https://doi.org/10.33778/kcsa.2022.22.3.041

기술유출 형사사건의 처리 실태와 개선 고려사항 논의: 무죄사건을 중심으로

황 경 준*, 권 헌 영**

요 약

기술보호의 중요성이 날로 강조됨에 따라 기술보호를 위한 다양한 보호조치들이 수행되고 있으나 기술유출을 위한 시도가 끊이지 않고 있으며 이에 대한 대안으로 기술유출 범죄에 대해 보다 강력한 처벌이 사회적으로 요구되고 있는 실정이다. 이러한 사회적 요구에 맞춰 그간 꾸준히 처벌 기준이 상향되어 왔으며 현재도 추가적인 강화 내용을 담은 입법안들이 국회에 계류 중인 상황이다. 하지만 범죄에 대한 억제력을 실질적으로 제고하기 위해서는 처벌 기준을 강화하는 것만으로는 충분하지 않으며 처벌의 확실성이 높아졌을 때야 비로소 그 효과를 온전히 발휘될 수 있다. 따라서 본 논문에서는 처벌 자체의 강화적인 부분보다는 현 제도 하에서 처벌의 확실성을 높이기 위한 방안을 모색하는데 초점을 맞췄으며 이를 위해 기술유출 형사사건 중 무죄 사건을 중심으로 사례 및 원인을 유형별로 분석함으로써 기술유출 형사사건에서의 무죄율이 일반 형사사건 대비 높은 이유를 도출해보고 이를 토대로 부당한 무죄사건을 줄이기 위한 개선 고려사항들을 논의하고자 하였다.

Discussion On the Status and Improvements For Technology Leakage Crimes: Based on Acquittal Case

Kyung Joon Hwang*, Hun Yeong Kwon**

ABSTRACT

As the importance of technology protection is emphasized day by day, various protection measures are being carried out to protect technology. But attempts to leak technology are continuing. As an alternative to this, stronger punishment is socially required for technology leakage crimes. In response to these social demands, the standard for punishment has been steadily raised. Legislative bills containing additional reinforcement are still pending in the National Assembly. However, in order to substantially enhance the deterrence against crime, it is not enough to strengthen the punishment standards. The effect can only be fully exercised when the certainty of punishment increases. Therefore, this paper focused on seeking ways to increase the certainty of punishment under the current system rather than the reinforcement of the punishment itself. The purpose of this study was to derive the reason why the innocence rate in technology leakage criminal cases is higher than that of general criminal cases by analyzing cases and causes of innocent cases in technology leakage criminal cases. Based on this, I discussed improvement considerations to reduce unfair acquittal cases.

Key words : Technology leakage, Industrial technology, Trade secrets, National core technology, Technology protection

접수일(2022년 8월 20일), 수정일(2022년 9월 21일), 게재확정일(2022년 9월 27일)

* 고려대학교 정보보호대학원 융합보안학과(주저자)
** 고려대학교 정보보호대학원(교신저자)

1. 서 론

최근 산업기술의 급격한 발전과 함께 기술을 무기로 한 국가 간의 패권 경쟁이 가속화되고 있는 실정으로 과거 국방, 안전 분야에서 주로 사용하던 '기술 패권(Technology Sovereignty)'이라는 용어가 경제, 산업 분야로 확대되었으며 특히 반도체, 5G, 디스플레이 등 첨단산업 분야 기술에 대한 우위 선점을 위한 경쟁국 간의 기술 패권 확보 노력이 갈수록 치열해지는 상황이다[1][2].

이에 따라 미국, 일본, EU 등 주요국들은 이러한 자국 기술의 유출에 대해 기업 차원의 문제를 넘어 국가 경제 및 안보의 문제로 인식하고 이를 방지하고자 법적 처벌 강화, 외국인에 의한 기술 관련 투자 및 인수·합병 제한, 기술수출 통제 등 다양한 노력을 기울이고 있다.

우리나라도 기술보호와 관련한 대표적인 법률로 「부정경쟁방지 및 영업비밀에 관한 법률」(이하 "부정경쟁방지법")과 「산업기술의 유출방지 및 보호에 관한 법률」(이하 "산업기술보호법")이 존재하며(국가첨단전략기술 및 전략기술 취급인력 등을 종합적으로 통제, 보호하고 국내산업의 글로벌 경쟁력 제고 기반 마련을 위한 「국가첨단전략산업 경쟁력 강화 및 보호에 관한 특별조치법」이 2022. 2. 3 제정) 여러 차례의 개정을 통해 벌칙규정(법정형)을 상향하는 동시에 산업 환경 및 국내외 기술수준 등을 고려한 국가핵심기술을 지정하여 관련 기술 보유기관에 대한 외국인의 인수·합병을 승인하는 제도를 운용하고 관련 전문인력에 대한 이직 관리 및 비밀유지 계약을 의무화하는 등의 제도적 보호조치를 다각도로 수행하고 있으나 기술유출 시도가 끊이지 않고 발생하고 있다.

