p.1176.

한정된다. 다만, 기업이 파견한 요원이 다른 국가에서 또는 A국의 국민이 B국 또는 B국의 기업으로부터 모종의 대가를 받기로 계약한 이후에 B국 또는 C국에서 산업스파이행위를 자행한 경우는 처벌의 문제와 관련하여 제한적으로 기술하고자 한다. 그러므로 II에서 산업스파이에 관한 일반적 고찰, III에서 산업스파이행위의 규제에 대한 법적 근거와 그 내용, IV에서 산업스파이의 이중적 지위에 따른 처벌 문제를 살펴보고자 한다. 마지막으로 V에서 본 연구의 결론으로서 산업스파이의 예방과 진압에 관련하여 제안하고자 한다.

II. 산업스파이에 관한 일반적 고찰

1. 의의

(1) 용어 및 개념의 다양성

현대 사회는 정보화 사회라고 한다. 실질적으로 정보 자체가 경제적 가치를 지니고 있다는 것은 부인할 수 없는 사실이다. 특히 첨단산업기술정보는 천문학적 가치를 지니고 있는 것으로 평가할 수 있다. 따라서 냉전체제가 무너진 이후에 비정상적인 방법으로 첨단산업기술을 습득하기 위한 첩보전은 총성이 없는 전쟁의 한 유형으로 볼 수도 있다. 이것은 각국이 첨단산업기술을 습득하고자 한 반면에 그 기술을 보유한 국가는 그 기술의 보호 자체가 국가안보의 중요한 요소로 간주한다는 측면이 있다. 일반적으로 각국이 산업스파이를 활용하는 이유는 다음과 같다.⁸⁾ 첫째, 국가(또는 기업)가 전략적으로 육성하고자 하는 특정 분야의 기술을 개발하기 위하여 소요되는 시간과 재정지출을 줄일 수 있다는 점이다. 둘째, 특정 기술을 개발하였다고 하여도 대량생산을 위한 생산기술의 습득이 매우 중요하다는 점이다. 셋째, 국가 경제력의 증진은 군사력의 향상뿐만 아니라 국가안보를 강화하게 한다는 점이다. 넷째, 천문학적 규모의 국제입찰에서 낙찰을 받아 국제시장에서 성공할 가능성을 증대하기 위함이다. 다섯째, 냉전시대에 활용하던 스파이활동을 유지하기 위함이다.

국제법상 일반적으로 산업스파이의 정의가 무엇인지 명확하지 않으나 소개하면 다음과 같다. 첫째, 산업이 아니라 경제라는 좀더 포괄적인 용어를 사용하여 정의한 경우이다. 즉 경제스파이(economic espionage)는 자국정부, 기업, 또는 사인의 지시로 불

8) Karen Sepura, "Economic Espionage: The Front Line of a New World Economic War", *Syracuse Journal of International Law and Commerce*, vol.26, Fall 1988, pp.133-134.

법적이거나 은밀한 대상 또는 영업비밀의 습득이 관련되는 외국정부의 후원, 조정 또는 지원으로 행해지는 첩보수집활동을 말한다.⁹⁾ 또는 경제적 이익을 위한 재산정보 또는 기술과 같은 경제정보에 대하여 허용되지 아니한 방법으로 입수하기 위하여 외국정부에 의해서 종사되거나 또는 조장되는 불법, 은밀, 강압 및 속임수적인 활동을 말한다.¹⁰⁾ 반면에 산업스파이는 원천기술 자체에서 자동적으로 제공하는 것이 아니라 영업비밀과 같은 정보를 수집하기 위하여 특정 기업의 불법적 기술의 유용을 말한다.¹¹⁾ 따라서 산업스파이와 경제스파이의 주된 차이점은 파견자가 누구이냐에 따라서 국가가 파견하면 경제스파이이고 기업이 파견하면 산업스파이라는 견해이다.¹²⁾ 둘째, 경제스파이와 산업스파이를 동의어적인 관점에서 접근하는 경우이다. 즉 “경제적 목적으로 산업비밀 등을 비밀리에 입수하기 위하여 상대국의 기업을 대상으로 스파이 활동이 전개될 때 이를 통상 산업스파이 또는 경제스파이라고 한다. 이렇게 볼 때 산업스파이란 상대국 기업이 소유하고 있는 물품의 제조방법, 기타 산업상, 영업상 유용한 기술이나 경영정보 등 산업체의 업무에 관한 비밀, 줄여서, 영업비밀을 부정하게 입수하거나 정탐하는 일체의 행위를 말한다.”¹³⁾ 셋째, 절취행위를 중심으로 정의하는 경우이다. 즉 절취자(산업스파이)가 그 행위로 인하여 자국 정부, 기업, 고용인의 이익을 초래할 것이라는 사정을 알고서 경제적 가치가 있는 정보를 절취하는 행위를 자행하는 사람이다.¹⁴⁾ 산업스파이가 절취하고자 하는 대상을 재산권으로 본다는 측면으로 이해할 수 있다.

(2) 절취하고자 하는 목적물이 무엇인지?

산업스파이의 정의는 산업스파이가 비정상적인 방법으로 절취하고자 하는 목적물이 무엇이고 그 목적물의 본질을 어떻게 파악하느냐에 따라서 다를 수 있다. 먼저 산업스파이가 비정상적인 방법으로 절취하고자 하는 목적물이 무엇인가? 두 종류의 유형으로 나누어 볼 수 있다.¹⁵⁾ 하나는 산업정보라는 관점에서 첨단산업기술정보를 의

9) Darren S. Tucker, “The Federal Government's War on Economic Espionage”, University of Pennsylvania Journal of International Economic Law, vol.18, Fall 1997, p.1112.

10) Karen Sepura, op. cit., p.128.

11) Darren S. Tucker, op. cit., p.1113.

12) Ibid.

13) 한상훈, 『산업스파이에 대한 형사법적 대응방안』, 한국형사정책연구원, 2000. 12, p.33-34.

14) Katherine Barr, Melissa Beiting and Amy Grzesinski, “Intellectual Property Crimes”, American Criminal law Review, vol.40, Spring 2003, p.777 참조.

미한다. 즉 생물공학, 항공, 정보통신, 컴퓨터 관련 기술, 첨단 무기제조기술, 반도체, 환경관련 기술 및 기타 등을 말한다. 다른 하나는 재산정보의 관점에서 입찰정보, 계약정보, 고객과 기업전략 정보 등을 의미한다. 재산정보라는 관점에서 보면 이들 양자는 모두 첨단산업기술정보도 포함될 수 있으나 그 정보의 성질에 차이가 있다. 즉 전자는 순수한 첨단산업기술에 관한 정보로서 기업이나 국가에게 모두 지극히 유용한 정보인 반면에 후자는 주로 특정 기업의 측면에서 경제적 가치가 있는 정보이다. 또한 전자는 지적재산권적 성질이 있는 정보인 반면에 후자는 경제적 측면에서 재산적 가치가 있는 정보라고 볼 수 있다.

산업스파이의 목적물은 WTO/TRIPS(Agreement on Trade-Related Aspects of Intellectual Property Rights) 협정 제7절 제39조 2항의 미공개정보(undisclosed information), NAFTA¹⁶⁾ 제1711조 1항에서 규정된 영업비밀(trade secrets),¹⁷⁾ 그리고 EU(European Union)에서 노하우¹⁸⁾ 등으로 불려지고 있다. 반면에 산업재산 보호를 위한 파리협약(Paris Convention for the Protection of Industrial Property: 이하 파리협약) 제1조 2항에서 규정된 산업재산이 될 수 있다.¹⁹⁾ 문제는 동 협약에서 산업재산이라

15) Karen Sepura, op. cit., pp.132-133; Darren S. Tucker, op. cit., p.1117 참조.

16) North American Free Trade Agreement Between the Government of Canada, the Government of the United Mexican States and the Government of the United States of America of December 8, 1993.

17) 미공개정보는 WTO/TRIPS 협정 제7절(미공개정보 보호) 제39조 2항, 영업비밀은 NAFTA 제1711조 1항에서 규정된 용어로서 양자의 개념은 실질적으로 동일한 개념이다. WTO/TRIP협정에서 미공개정보는 사람과 법인은 합법적으로 그들 자신의 통제 하에 있는 정보가 건전한 상업적 관행에 반하는 방법으로 그들 자신의 동의가 없이 다른 사람에 의해서 공개되거나 습득되거나 또는 사용되는 것을 방지할 수 있는 다음과 같은 정보를 말한다. 즉 (a) 정보가 전체로서 또는 그 구성요소의 엄밀한 배열 및 조합의 형태로서 당해 정보의 종류를 정상적으로 다루고 있는 업계의 사람들에게 일반적으로 알려져 있지 아니하고 또는 쉽게 접근하기 어렵다는 의미에서 비밀인 것, (b) 그것이 비밀이기 때문에 상업적 가치를 지니고 있는 것, (c) 적법하게 비밀을 통제하고 있는 자에 의하여 그 정보를 비밀로 유지하기 위하여 정황상 적절한 조치 하에 있는 정보를 의미한다. 따라서 본 규정에 의하여 미공개정보의 개념 속에 ① 비밀성을 지니고 있고, ② 상업적 가치가 있으며, ③ 그 비밀을 지키기 위하여 특정한 조치가 필요하다는 점이 포함되어 있다.

18) EC Commission Regulation (EEC) No 556/89 of 30 November 1988 on the application of Articles 85(3) of the Treaty to certain categories of knowhow licensing agreements에서 Knowhow는 어떤 적절한 형태로 비밀성이 있고 실체성이 있으며 독자성이 있는 기술정보의 실체를 의미한다(1조 7항 1호) O.J. L061, 04/03/1989. pp.1-13 참조.

19) 동 협약에 의하여 보호받고 있는 산업재산은 특허, 실용신안, 의장, 상표, 서비스 마크, 상호, 원산지 표시 또는 원산지 명칭 및 부정경쟁방지에 관한 것까지 그 대상으로 한다.

는 용어를 가장 넓은 의미로 해석함과 동시에 본래의 공업·상업뿐만 아니라 농업 및 채취산업분야, 포도주, 곡물, 담배 잎, 과일, 가축, 광물, 광천수, 맥주, 꽃, 밀가루와 같은 모든 제조된 또는 천연 상품의 모든 산업에게도 적용된다는 점이다.²⁰⁾ 따라서 산업스파이의 목적물은 첨단기술정보, 미공개정보 또는 영업비밀을 의미한다. 파리협약에서 말하는 산업재산은 너무 광범위한 의미이므로 좁은 의미의 산업재산으로서 첨단산업기술정보를 의미한다고 볼 수 있다.²¹⁾ 그러므로 산업스파이의 목적물은 비밀성과 상업적 가치가 있고, 그 비밀 보호를 위하여 특정한 조치를 필요로 하는 대상으로 볼 수 있으므로 영업비밀, 그리고 좁은 의미의 산업재산으로 보는 것이 타당하다.²²⁾

(3) 취득하고자 하는 목적물의 본질은 무엇인지?

산업스파이의 목적물이 첨단산업기술정보이고, 이것을 영업비밀이라고 한다면 이러한 목적물의 본질을 어떻게 이해해야 하는지? 즉 재산적 가치가 있는 것으로 보아야 하는지 또는 지적소유권의 한 형태로 보아야 하는지 여부이다. 이러한 문제는 각국의 국내법상 영업비밀을 보호함에 있어서 그 보호방법과 보호의 정도 및 법체계가 상호간에 밀접한 관계가 있기 때문이다. 간략하게 설명하면, 영업비밀을 재산권으로 보는 견해는 산업스파이가 영업비밀을 침해하는 행위를 금지하고 침해로 인하여 손해가 발생하는 경우에 손해배상을 허용하는 부정경쟁행위로 본다. 따라서 그 보호요건과 구제수단은 부정경쟁방지법에 규정되어 있고 보호의 정도는 부정경쟁방지법을 비롯하여 각국의 형법, 계약법, 불법행위법 등 복수의 개별법으로 보호하고 있다. 영

20) 파리협약 제1조 3항.

21) 그 이유는 첫째, 파리협약에서 규정된 바와 같은 가장 넓은 의미의 산업재산으로 이해한다면 산업스파이가 주로 절취하고자 하는 대상의 범위가 너무 광범위하다는 점이다. 즉 단순한 정보를 얻을 목적으로 위험을 감수하면서 산업스파이를 파견한다는 것은 이해하기 어렵다. 둘째, 입찰정보와 계약정보는 특정 사업에 대한 정보이기 때문에 국가적 관점에서 입수하기 보다는 특정 기업이 그 기업의 사활적 이익을 위하여 로비스트를 활용할 수 있다는 점이다. 즉 국가적인 측면에서는 좁은 의미의 산업기술정보를 입수하는 것이 필요하고, 특정 기업의 측면은 좁은 의미와 넓은 의미의 모든 유형의 산업정보가 필요하다. 셋째, 산업재산을 좁은 의미로 본다면 WTO/TRIPS와 NAFTA에서 규정한 미공개정보 또는 영업비밀의 개념과 사실상 동일한 개념으로 인식할 수 있다는 점이다.

22) 산업스파이가 비정상적인 방법으로 절취하고자 하는 목적물은 미공개정보, 영업비밀 및 좁은 의미의 산업재산(첨단산업기술정보) 등으로 불리어질 수 있으나 본 논문에서는 이들 모두를 혼용하여 사용하고자 한다.

영업비밀을 지적재산권으로 보는 견해는 영업비밀은 배타적으로 특정 기간 동안 보호하는 한편 권리보호 요건으로서 등록해야 한다. 유체재산권과 같이 보호하는 유형이므로 공시되면 그 보호요건은 갖추어져 있다. 그러나 그 비밀성이 공시됨으로 인하여 그 비밀성을 유지하지 못하여 침해받을 가능성이 높다. 반면에 영업비밀 보유자의 측면에서 비밀유지가 되는 경우에 무기한으로 제3자를 지나치게 희생하게 된다.

이러한 문제점이 내재되어 있다는 점을 인식한 GATT/UR 협상단은 절충적 방법을 택하였다. 즉 WTO/TRIPS협정에서 영업비밀을 지적재산권의 한 유형으로 보고, 그 보호방법은 각 국의 법체계와 관행의 범위 내에서 적절한 이행방법을 결정할 수 있도록 하였다.²³⁾ 그러므로 국내법상 산업스파이가 절취하고자 하는 목적물의 본질은 재산적 가치가 있는 것으로 보는 견해와 지적소유권의 한 형태로 보는 견해에 따라서 그 보호방법과 보호 정도가 다르다.²⁴⁾

(4) 산업스파이의 개념 및 개념적 요소

위에서 소개한 산업스파이의 개념은 모두 산업스파이가 비정상적인 방법으로 취득하고자 하는 목적물이 재산적 가치가 있다는 관점에서 내린 정의로 보인다. 따라서 영업비밀이 지적재산권의 한 형태라는 측면에서 살펴보면, 산업스파이란 특정 국가의 기업이 배타적으로 보호하고 있는 영업비밀을 부정한 방법으로 절취하여 파견국에게 그 지적재산권을 전달한 사람이다. 이와 같은 맥락에서 재산적 가치가 있다는 측면에서 살펴보면, 산업스파이란 특정 국가의 기업이 배타적으로 보호하고 있는 영업비밀을 법적으로 허용되지 아니한 경쟁방법으로 입수하여 파견국에게 그 특정 정보를 전달한 사람이다.²⁵⁾

따라서 본 논문에서 산업스파이가 비정상적인 방법으로 취득하고자 하는 내용이

23) 동 협정 제1조 1항 및 동조 2항.

24) 법무부, UR협정의 법적 고찰(하), 1994, pp.594-596 참조; 정진섭·황희철, 『국제지적재산권법』, 육법사, 1995, pp.211-214 참조; 정진옥, “산업재산권으로서 영업비밀의 보호”, 『법학연구』, 부산대학교 법과대학 법학연구소, 제40권 제1호(제48호), 1999. 12, p.336 참조; 한상훈, 전게서, pp.100-102.

25) 특정 국가의 기업이 파견한 요원 또는 특정 국가의 국민이 외국, 외국 기업 및 사인의 지시로 산업스파이행위를 자행한 경우에 산업스파이의 개념은 산업스파이행위를 한 행위자에게 산업스파이행위의 결과에 따라서 고용주로부터 모종의 대가를 받기로 거래하였다는 사실이 포함되어야 한다. 그 이유는 국가가 파견한 산업스파이는 파견국의 이익이라는 애국적 행위가 포함될 수 있지만 국가가 파견하지 아니한 사람은 단지 금전적 이익과 같은 모종의 대가를 목적으로 산업스파이행위를 자행한 것으로 이해되기 때문이다.

재산적 가치가 있는 것이든 또는 지적재산권이든지 간에 일단 산업스파이의 개념은 다음과 같은 요소가 포함되어 있다. 즉 ① 파견자는 국가이다. ② 행위자는 외교관 또는 국가가 파견한 비밀 요원이다. ③ 목적물의 내용이 무엇이고 그 내용물을 무엇으로 불리어지든지 간에 산업스파이의 목적물은 취득하고자 하는 국가의 입장에서 대규모의 재산적 가치가 있어야 한다. ④ 취득 방법은 법적으로 비난을 받을 수 있는 방법을 이용하여야 한다.

2. 성격

산업스파이가 첨단기술정보 또는 영업비밀의 절취 방법은 79종에 달한다고 한다.²⁶⁾ 이들의 주된 방법은 전통적인 절도, 항공촬영, 컴퓨터해킹, 도청, 기업내부자의 매수, 스카우트, 공공기관의 정보를 이용하는 방법 및 기타 등이 있다고 한다. 이러한 다양한 방법들을 이용하는 산업스파이행위는 보통범죄와 구별하여 볼 때 다음과 같은 성격을 지니고 있다.