국가정보원에 따르면, 최근 5년간(2017 - 2022. 2) 적발한 국내 산업기술의 해외 유출 시도가 99건에 달하며 유출될 뻔했던 기술 99건은 디스플레이 19건, 반도체 17건, 전기·전자 17건, 자동차 9건, 조선·통신·기계 관련 기술이 각 8건으로 모두 우리나라의 주력산업 기술이었고 이중 국가핵심기술이 34건이나 포함되어 있었는데 해당 기술들이 해외로 유출되었다고 가정하였을 때 추산된 피해규모만 약 22조 원에 달한다고 발표하였다[3]. 특히 국가핵심기술에 대한 해외 유출시도는 2017년 3건에서 2018년 5건, 2019년 5건, 2020년 9건, 2021년 10건으로 지속 증가하는 추세를 보인다는 점에서 앞서 언급한 다양한 제도적 보호조치의 범죄억제력이 충분하지 않다고 추론해 볼 수 있다.

<표 1> 산업기술 해외 유출시도 적발현황(최근5년)

년도	산업기술	국가핵심기술
2017년	24	3
2018년	20	5
2019년	14	5
2020년	17	9
2021년	22	10
2022년(~2월)	2	2
합계	99	34

범죄 억제력은 '범죄로부터 얻을 수 있는 이익보다 범죄사실이 발각되었을 때 받게 되는 피해와 그 리스크(Risk)가 확실하게 높다'고 인식되어야 적절하게 작동할 수 있는데 다툼의 여지가 많은 기술유출 사건의 특수성 및 수사·공판 과정의 절차적 한계 등으로 인해 일반 형사사건 대비 상당히 높은 비율로 무죄 처리되는 현재 상황에서는 기술유출 범죄를 억제하기 어려워 보인다[4].

따라서 이 연구에서는 기술유출 형사사건의 무죄 사례 및 원인을 유형별로 분석해 봄으로써 기술유출 형사사건에서의 무죄율이 다른 형사사건 대비 높은 이유를 도출해보고 부당한 무죄 사건을 줄이기 위한 개선 고려사항들에 대해 논의하는 것을 중심으로 논문을 전개하고자 한다.

2. 기술유출 형사사건의 처리 실태

2.1 기술유출 관련 글로벌 동향

세계는 첨단기술의 패권을 선점하기 위한 미·중 간 기술경쟁이 장기화되고 있는 국면이며 미·중 외 주요국에서도 보호무역주의의 기조가 강화되고 있는 실정이다[5]. 기술은 국가간 패권 경쟁에서 항상 중요한 역할을 차지했는데 현대의 기술경쟁이 과거와 차별화되는 점은 기술의 변동 및 혁신

의 속도가 과거와는 비교할 수 없을 정도로 빨라짐에 따라 어느 국가도 기술 우위에 대한 확신을 갖기 어렵다는 점이다[6]. 또한 과거 군사 부문을 중심으로 한 냉전시대의 미·소 경쟁과는 달리 다양한 이슈와 분야, 차원을 아우르는 복합 경쟁이라는 점에서 '혁신 냉전(Innovation cold war)'이라고도 불린다[7]. 이러한 미·중간 기술경쟁이 대두된 근본 원인을 살펴보면 중국의 무서운 기술 추격이라고 할 수 있는데 5G 통신장비로 촉발된 기술경쟁은 반도체, 배터리, AI, 퀀텀 컴퓨팅 등 다양한 분야로 확대되고 있는 추세이다[8].

미·중을 중심으로 한 기술 패권 경쟁은 미국과 중국이 상대국의 기술경쟁력 강화를 존재적 위협으로 인식한다는 점에서 갈등이 불가피한 측면이 있는데[9][10][11] 특히나 상대적으로 기술 후발국이었던 중국의 경우 2050년까지 글로벌 과학기술 혁신강국을 건설하겠다는 목표의 '중국제조 2025'라는 중장기 국가전략을 추진하는 과정에서 신속한 시장진입, 개발 리스크 완화 등을 위해 사이버 해킹, 산업스파이, 인수·합병, 핵심 기술인력 영입 등 불법과 합법을 넘나드는 무차별적인 기술탈취 행위를 자행하고 있는 상황이다. 현재와 같은 속도로 중국의 기술 부상이 지속될 경우 2030년대에는 중국이 미국을 추월할 것이라는 전망이 제시되기도 하는데[8] 이러한 환경하에서 미국을 중심으로 주요국들은 동맹을 강화하는 등의 방법으로 중국의 기술탈취 행위에 대한 전략적 대응을 한층 강화하고 있다.