첫째, 산업스파이행위는 각국의 국내법상 허용되지 아니한 불법적인 방법 또는 경쟁법적으로 허용되지 아니한 방법을 동원하여 정보를 습득한다는 측면에서 볼 때 고의에 의한 범죄행위이다. 반면에 보통범죄는 고의와 과실에 의해서 행해진다. 둘째, 그 고의도 보복, 원한관계의 청산, 충동으로 자행되는 보통범죄와는 달리 오로지 첨단산업기술정보를 절취하여 경제적 이익을 달성하기 위한 목적으로 행해진다. 셋째, 산업스파이의 목적물의 소유주는 국가, 기업 또는 사인이 될 수 있다. 또 그 목적물은 절취된 이후에 경제적 가치로 환산하기 위하여 생산과 판매라는 일련의 과정이 필요하다. 즉 목적물이 생산기술, 생산방법, 설계도 등이므로 금전적으로 환산되기 위해서는 투자·생산이라는 일련의 과정이 필요하다. 반면에 보통범죄는 일반적으로 범죄자들의 목적물의 소유주는 국가, 기업 및 개인이지만 주로 개인과 기업이다. 그 목적물도 금전 또는 금전적 가치가 있는 장물이 대부분이고 투자와 생산이라는 일련의 과정은 필요가 없다. 다만, 장물을 금전으로 환산하기 위하여 판매가 필요하다. 넷째, 그 목적물의 경제적 가치는 얼마라고 간단히 대답할 수 있는 성질의 것이 아니다. 목적물에 따라서 수 천 억원의 가치로 환산될 수 있고 그 기술의 내용에 따라서 크게 차이가 날 수 있다. 반면에 보통범죄의 목적물은 대부분 쉽게 금전적 가치로 환산할

26) 한상훈, 전게서, pp.35-43 참조.

수 있는 것들이다. 다섯째, 목적물이 어떠한 형태로 있느냐라는 측면에서 볼 때 설계도, 컴퓨터에 입력된 프로그램 및 첨단기술을 개발한 사람의 머리에 기억될 수 있다는 점에서 주로 무형적 형태로 존재한다. 반면에 보통범죄의 대상은 지폐, 지갑, 신용카드 및 타인이 소유 또는 점유하는 재물로서 주로 유형적 형태로 존재한다. 여섯째, 산업스파이행위는 첨단산업기술을 개발한 또는 개발할 능력이 있는 사람을 스카우트하는 것도 가능하다는 점에서 특정 분야의 전문가여야 한다. 반면에 보통범죄는 누구나 자행할 수 있다. 일곱째, 산업스파이는 007과 같이 고도의 훈련을 받은 사람 또는 해당기업 내부에서 근무하는 사람을 매수해서 행해질 수 있다는 점에서 항상 은밀한 방법으로 행해진다. 반면에 보통범죄는 누구나 악의적인 생각이 행위로 드러나면 공개 또는 은밀한 방법으로 행해질 수 있다. 여덟째, 신분적인 측면에서 산업스파이는 외교관 또는 비밀리에 파견한 국가요원이 행할 수도 있다. 반면에 보통범죄는 범죄단체에서 특정한 범죄행위를 자행할 목적으로 다른 나라로 파견한다 하더라도 모두다 일반 사인의 신분이다. 이와 같은 점을 도표로 정리하면 <표 1>과 같다.

<표 1> 보통범죄행위와 산업스파이행위간의 다른 점

구분	보통범죄행위	산업스파이행위
정신적 요소	고의 및 과실	고의
주된 목적	보복, 원한 관계청산, 충동, 경제적 이익	경제적 이익
목적물의 소유주 및 목적물의 형태	국가, 기업 및 개인이지만 주로 개인과 기업임. 금전적으로 쉽게 환산할 수 있는 장물이고 그 장물의 판매가 필요함	국가, 기업 및 사인이지만 주로 기업과 국가임. 생산기술, 생산방법, 설계도가 금전적으로 환산되기 위하여 투자·생산이라는 일련의 과정이 필요함
목적물의 가격	쉽게 금전적 가치로 환산할 수 있는 것	기술의 내용에 따라서 그 경제적 가치의 차이가 현격하게 다름
목적물의 존재형태	유형적 형태로 존재함	유·무형적 형태로 존재함
누가 될 수 있는지	누구나 될 수 있음	특정 분야의 전문가
방법	공개 또는 은밀하게 행해짐	항상 은밀한 방법으로 행해짐
신분	일반 사인의 신분	외교관의 신분으로도 가능함

* 필자가 연구·분석하여 작성함

3. 실태

역사적 측면에서 산업스파이의 유래는 1500년경에 중국에서 실크기술과 도자기 기술이 도난당한 사건,²⁷⁾ 고려 공민왕 때에 중국 원나라에서 문익점이 붓투쟁 속에 목화씨를 숨겨 들여와서 재배한 경우 등이 있다.

ASIS(American Society for Industrial Security)는 1999년에 미국 1000개의 우수기업이 영업비밀의 도난으로 인하여 450억 달러, 미국회사들은 2000년에 1조 달러,²⁸⁾ 그리고 제조기술의 도난으로 건당 평균 5천만 달러 정도의 손실을 받았다고 한다.²⁹⁾ 한국의 경우에 1998년 이후 한국에서 적발된 기술유출의 가치는 44조원, 건수는 51건이었다. 그 적발사례 중 중국(39%)이 가장 많았고, 그 다음은 미국(21%), 대만(18%), 일본(10%) 등이었다.³⁰⁾ 국가정보원에 따르면 2004년 1월부터 동년 11월 25일 까지 적발된 산업스파이 사건은 모두 22건으로 총 31조원 가량의 국부가 새나갈 뻔한 것으로 나타났다.³¹⁾ 이러한 기술들은 반도체, 휴대전화, LCD, 의료장비, 제약기술 등 '주식회사 한국'의 첨단 핵심 산업들이다.

4. 평가

산업스파이의 목적물이 지적소유권의 한 형태 또는 재산적 가치가 있는 것으로 보느냐에 따라서 산업스파이의 개념은 약간 다를 수가 있다. 그러나 문제의 핵심은 산업스파이가 첨단산업기술정보가 소재하는 국가에서 스파이(간첩)와 동일하게 은밀하고 비파괴·비정상적인 방법으로 활동한다는 점이다. 따라서 산업스파이는 대규모의 경제적 가치가 있는 첨단산업기술정보를 입수한다는 측면에서 볼 때 육전규칙 및 제네바협약에 의해서 허용된 스파이가 군사적 성격의 정보를 입수하는 것과 비교해 보면 다음과 같은 다른 점이 있다.³²⁾

첫째, 스파이는 적국 또는 적국의 동맹국에서 행해진다. 반면에 산업스파이는 목적물의 소재지가 우호국, 비우호국이 포함된 모든 국가에서 행해질 수 있다. 둘째, 스파

27) Robert C. Van Arnem, op. cit., p.97; Karen Sepura, op. cit., pp.129-130.

28) Katherine Barr, Melissa Beiting and Amy Grzesinski, op. cit., p.773.

29) Robert C. Van Arnem, op. cit., p.97.

30) 동아일보, 2004. 11. 8(제40판), p.B2.

31) 문화일보, 2004. 11. 25(제3판), p.16.

32) 육전규칙 제29조 - 제33조 및 제네바협약 제1 추가의정서 제46조.

이가 활동하는 시기는 전시이다. 반면에 산업스파이는 전시와 평시를 가리지 아니하고 어느 때든지 수행될 수 있다. 셋째, 스파이가 입수하는 정보는 국가기밀에 해당하는 정보이고 이 정보는 전쟁의 승리와 직·간접적으로 연계된 군사정보에 초점이 맞추어져 있다. 반면에 산업스파이는 대규모의 경제적 이익을 목적으로 하는 첨단산업기술정보이다. 넷째, 스파이와 산업스파이가 활동하는 도중에 행위지 국가에서 체포될 위험을 감수하면서 파견하는 이유는 스파이의 경우에 궁극적으로 전쟁의 승리를 목적으로 한다. 산업스파이는 경제안보의 강화(군수산업 강화)라는 목적과 자국 기업에게 최소의 투자로 대규모의 경제적 이익을 창출하게 하기 위함이다. 다섯째, 행위지 국가에서 행해지는 범죄행위의 시효에 차이가 있다. 스파이는 현행범으로 체포된 행위에 한하여 처벌되고 군대로 복귀한 이후에 체포되면 과거의 간첩행위는 처벌되지 않는다.³³⁾ 범죄인인도를 요청하면 정치범불인도의 원칙을 근거로 그 인도를 거절하는 것은 당연하다. 반면에 산업스파이는 산업스파이행위를 자행한 후에 본국 또는 제3국으로 도피하였다가 다시 그 행위지 국가로 귀국한 경우에 과거의 행위로 처벌될 수 있다. 범죄인인도를 요청한 경우에 정치범불인도의 원칙을 근거로 그 인도를 거절할 수 있는 것인지 여부는 논란의 여지가 있으나 일단 행위지 국가로 인도되면 처벌된다. 위에서 설명한 사항을 도표로 정리하면 <표 2>와 같다.

<표 2> 스파이(간첩)과 산업스파이간의 같은 점과 다른 점

구분		스파이(간첩)	산업스파이
같은 점		은밀하고 비파괴·비정상적인 방법으로 활동함	
다른 점	행위지	적국	첨단산업기술정보가 소재하는 모든 국가(우호국 및 비우호국 모두가 포함될 수 있음)
	시기	전시	전시 및 평시
	입수하는 정보	국가기밀(전쟁의 승리와 직·간접적으로 연계된 군사정보)	첨단산업기술정보
	정보를 입수하는 목적	전쟁의 승리	군수산업 강화 및 대규모의 경제적 이익의 창출

33) 육전규칙 제31조.

구분		스파이(간첩)	산업스파이
	범죄행위의 시효	현행범으로 체포된 경우에 처벌되고 본국으로 복귀한 이후에 체포되는 과거의 간첩행위는 처벌되지 않음	본국으로 귀국한 이후에 행위지 국가로 인도되면 처벌될 수 있음

* 필자가 연구·분석하여 작성함

III. 산업스파이의 규제에 관한 법적 근거 및 그 내용

1. 서언

산업스파이의 목적물은 국제조약에 따르면 이미 언급한 바와 같이 미공개정보, 영업비밀 및 노하우 등으로 불려지고 있다. 문제는 산업스파이행위가 마치 전시에 스파이(간첩)와 같이 본질적으로 은밀하게 비파괴적인 활동으로 수행되고 또 자국의 이익을 위한 애국적 행위로 간주하므로 산업스파이행위의 규제에 대한 법적 근거 및 그 내용이 무엇이나 라는 점이다.

2. 법적 근거

(1) WTO/TRIPS 및 NAFTA협정

WTO/TRIPS협정 제1조 2항에 따르면 동 협정에서 지적재산권의 범주에 해당하는 카테고리에 대하여 제2부 제1절에서 제7절까지 규정해 놓고 제3부에서 민사·행정 절차와 구제, 잠정조치, 국경조치에 관한 특별요건 및 형사절차를 규정해 놓고 있다. 문제는 문학, 예술, 과학 작품, 산업활동 등과 같이 인간의 지적창작활동의 결과로 생기는 모든 무형의 소산물에 대한 권리이므로 등록 또는 공개라는 일정한 절차가 이미 종료된 상태라는 점이다. 즉 등록과 공개된 지적재산권은 침해될 가능성은 있어도 산업스파이가 은밀하고 비밀스런 방법을 동원하여 절취하고자 하는 목적물은 아니다. 따라서 산업스파이활동에 대한 규제에 대한 법적 근거는 WTO/TRIPS협정 제39조와 NAFTA협정 제1711조 및 이들 협정에서 규정하고 있는 미공개정보와 영업비밀의 보호에 관한 규정이다.

(2) 파리협약

예로부터 산업재산권은 각국의 국내법의 범주로 인정해 주고 보호해 왔었다. 그러나 교통·통신수단의 발달로 인하여 다른 국가로 전파되어 모방과 모조가 손쉽게 이루어질 가능성이 증대되었다. 따라서 선진국들은 산업재산권의 속지주의적인 성질을 수정하여 국제적으로 보호할 수 있는 제도를 확립하기 위하여 노력하였다. 그 결과가 1883년 3월 20일에 체결된 파리협약이다.³⁴⁾ 동 협약은 속지주의를 기초로 국제적으로 통일하여 보호가 가능한 사항을 조약으로 성문화시킨 것이다.³⁵⁾ 따라서 파리협약은 특허, 실용신안, 의장, 상표, 서비스마크, 상호, 원산지표지(원산지 명칭) 및 부정경쟁의 방지를 대상으로 하고 있으므로 산업스파이와 관련된 사항은 부정경쟁 방지로 볼 수 있다.

동 협약 제10조 bis에서 규정된 부정경쟁방지에 관한 내용에서 부정경쟁행위는 산업상 또는 상업상 건전한 관행에 반한 다음과 같은 행위를 말한다. 즉 금지된 경쟁행위는 ① 경쟁자의 영업소, 상품, 공업상 또는 상업상의 활동 등으로 여하한 혼란을 일으키게 하는 모든 행위, ② 거래의 과정에 있어서 경쟁자의 영업소, 상품, 공업상 또는 상업상의 활동에 관하여 신용을 해하게 할 허위의 주장, ③ 거래의 과정에 있어서 상품의 성질, 제조방법, 특징, 용도 또는 수량에 대하여 공중을 오도할 표시 또는 주장 등을 의미한다.³⁶⁾ 따라서 동 협약에서 각 당사국은 당사국의 국민이 자행할 부정경쟁행위를 억제하기 위하여 효과적인 보호조치를 취하여야 한다.³⁷⁾ 그 보호조치의 상세한 내용은 결과적으로 각국의 국내법에 위임하고 있는 상태이다. 그러므로 산업스파이의 규제에 대한 명시적인 법적 근거는 동 협약 제10조 bis를 근거로 볼 때 부정경쟁방지의 차원이고 그 구체적 내용은 각국의 국내법에 따라서 차이가 있다.

(3) 국제관습법

평시에 비우호국 또는 잠재적 적국의 영토에서 은밀하게 군사 및 정치에 관한 정

34) 동 협약은 이후에 1900. 12. 14, 1911. 6. 2, 1925. 11. 6, 1934. 6. 2, 1958. 10. 31, 1967. 7. 14 일에 각각 개정되었다. 개정된 주된 내용은 1911년에 실용신안이 새로이 보호대상이 되었고, 1925년에 부정경쟁행위의 방지규정이 강화되었으며, 1958년 서비스마크의 보호 및 1967년 발명자에 대한 우선권이 부여되었다.

35) 정동섭·황희철, 전거서, p.69.

36) 동 협약 제10조 bis (3)항

37) 동 협약 제10조 bis (1)항.

보를 입수하기 위한 목적으로 스파이를 파견하는 것을 금지하는 국제조약은 찾아볼 수 없었다. 오히려 스파이가 은밀하게 타국에서 정보수집활동을 행하는 것이 국제관습을 위반하지 아니하고 이러한 스파이활동은 장기간 지속된 국가의 관행으로 발전되어 왔다는 견해도 있다.³⁸⁾ 현실적으로 외교관계가 수립된 국가간에 외교사절로 파견된 요원이 자국을 위하여 특정 분야의 정보수집에 관한 업무를 수행하는 것은 외교관례상 어느 정도의 범위에서 묵인되고 있다.³⁹⁾ 따라서 국제관습법적인 측면에서 산업스파이의 활동을 규제할 법적 근거를 찾아보기 어렵다.

(4) UN헌장상 영토의 불가침성

산업스파이의 규제에 대한 국제법적 근거로 검토해 볼 수 있는 것은 UN헌장 2조 4항에서 무력사용금지의 원칙과 관련하여 산업스파이가 영토의 보존을 침해하였는지 여부이다. UN헌장 제2조 4항에서 모든 회원국은 다른 국가의 영토의 보전과 정치적 독립을 위해서 무력의 위협이나 행사를 삼가야 한다. 문제는 여기서 영토보전의 의미가 여하한 종류의 강제적 침입을 금지하는 불가침성으로 이해한다면⁴⁰⁾ 산업스파이는 영토의 보존이라는 불가침성을 침해하였다고 볼 수도 있다. 그 이유는 두 가지가 있다. 하나는 산업스파이는 특정 국가가 보호하고 있는 첨단산업기술정보를 절취하려는 목적으로 그 특정 국가에 입국하여 은밀하고도 비밀스럽게 활동하고 있다는 점이다. 다른 하나는 절취된 기술은 그 첨단산업기술을 보유하는 국가에게 중대한 경제적 손실을 초래할 수 있다는 점이다. 그러나 산업스파이가 외교관인 경우에 외교관은 자국의 이익을 위하여 특정분야의 정보수집에 관한 업무를 수행하는 것은 외교관례상 어느 정도의 범위에서 묵인되고 있다. 국가가 파견한 비밀요원은 특정 국가에서 산업정보수집활동을 행하는 것 자체가 국제법상 불법행위라는 법적 근거를 찾아볼 없다. 또한 UN헌장 제2조 4항에서 영토의 보전과 정치적 독립을 위해서 금지하고 있는 무력은 기동력을 지니면서 군사적인 힘으로 표출되는 다양한 형태의 군사 활동을 의미한다.⁴¹⁾ 이러한 관점에서 볼 때, 산업스파이의 활동 그 자체는 첨단산업기술정보가 소

38) Roger D. Scott, "Territorially Intrusive Intelligence Collection and International Law", Air Force Law Review, 1999, vol.46, p.218.

39) 외교사절은 정치, 경제, 군사, 여론 및 기타 모든 사정을 합법적인 방법으로 관찰하고 이것을 파견국에게 보고할 수 있다. 외교관계에 관한 비엔나협약 제3조 1항 (d).

40) Bruno Simma(ed.), The Charter of the United Nations: A Commentary, 2nd ed., vol.I (Oxford : Oxford University Press, 2002), p.123 참조.