<표 2> 미국 중심의 경제・안보 관련 동맹 현황

명칭	출범시기	주요 내용
IPEF	'22. 5월	인도태평양 지역에서 중국의 경제영향력 확대를 억제하기 위해 출범한 다자 경제협력체
Chip4	'22. 3월 (제안)	동맹국간 안정적 반도체 공급망 형성을 목적으로 미국이 한국, 일본, 대만에 제안한 동맹
AUKUS	'21. 9월	미국이 인도태평양 지역의 안보 증진 목적으로 영국, 호주와 함께 출범한 외교안보 협의체
QUAD	'21. 3월 (첫 정상회담)	중국을 견제하는 공동의 목표를 기반으로 하는 미국, 일본, 인도, 호주 4자간 안보협의체

우리나라 역시 반도체, 디스플레이, 배터리, 조선 등 업종에서 세계적인 기술경쟁력을 보유한 기술유출의 주요 타깃 국가이며 최대 우방국이자 동맹국인 미국의 중국 배제 기조가 한층 강화되고 있는 상황에서 미국이 주도하는 중국 견제 노선에 참여하는 것이 일면 타당하나 중국은 우리나라의 최대 무역 상대국으로 관세청 통계에 따르면 2021년 대중국 수출 규모는 1,629억 달러로 2위인 미국(959억 달러)의 약 1.7배에 달하며 이는 전체 수출의 25.3%를 차지한다는 점에서 일방적으로 한 국가에 협조적인 태도를 취할 경우 발생할 경제적 강압으로 인한 피해를 고려하지 않을 수 없기에 국익을 중심으로 한 전략적인 대응에 대한 검토가 필요한 상황이다[6].

이런 혼란한 국제 정세 속에서 국가의 국제정치적 대응전략을 수립하는 것과는 별개로 기업 등 산업 현장에서 끊임없이 발생하고 있는 기술유출 범죄에 대한 실질적인 억제력을 제고하기 위한 자구적 노력이 그 어느 때보다 절실히 필요한 시점이라고 하겠다.

2.2 법정형 및 무죄 현황

2.2.1 법정형 관련

우리나라는 2019년을 기점으로 기술유출 관련 법정형이 전체적으로 상향되었는데 부정경쟁방지법은 2019년 1월 8일 개정에 따라 영업비밀의 국외유출은 15년 이하의 징역 또는 15억 원 이하의 벌금(기존 10년 이하의 징역 또는 1억 원 이하의 벌금), 국내유출은 10년 이하의 징역 또는 5억 원 이하의 벌금(기존 5년 이하의 징역 또는 5천만 원 이하의 벌금)에 처하도록 법정형이 상향되었으며 산업기술보호법의 경우, 2019년 8월 20일 개정에 따라 국가핵심기술의 국외유출죄가 3년 이상의 유기징역과 15억 원 이하의 벌금 병과로 신설되었고, 산업기술의 국외유출은 15년 이하의 징역 또는 15억 원 이하의 벌금(2019년 이전과 동일), 산업기술의 국내유출은 10년 이하의 징역 또는 10억 원 이하의 벌금(기존 7년 이하의 징역 또는 7억 원 이하의 벌금)에 처하도록 상향되었다.

<표 3> 기술유출 형사사건 관련 법정형 변화 현황(2019년 개정 기준)

구분	부정경쟁방지법				산업기술보호법					
	국외유출		국내유출		국외유출				국내유출	
					국가핵심기술		산업기술			
	기존	현행	기존	현행	기존	현행	기존	현행	기존	현행
징역	10년 이하	15년 이하	5년 이하	10년 이하	(신설)	3년 이상	15년 이하	15년 이하	7년 이하	10년 이하
벌금 (원)	1억 이하	15억 이하	5천만 이하	5억 이하		15억 이하	15억 이하	15억 이하	7억 이하	10억 이하

이는 미국, 중국, 일본 등 주요 국가들의 기술유출 관련 법정형과 비교해 보았을 때도 벌금 측면에서 최대 금액이 다소 낮아 보이긴 하지만 전반적으로 유사한 수준으로 법정형 자체가 절대적으로 부족하다고 판단하기에는 어려운 부분이 있다[12].