41) 문규석, "국제법상 정보전에 관한 연구", 『국제법학회논총』, 제48권 제1호(2003. 6), pp.173-176

제하는 국가가 허용하지 아니한 방법으로 그러한 정보를 입수하였다고 하여도 영토의 보존이라는 불가침성을 침해하였다고 결론을 내릴 수 없다. 다만, 은밀하고 비정상적인 방법으로 미공개정보를 취득하였다는 점에서 UN헌장상 영토의 불가침성을 침해하였다고 보기 보다는 해당국가의 국내법을 위반하였다고 볼 수 있다.

(5) 각국의 국내법

파리협약과 WTO/TRIPS협약 당사국은 불공정 경쟁에 대한 효과적 보호를 보장하기 위하여 미공개정보와 정부 또는 정부기관에 제출된 자료는 자국의 고유한 법제도 및 관행의 범위에서 적절한 이행방법을 자유로이 결정할 수 있다.⁴²⁾ 따라서 각국은 영업비밀의 본질이 지적재산권이든 또는 재산권이든 간에 산업스파이에게 의해서 자행되는 부정경쟁행위 또는 영업비밀 침해행위를 방지하여 건전한 거래질서를 유지하기 위한 목적으로 관련 법률이 있다. 대한민국의 경우에 주된 법률은 부정경쟁방지 및 영업비밀보호에 관한 법률(이하 부정경쟁방지법)이다.⁴³⁾ 미국은 1996년의 경제스파이법(Economic Espionage Act, 18 U.S.C. §1831-1839), 독일, 일본, 스위스 및 오스트리아도 각각의 부정경쟁방지법이다.

3. 규제의 내용

산업스파이가 절취하고자 하는 목적물은 WTO/TRIPS협정 제1조 2항에 따르면 미공개정보는 지적재산권으로 보고 있고 그의 보호조치를 위한 구체적 이행방법은 제1조 1항에서 각국의 국내법에 위임시키는 숙지주의 원칙을 채택하고 있다. 파리협약도 부정경쟁방지의 차원에서 산업스파이가 산업상 또는 상업상 건전한 관행에 반하는 경쟁행위를 금지하고 각 당사국은 자국민이 자행할 부정경쟁행위를 억제하기 위하여 효과적인 보호조치를 취하여야 한다. 이러한 규제의 내용은 WTO/TRIPS협정에 따르면, 자연인과 법인은 합법적으로 자신의 통제 하에 있는 정보가 자신의 동의가 없이 건전한 상업적 관행에 반하는 방법으로 타인에게 공개되거나 타인에 의해서 획득 또는 사용되는 것을 금지하기 위한 수단을 허용하고 있다. 그 수단은 각국의 국내법상 영민사, 형사 및 행정절차를 통하여 규제하도록 하고 있다. 따라서 각국의 국내법상 영

참조.

42) WTO/TRIPS협약 제1조 1항 및 제39조 및 파리협약 제10조 bis 제(1)항 참조.

43) 동 법률은 1986. 12. 31에 법률 제3897호로 제정된 이후에 4차례(1991. 12, 1997. 12, 1998. 12, 1999. 2) 개정되었다.

업비밀의 개념상의 차이 및 영업비밀의 보호가 부정경쟁방지의 차원인지, 재산권보호의 차원인지에 따라서 산업스파이의 정의와 그 범죄행위에 대한 구성요건, 민·형사 및 행정절차를 통한 규제의 방법이 국가마다 차이가 있을 수 있다.⁴⁴⁾

4. 평가

산업스파이의 규제에 대한 법적 근거로 일반 국제법상 UN헌장 제2조 4항에서 규정하고 있는 영토의 불가침성을 위반하였는지 여부에 대하여 검토해 보았으나 영토의 불가침성을 위반하였다는 명확한 근거를 제시할 수 없었다. 반면에 국제관습은 오히려 산업스파이의 활동을 국가의 관행으로 묵인하고 있는 양상이다. 따라서 산업스파이의 활동에 대한 처벌 및 규제에 대한 법적 근거는 국제경제법과 연관해서 생각해 볼 문제이고 그 구체적 근거는 파리협약과 WTO/TRIPS 및 NAFTA협정으로 지적재산권의 보호와 연계된다.

지적재산권의 보호라는 측면에서 지적재산권은 특허권, 실용신안, 상표권, 의장권 및 기타 제 권리는 WTO/TRIPS, NAFTA, 파리협약 및 WIPO 등에서 국제적으로 보호하기 위한 기본 체제는 잘 갖추어져 있다고 볼 수 있다. 문제는 영업비밀, 미공개정보 및 Knowhow에 관한 국제적 보호체제는 속지주의적인 측면으로 사실상 이양되어 있다. 즉 특허권 및 상표권과 같이 국제적으로 등록된 지적재산권은 국제적으로 잘 보호되고 있으나 미공개정보 또는 영업비밀은 국제적으로 공개할 수 있도록 등록할 수가 없다. 따라서 비밀성이 있고 그 상업적 가치는 무한대로 확대될 수는 있는 영업비밀을 보호하기 위하여 각국은 영업비밀을 적극적으로 보호하기 위한 법적 체제를 갖추고 있다. 그 내용도 부정경쟁방지의 차원에서 보호하는 국가와 지적재산권이라는 측면에서 보호하고 있는 국가가 있다. 그러므로 산업스파이를 체포한 국가는 국제경제법상 영업비밀을 보호하기 위한 파리협약, WTO/TRIPS 및 NAFTA를 근거로 제정된 각국의 국내법으로 처벌하고 있다.

각국은 첨단산업기술정보를 비정상적인 방법으로 절취하기 위하여 산업스파이를

44) 산업스파이행위를 규제하기 위하여 한국은 부정경쟁방지법 제2조 2항에서 영업비밀의 개념을 정립하고, 제3항에서 영업비밀을 침해하는 행위에 대하여 규정하고 있다. 이외에 영업비밀에 접근할 권한이 없는 자가 비밀누설인 경우에 형법, 해킹을 통한 경우에 정보통신망이용촉진 등에 관한 법률, 첨단산업기술정보의 절취하기 위하여 도청·감청을 하는 경우에 통신비밀보호법, 신용정보업자가 기업의 영업비밀(독창적인 연구개발정보)을 수집·조사한 경우에 신용정보의 이용 및 보호에 관한 법률 및 기타에서 산업스파이행위에 관한 규제의 내용을 규정하고 있다.

첨단산업기술정보가 소재한 국가로 파견할 수 있다. 제기되는 문제는 파견된 산업스파이의 신분은 전시에 파견된 간첩과 같이 이중적 지위를 지니고 있는지? 이중적 지위를 누리고 있다면 전시의 간첩에 준하여 범죄인인도에 있어서 정치범불인도의 원칙이 적용되는 정치범으로 포함될 수 있는지 여부이다.

IV. 산업스파이의 이중적 지위에 따른 처벌 문제

1. 서언

산업스파이는 일반적으로 비정상적인 방법으로 적국 또는 우호국에서 대규모의 경제적 가치가 있는 첨단산업기술정보를 절취하여 파견자·고용주에게 그 정보를 전달하는 자라고 볼 수 있다. 따라서 파견자가 국가 또는 특정 기업이 될 수 있고, 그 행위자는 파견국의 국민으로 외교관, 비밀요원, 일반 사인, 그리고 첨단산업기술정보가 소재하는 국민 또는 제3국인이 될 수도 있다. 일반적으로 산업스파이의 파견자가 특정 국가 또는 기업이라는 관점에서 파견국의 국민이 다른 국가에서 산업스파이행위를 하는 경우에 이들이 산업스파이행위를 하던 국가에서 체포된 경우에 신분적 지위에 따른 처벌의 문제가 제기된다. 또한 그 산업스파이행위를 한 자가 본국 또는 제3국으로 도피한 경우에 범죄인인도와 관련하여 정치범으로 포함될 수 있는지 여부이다.

2. 이중적 지위

산업스파이의 법적 지위는 산업스파이가 어떠한 신분적 지위를 누리는 상태에서 산업스파이행위를 하느냐에 따라서 다를 수 있다. 먼저 파견자가 누구이냐에 대하여 살펴보면, 미국의 Annual Report 2000에 따르면, 산업스파이의 파견자는 국가와 특정 국가의 정부와 연대한 기업에 의해서 수행되는 산업스파이행위가 58%에 달한다는 것이다.⁴⁵⁾ 따라서 나머지는 42%는 ① 기업이 단독으로 사인을 고용하여 직접 파견하는 경우, ② 기업이 현지에서 고용된 사람을 사용하는 경우, ③ 사인이 특정 기업의 사주 또는 독자적으로 다른 사인을 고용하여 파견하거나 또는 현지인을 고용하여 사용하는 경우, 그리고 ④ 특정한 개인이 수집된 첨단산업정보기술을 판매하려는 목적으

45) Annual Report to Congress on Foreign Economic Collection and Industrial Espionage(2000)
<http://www.nacic.gov/fy00rpt.html> (2005. 9. 10. 방문)

로 스스로 또는 다른 사람을 고용하여 산업스파이행위를 하게 하는 경우 등도 있을 수 있다고 추정된다.

산업스파이의 신분적 지위는 파견자의 측면에서 볼 때 국가와 기업 및 일반 사인이 될 수 있다. 또 구체적으로 산업스파이행위를 할 수 있는 사람의 신분적 지위는 국가가 파견하는 경우에 외교관과 비밀요원이다. 기업 또는 일반 사인이 파견한 경우는 일반 사인이 될 수 있다. 이들의 국적은 파견자 또는 고용주의 국적과 동일한 사람, 입수하려는 산업정보가 소재하는 국가의 국민 및 제3국의 외국인이 될 수도 있다. 문제는 산업스파이행위가 본질적으로 은밀하게 수행되고 비파과적·비정상적인 방법으로 첩보를 수집하고 있다는 점이다. 따라서 산업스파이의 국적은 세 가지로 이들의 신분적 지위를 살펴볼 수 있다. 하나는 산업스파이가 파견국의 국민이라는 관점, 다른 하나는 첨단산업기술정보가 소재하는 국가의 국민, 또 다른 하나는 제3국의 외국인이 될 수 있다.

산업스파이가 파견국의 국민이라는 관점에서 살펴보면 그 산업스파이활동은 스파이(간첩)와 같이 이중성을 지니고 있고 그 산업스파이는 이중적 지위를 누리고 있다고 평가된다. 먼저 산업스파이는 다음과 같은 이유로 이중성을 지니고 있다고 생각한다.⁴⁶⁾ 그 이유는 첫째, 자국의 경제적 이익을 위하여 다른 나라에서 수행한 산업스파이활동은 애국적인 활동으로 옹호될 수 있다. 반면에 피해국은 그러한 유형의 산업스파이활동을 범죄행위로 보고 있다는 점이다. 둘째, 특정 국가에서 산업스파이활동을 하다가 발각되면 엄하게 처벌된다는 위협성을 인식하고 있다. 반면에 그러한 위협을 인식하고 있음에도 불구하고 그 위협을 감수하면서 특정한 첨단산업기술정보의 수집을 위하여 특정 국가로 파견한다는 점이다. 셋째, 각국의 국내법상 외국인이 자국 내에서 산업스파이활동을 수행하는 것을 금지하고 있다. 반면에 자국의 국내법에서 다른 나라에서 스파이활동을 수행하는 것을 금지하고 있지 않다는 점이다.

그러므로 산업스파이는 파견국의 국민이라는 관점에서 볼 때 다음과 같은 이유로 이중적 지위를 지니고 있다. 그 이유는 첫째, 파견국에서 공식적으로 인정된 요원은 아니지만 비공식적으로 인정하고 있다는 점이다.⁴⁷⁾ 둘째, 행위지 국가에서 산업스파이활동을 하다가 체포되면 엄하게 처벌되는 반면에 처벌되지 아니하면 추방된다는 점이다.⁴⁸⁾ 반면에 행위지 국가에서 산업스파이활동을 하다가 체포되지 아니하고 무사

46) Roger D. Scott, op. cit., pp.220-221 참조.

47) Robert Jennings & Arthur Watts, op. cit., pp.1176-1177 참조.

48) Ibid., p.1177.

히 파견국으로 귀국하게 되면 완전범죄가 되는 형태가 된다. 즉 쌍방가벌성의 원칙을 인정하려고 하지 아니할 것이다. 또한 산업스파이가 본국으로 귀국한 이후에 산업스파이활동을 하였다는 점이 입증되었을 때 범죄인인도를 요청하면 정치범의 한 유형으로 포함되어 인도가 거절될 가능성도 배제할 수 없다. 셋째, 산업스파이를 파견한 국가는 산업스파이활동 그 자체가 애국적인 행위로 옹호되지만 그 피해국은 자국에게 중대한 경제적 손해를 끼친 범죄자로 간주된다는 점이다.⁴⁹⁾

첨단산업기술정보가 소재한 국가의 국민이 자국에서 산업스파이행위를 하였다면 그들의 신분적 지위는 여전히 자국 국민이다. 물론 이러한 유형의 산업스파이는 특정한 분야의 정보 사냥꾼, 특정 기업에 소속된 근로자 또는 연구원이다. 또한 행위지 국가와 파견자의 국적을 제외한 제3국인이 파견자에게 고용된 경우에도 그 외국인이 단지 첨단산업기술정보가 소재한 국가에서 범죄행위를 한 것과 같다. 따라서 산업스파이의 지위는 파견국 또는 특정 기업의 소속 국민이 외국에서 산업스파이행위를 하는 경우에 한하여 이중적 지위가 인정된다.

3. 정치범의 관련성 여부

산업스파이의 이중적 지위는 이들이 산업스파이행위를 수행하는 과정에서 체포된 경우에 이들의 신분적 지위에 따라서 처벌의 문제에 차이가 있다. 먼저 서론 부분에서 열거한 사례와 같이 외교관이 산업스파이행위를 한 것으로 드러난 경우이다. 외교관은 외교관계에 관한 비엔나협약에 의해서 외교관의 면책특권이 적용되어 추방하거나 소환을 요청할 수 있으므로 이 문제는 정치적으로 해결될 것으로 예상된다. 특정 국가가 파견한 비밀요원이 외교관이 아니라 일반 사인의 신분인 경우에 체포되었다고 한다면 중한 형벌로 처벌되거나 아니면 추방될 것이다. 문제는 특정 국가가 파견한 산업스파이가 첨단산업기술정보를 절취한 이후에 파견국으로 귀국한 경우에 그 행위지 국가가 그 산업스파이에게 범죄인인도를 요청하였다면 그 산업스파이가 정치범의 범주에 포함되는지 여부이다.

정치범의 개념은 학설과 각국의 국내법상 접근방법에 따라서 차이가 있기 때문에 간단하게 정의하기 어렵다.⁵⁰⁾ 일단 정치범이 “특정 국가의 정치 질서를 변경할 정치

49) 우리의 스파이는 애국자이다(Our spies are patriots)라는 관점이다. Roger D. Scott, op. cit., p.218.

50) 신의기, 『범죄인인도제도』, 한국형사정책연구원, 1996, pp.71-92 참조; Geoff Gilbert, Transnational Fugitive Offenders in International Law (The Hague-Boston-London : Martinus Nijhoff

상의 목적으로 범죄행위를 감행하는 자”를⁵¹⁾ 의미한다고 할 경우에 산업스파이가 정치범의 범주에 포함될 것인지? 산업스파이가 정치범으로 포함될 수 있는지 여부는 두 가지 경우로 나누어서 접근하는 것이 타당하다.

첫 번째 경우는 파견국이 비밀스럽게 산업스파이를 파견한 경우이다. 이러한 경우에 정치범으로 포함될 수 있다는 긍정론의 근거는 ① 국가가 파견하는 경우에 전시에 간첩과 동일하게 이중적 지위를 누리고 있다는 점, ② 입수하고자 하는 정보의 성격이 전시의 간첩과 차이가 있다고 하더라도 궁극적으로 자국의 이익을 위한다는 점, ③ 국가가 파견하는 경우에 보통 그 국가의 비밀요원이므로 발각되는 경우에 신분적 보장을 책임질 것이라는 점 및 ④ 산업스파이행위가 자국의 이익을 위한 행위이므로 애국적 행위로 생각할 수 있다는 점 등이다. 반대로 부정론의 근거는 ① 혁명과 군사 쿠데타와 같은 정치적 활동과는 거리가 멀다는 점, ② 정치질서의 변혁을 시도하기 위한 행위가 아니라는 점, ③ 전시의 간첩과 산업스파이는 그 입수하고자 하는 정보의 성격이 다르다는 점 및 ④ 파견국이 자국의 경제적 이익을 비정상적인 방법으로 얻고자 한다는 점 등이다.

필자는 국가가 파견한 산업스파이는 정치범의 범주에 포함될 수 있다고 생각한다. 그 근거는 첫째, 정치범의 개념에 대한 특정설에 따르면 간첩죄는 정치범의 범주에 포함되고 있고,⁵²⁾ 산업스파이도 경제안보의 측면에서 전시의 간첩에 준하여 생각할 수 있다는 점이다. 둘째, 절대적 또는 순수 정치범죄의 범주에 간첩죄 또는 간첩행위가 포함되어 있으므로 산업스파이행위도 간첩행위에 준하여 생각할 수 있다는 점이다. 셋째, 특정인이 정치범인지 여부는 관행을 살펴보면 피청구국에 의하여 내려지는 것이 보통이다.⁵³⁾ 따라서 피청구국(산업스파이를 파견한 국가)은 자국이 파견한 산업스파이를 보호하기 위하여 범죄인인도를 거절하는 명분으로 정치범이라고 주장하는 것은 당연하기 때문이다. 넷째, 산업스파이행위의 금지에 대하여 국제조약과 국제관습을 찾아볼 수 없다는 점이다. 다섯째, 산업스파이행위는 행위지 국가의 국내법을 위반하였지만 파견국의 국내법은 위반하지 아니하였다는 점에서 쌍방가벌성의 원칙이 적용되지 아니한다는 점이다. 여섯째, 산업스파이행위는 파견국의 전지에서 파견

Publishers, 1998), pp.203-334 참조.

51) 김정균·성재호, 『국제법』, 박영사, 2003, p.386.

52) 김명기, 『국제법원론(상)』, 박영사, 1996, p.709; 신의기, 전게서, p.73; 김주덕, 『국제형법』, 육서당, 1998, p.214.

53) 김대순, 『국제법론』, 제9판, 삼영사, 2004, p.316.

국을 위한 애국적 행위로 볼 수 있다는 점이다.

두 번째 경우는 특정 기업이 비밀스럽게 산업스파이를 파견한 경우이다. 이 경우에도 국가가 파견한 산업스파이와 준하여 정치범의 범주에 포함된다고 주장할 수 있다. 그러나 ① 사경제의 주체인 특정 기업이 그 기업의 경제적 이익을 얻기 위한 목적으로 파견하였다는 점, ② 그 산업스파이는 파견자가 요청한 정보를 제공하여 준대가로 특정한 액수의 금액을 받기로 계약할 수 있다는 점, ③ 특정한 액수의 금액을 받기로 계약하였다는 측면에서 볼 때 국가가 파견한 산업스파이와 본질적으로 그 성격이 다르다는 점, ④ 위의 이유로 인하여 전시의 간첩과 같이 이중적 지위를 누리고 있다고 인정하기 어렵다는 점 등이 있다. 따라서 기업이 파견한 산업스파이는 정치범의 범주에 포함될 수 없다. 마찬가지로 산업스파이가 파견국의 국민이 아니라 첨단산업기술정보가 소재한 국가의 국민 또는 제3국의 외국인이 특정 국가(기업)에게 고용되어 산업스파이행위를 하는 경우에도 정치범의 범주에 포함될 수 없다. 그 이유도 그 산업스파이는 주로 자신의 경제적 이익을 위하여 산업스파이행위를 하였다고 볼 수 있으므로 이중적 지위가 인정되지 아니하기 때문이다. 그러므로 기업이 파견한 산업스파이의 국적이 어느 국가라고 할지라도 피해국이 그 산업스파이가 소재하는 국가에게 그를 인도하라고 요청하면 그가 소재한 국가는 정치범이라는 이유로 인도를 거절하지 말아야 한다.

4. 평가

첨단산업기술정보가 경제안보라는 관점에서 볼 때 국가기밀로 볼 수 있다. 반면에 국가기밀의 의미가 군사적 측면을 강조할 경우 및 국가안전에 대한 중대한 불이익을 침해하였다는 측면으로 이해할 경우에 첨단산업기술정보가 국가기밀로 포함된다고 보기 어렵다는 측면이 있다.⁵⁴⁾ 그 이유는 ① 첨단산업기술정보는 주로 경제적 이익을 위한다는 점, ② 산업스파이의 국제적 규제에 대한 근거를 국제경제법적인 측면에서 찾아볼 수 있으나 그 규제의 구체적인 내용은 각국의 국내법에 위임되어 있다는 점, ③ 산업스파이의 규제에 관한 부정경쟁방지법의 견지에서 볼 때도 비파괴·비정상적인 방법으로 활동한다는 측면에서 간첩과 비슷하지만 그 내용이 주로 경제적 이익을 목적으로 수행된다는 점 등이 있기 때문이다. 따라서 첨단산업기술정보를 절취당한 피해국의 견지에서 범죄행위로 보고 있는 반면에 파견국은 자국의 이익을 위한 애국적

54) 국가보안법 제4조 참조.

행위로 보고 있다.

산업스파이행위를 자행한 자에 대한 처벌의 문제는 그 산업스파이가 행위지 국가에서 체포되는 경우에 신분상의 지위 및 그 파견자가 누구인지에 따라서 다르게 접근해야 한다. 즉 국가가 파견한 산업스파이가 외교관인 경우는 외교관의 신분적 특권으로 인하여 처벌할 수 없고 다만 소환요청 또는 추방과 같은 조치가 필요할 뿐이다. 반면에 신분상의 지위가 파견국의 비밀요원인 경우에 파견국과 그 체포한 국가는 비밀리에 협상을 하여 정치적으로 처리할 것으로 예상된다.⁵⁵⁾ 그러나 기업 또는 사인이 파견한 경우는 첨단산업기술이 소재한 국가가 자국의 국내법에 따라서 처벌할 것이다. 특정 분야의 기술자가 외국 기업이 제시한 조건으로 첨단산업기술을 제공하고 해외로 도피한 경우도 정치범의 범주에 포함되지 아니한다. 특히 자국 국민이 금전을 매개로 최첨단산업기술정보를 경쟁상대국에게 제공한 경우에 자국에게 상당한 손실을 야기하였다는 점에서 끝까지 추적해서 처벌하여야 한다.⁵⁶⁾ 반면에 국가가 파견한 산업스파이는 전시에 적국 또는 적국의 동맹국에 파견한 스파이와 같이 이중적 지위를 누리고 있으므로 정치범의 범주에 포함될 수 있다.

V. 결론

평시에 정보 수집을 목적으로 다른 나라에 스파이를 은밀하게 침투시키는 것은 영토의 보존의 원칙과 잠정적으로 충돌하지만 국제법은 명백하게 스파이활동을 특별히 금지하고 있지 않다. 그러나 분명한 사실은 그러한 스파이활동은 피해국가의 국내법을 위반하게 되므로 피해국의 국내법으로 처벌된다. 평시에 파견된 산업스파이도 경제안보라는 측면에서 볼 때 다른 국가의 영토 내에서 정보수집활동은 다른 국가의 영토에 대한 불가침성을 존중하지 아니하였다는 점에서 불법적인 간섭이라는 견해도 있다.⁵⁷⁾ 문제는 어떠한 국제조약도 평시에 행해지는 스파이활동이 합법성을 지니고

55) 물론 국가가 비밀리에 파견한 산업스파이가 행위지 국가에서 체포된 경우에 국가책임이 제기될 수 있다. 문제는 산업스파이행위는 명시적으로 국제조약 및 국제관습법을 위반한 것이 아니고 다만 행위지 국가의 국내법을 위반하였다는 점이다. 따라서 행위자 자체에 대해서는 행위지 국가의 국내법에 따른 처벌이 가능하지만 산업스파이행위의 금지와 같은 국제의무의 연원이 없으므로 국가책임은 성립되지 아니한다고 생각한다.

56) 국가정보원이 삼성전자의 기술을 유출한 산업스파이를 6년여 동안 추적한 후에 그 자를 인도해 온 사례가 있다. 문화일보, 2004. 11. 25(제3판), p.16.

57) Roger D. Scott, op. cit., p.219.

있다고 말하지 아니한다는 점이다.⁵⁸⁾ 외국에서 행해지는 정보수집활동이 국제법을 위반하였다는 진지한 제안도 행해진 적이 없다는 점이다.⁵⁹⁾ 국제관습도 은밀하고 비파괴적인 정보수집활동이 불법적인 행위라고 지적하지 아니하고 오히려 장기간 지속된 국가의 관행으로 발전되어 왔다고 보고 있다. 미국도 은밀하고 비파괴적인 정보수집 활동에 대하여 긍정하고 있고,⁶⁰⁾ 은밀하고 비파괴적인 정보수집활동을 금지하는 조약의 당사국이 아니다.⁶¹⁾ 이 점은 우리나라도 마찬가지이다.

무력충돌에서 스파이는 적의 전술전략을 간파하여 그에 대한 효과적인 대응책을 수립하기에 매우 유용하다. 물론 자국을 이롭게 할 수 있는 모든 정보를 수집하기 위한 그들의 활동은 상당한 정도의 위험을 부담하고 있다. 반면에 그들의 활동이 성공하는 경우에 무력충돌에서 승리로 이끄는 견인차의 역할을 수행한다는 것은 두말할 필요가 없다. 사실상 스파이활동은 여러 세기 동안에 국가들에 의해서 관행적으로 수행해 왔다. 반면에 각국은 자국 내에서 자국의 이익에 반한 스파이활동에 대하여 엄하게 처벌하는 국내법을 제정하였다. 산업스파이도 결국은 경제안보라는 관점에서 자국의 경제적 이익을 획득하기 위한 목적으로 파견된 비밀요원으로 본다면 전시의 간첩과 동일한 선상에서 바라보아야 한다. 다만, 첨단산업기술정보가 소재하고 있는 국가의 입장은 방어적 상태에 있으므로 산업스파이의 진압을 위한 활동은 파견자가 누구이고 그 사람이 어떠한 신분적 지위를 누리고 있는지 여부를 근거로 이원적으로 접근하는 것이 바람직하다. 즉 외국이 파견한 산업스파이가 외교관 또는 비밀요원인 경우에 쌍방가벌성의 원칙이 적용되지 아니하고 정치범과 동일하게 취급할 수밖에 없다. 반면에 외국 또는 외국의 특정 기업의 지시로 제3국인 또는 자국민이 자국의 영토에서 산업스파이행위를 하는 경우에 일반 보통범죄와 같이 취급하여 처벌하여야 한다.

그러므로 산업스파이의 예방 및 처벌과 관련하여 다음과 같은 사항을 강조하고자 한다. 첫째, 비록 우리나라가 기술무역에 있어서 적자상태에⁶²⁾ 있다고 하더라도 반도체 및 정보·통신 분야에서 비교적 세계 최고 수준의 기술을 보유하고 있는 것으로 알

58) Ibid., p.218.

59) Ibid., p.220.

60) Ibid.

61) Ibid., p.217.

62) 과학기술부가 발표한 '2004년도 기술수출 및 기술도입 실적'에 따르면 2004년 기술수출은 14억 1600만 달러, 기술도입은 41억 4800만 달러로 27억 3200만 달러의 적자를 나타냈다. 동아일보, 2005. 7. 13(제45판), p.B1.

고 있다. 따라서 기술개발을 위한 투자도 중요한 만큼 개발한 첨단산업기술정보가 유출되지 아니하도록 잘 지키는 것이 매우 중요하다. 둘째, 첨단산업기술정보인 경우에 그러한 기술정보를 보유한 회사뿐만 아니라 경제안보라는 관점에서 산업기밀 보안활동이 전개되어야 한다. 셋째, 산업스파이행위는 전시의 스파이활동과 같이 이중성을 지니고 있으므로 예방만이 최선의 정책이다. 넷째, 국내법상 영업비밀의 범위를 어느 정도까지 인정할 것인지에 대하여 명확한 한계 또는 해석의 범위를 정하여야 한다. 즉 근로자가 별 문제가 아니라고 생각한 부분이 법 해석에 따라서 기밀로 둔갑할 수 있다. 예를 들면, “노트북 PC에 회사 자료 하나 없는 엔지니어가 어디 있겠는가? 회사가 양심을 품으면 처벌 못할 직원이 없을 것이다”라는 점이다.⁶³⁾ 따라서 영업비밀의 범주를 명확히 하여 애매한 피해자가 나타나지 않도록 하여야 한다. 다섯째, 국제법적인 측면에서 산업스파이의 규제를 위한 국제규범을 제정하다는 것은 사실상 불가능하다.⁶⁴⁾ 그 이유는 세 가지가 있다. 하나는 무엇이 산업스파이행위인지에 대하여 Echelon 및 스파이위성과 같이 첨단정보통신기술이 접목되어 있는 선진국과 그러한 기술이 없는 개발도상국간에 견해 차이가 너무 크다는 점이다. 다른 하나는 국제관습상 은밀하고 비파괴적인 정보수집활동은 장기간 지속된 국가의 관행으로 보고 있다는 점이다. 또 다른 하나는 국가간에 첨단산업기술정보의 개념과 범위 및 무엇이 비정상적이고 비합리적인 산업스파이행위의 주된 요소인지에 대하여 상세하게 정립하기가 쉽지 않다는 점이다. 따라서 역시 예방만이 최선의 정책이다. 여섯째, 산업스파이행위자에 대한 진압 대책은 산업스파이가 자국민인 경우와 외국인 경우로 이원화하여 접근하여야 한다. 먼저 자국민이 산업스파이행위를 하는 경우이다. 이 경우는 대부분이 금전적 이익을 목적으로 그러한 행위를 한 것으로 추정되므로 끝까지 추적해서 처벌해야 한다. 해외로 도피하였다면 법무부는 해당국가에게 범죄인인도를 요청하고 경찰은 인터폴의 적색수배서 발행하여 강제로 송환하여야 한다. 산업스파이가 외국인이고 그 외국인이 외교관과 비밀요원인 경우에 사후적 조치는 사실상 불가능하므로 역시 사전적 예방조치만이 유일한 방법이다. 다만, 비밀요원이 행위시에 체포된 경우는 국내법에 따라서 처벌하거나 또는 추방조치를 취하여야 한다. 또 그 외국인이 일반사인이고 해외로 도피하였다면 법무부와 경찰은 자국민과 동일시하여 강제

63) 주간동아, “산업스파이냐 해외 취업이냐”, 제465호, 2004. 12. 23, p.17.

64) 산업스파이 방지를 위한 조약의 필요성은 공감하여 논의한 적은 있으나 차선책에 그치고 있다. 즉 부패한 거래관행을 중단하기 위하여 공무원 및 관련된 자에게 뇌물을 준거나 또는 비정상적인 거래관행을 방지하기 위한 노력으로 한정되어 있다. Karen Sepura, op. cit., pp.146-147 참조.

로 송환하여 처벌하여야 한다. 일곱째, 산업스파이의 문제에 대한 예방적 조치는 첨단산업기술을 보유한 회사의 내부적 측면과 관계 당국의 보안체계의 강화로 요약이 된다. 따라서 관련 회사는 먼저 내부자에 의하여 첨단산업기술정보가 유출되지 않도록 윤리의식 고취, 보안체제 구축, 인증메커니즘, 데이터의 암호화 및 기타 등이 요청된다.⁶⁵⁾ 반면에 관련 기관은 보안검사 및 기타 필요한 예방적 조치를 취하여야 한다.



▶ 문규석

산업스파이(industrial espionage), 경제스파이(economic espionage), 영업 비밀(trade secret), 간첩(spy), 파리협약(Paris convention), 산업정보(intellectual property), 미공개정보(undisclosed information)

65) 노시영, “기술유출 방지를 위한 정보시스템 보안 방향”, 국가정보원, 『산업보안 연구논총』, 창간호, 2004. 11, pp.191-243 참조.

[초록]

국제관계에서 경제문제가 차지하는 무게중심이 점차 확대됨으로 인하여 비정상적인 방법으로 첨단산업기술정보를 획득하기 위하여 산업스파이의 활동이 치열하게 전개되고 있다. 반도체 및 정보통신기술에서 우위를 점하고 있는 대한민국의 경우도 예외가 아니다. 문제는 평시에 국가가 파견한 간첩의 문제에 대하여 국제법적인 규범이 없는 것과 유사하게 산업스파이의 규제에 대한 국제법적인 근거 자체가 미약하다는 점이다.

국제경제의 활성화와 더불어 산업재산권에 관한 파리협약 및 WTO/TRIPS협정에 의하여 부정경쟁방지에 관한 규정이 있다고 해도 그 보호방법은 각 회원국의 법체계와 관행의 범위 내에서 적절한 이행방법을 결정할 수 있도록 허용하고 있다. 따라서 그 첨단산업기술을 보호하기 위한 방법과 그 보호정도는 국가에 따라서 다르다. 그러므로 산업스파이의 개념 속에 다음과 같은 사항이 포함되어 한다: 파견자가 누구인지, 파견된 자의 신분적 지위는 무엇인지, 목적물은 대규모의 재산적 가치가 있는 것으로 추정되어야 하며, 취득 방법은 법적으로 비난받을 수 있는 비정상적인 방법을 이용하여야 한다.

산업스파이의 규제에 관한 법적 근거는 WTO/TRIPS협정 제39조, NAFTA협정 제1711조, 파리협약 제10조 bis 및 각국의 국내법으로 볼 수 있다. 그 외에 UN헌장 제2조 4항을 근거로 영토의 불가침성 및 국제관습을 근거로 산업스파이에 대하여 규제가 가능한지 여부에 대하여 검토해 보았으나 그 근거를 제시하기에는 부정적으로 보였다. 따라서 산업스파이의 규제의 내용은 사실상 각국의 국내법에 위임되어 있는 것이 현실이다. 그러므로 산업스파이가 전시의 스파이(간첩)와 이중성 지위를 누리고 있다는 점을 고려할 때 산업스파이의 처벌에 관한 문제가 제기되고 그 핵심은 산업스파이가 정치범의 범주에 포함될 수 있는지 여부이다.

[Abstract]

Industrial Espionage from the Standpoint of International Law

Moon, Kyu-Seok

The activity of industrial espionage due to gradually expand the relative importance of economic issues in international relation is displaying intensively in order to gain advanced technology-information. Korea which takes priority of semiconductor and information-communication technology is not a calm area excluded from the activity of industrial espionage. The problem is that there is not any firm legal ground from the standpoint of international law on the regulation of industrial espionage. It is similar not to have any legal ground on the activity of spy in peace time.

Even though Paris Convention(Paris Convention for the Protection of Industrial Property) and WTO/TRIPS(Agreement on Trade-Related Aspects of Intellectual Property Rights) have provisions on unfair competition, member states shall be free to determine the appropriate method of implementing the provisions of both agreements within their own legal system and practice. That's why the protection method and level of advanced industrial technology differs from state to state. Therefore, the definition of industrial espionage should be contained as following elements: who is a seconding state of industrial espionage?, what is the legal status seconded?, the objects to be stolen must be presumed to have large-scale property value, and the way to get the information use unfair methods responsible for legal blame.

Legal ground on regulation of industrial espionage considers to be article 39 of WTO/TRIPS, article 1711 of NAFTA, Article 10bis of Paris Convention, and municipal law of individual state. I have checked it out to be legal

grounds whether industrial espionage can be regulated by the inviolability of territorial integrity based on article 2(4) of United Charter and international customary law, but the answer is negative. Therefore, contents of regulation of industrial espionage, in fact, is entrusted to each individual state. Consequently, it raises issues related to punishment of industrial espionage because an industrial espionage considers to enjoy double status just as a spy has in war time. And the most critical issue raised related to it is the point of whether or not to be contained with category of political offence