하지만 법정형을 상향하려는 시도가 지속되고 있으며 현재도 국가핵심기술에 대한 국외 유출범에 대해 무기징역 또는 최소 10년 이상의 유기징역에 처하도록 하는 내용을 담은 입법안 등이 국회에 계류 중이다(의안번호 2105544, 황운하 의원 등 10인).

<표 4> 주요 국가별 기술유출 범죄 관련 법정형

구분	국외유출		국내유출	
	최대징역	최대벌금	최대징역	최대벌금
미국	15년	$1,000만 (120억 원)	10년	한도 미규정
중국	10년	500만 위안 (9.6억 원)	10년	500만 위안 (9.6억 원)
일본	10년	10억 엔 (97억 원)	10년	5억 엔 (48억 원)
대만	12년	NT$ 1억 (43억 원)	5년	NT$ 0.1억 (4.3억 원)

2.2.2 무죄 현황 및 사유

대법원 사법연감(2021)에 따르면 부정경쟁방지법과 산업기술보호법 위반으로 처리된 형사사건 제1심을 기준으로 할 때, 법원이 2015년부터 2020년까지 처리한 사건은 총 835건이다[4]. 이 중 집행유예가 301건(36.05%)으로 가장 많았고 벌금형이 215건(25.75%), 징역형이 83건(9.94%), 그 외 선고유예, 공소기각 등이 45건(5.39%)을 차지하였으며 특이점으로 무죄가 무려 191건(22.87%)을 차지하였는데 이는 2015년부터 2020년 전체 형사사건의 1심 무죄율 평균이 3.64%인 것에 비해 약 6배나 높은 수치이다. 특히 무죄율이 높은 이유에 대해서는 우리나라 관련법들이 기술유출 행위에 대한 처벌 자체에 집중한 나머지 행위유형의 불법성이 충분히 드러나지 않고 불명확한 구성요건이 많다는 점 등이 지적되고 있으며 유죄의 경우에도 기술유출 범죄는 화이트칼라 유형의 범죄로 대부분 초범인 경우가 많고, 상습범죄 발생비율이 낮다는 점 등을 참작하여 감형 또는 집행유예가 되는 사례가 많다는 점 등이 문제로 지적되고 있는 실정이다[4][13][14][15][16][17].

<표 5> 기술유출 및 일반 형사사건 무죄율 비교

구분	기술유출 형사사건			일반 형사사건		
	처리 사건	무죄 사건	비율 (%)	판결 인원	무죄 인원	비율 (%)
2015	123	18	14.63	230,559	11,858	5.14
2016	136	49	36.03	243,781	9,080	3.72
2017	173	34	19.65	244,489	8,916	3.65
2018	171	45	26.32	220,123	7,496	3.41
2019	119	31	26.05	218,510	6,868	3.14
2020	113	14	12.39	227,920	6,267	2.75
총계	835	191	22.87	1,385,382	50,485	3.64

2017년부터 2019년 기간 동안 영업비밀 침해행위 관련 부정경쟁방지법 위반 피고인의 행위유형별 무죄 사유를 정리한 특허청(2020) 자료에 따르면, 무죄 사유 중에는 영업비밀로 인정받기 위해 충족되어야 하는 3가지 요건인 비공지성, 경제적 유용성, 비밀관리성[18] 중 비밀관리성 불인정이

압도적으로 다수(169건, 49.56%)를 차지하였으며 비공지성 불인정이 69건(20.23%), 경제적 유용성 불인정이 66건(19.36%)으로 높은 비율을 차지하였다[19].

이에 따르면 영업비밀성 자체가 부정된 무죄가 전체의 89.15%(304건)를 차지하였는데 이 수치만 보더라도 기술유출 형사사건에서 유죄 판결을 위해서 유출된 기술의 영업비밀 여부를 인정받기부터도 상당히 어렵다는 사실을 쉽게 유추해 볼 수 있다.

2.3.1 영업비밀성 부정

2006도9022 사건에서 법원은 피고인이 중국계 동종업체로 이직하는 과정에서 'Confidential'이라는 비밀 표시가 기재된 사업제안서 등이 포함된 CD 3장 분량의 사내 자료를 무단 유출한 사실은 인정되나 해당 자료들이 거래처 배포용 등으로 제공된 적이 있으며 내용 중 일부가 피해회사의 홈페이지에도 공개되어 있고, 문서의 내용이 기술적으로 중요한 정보가 기재되어 있다기보다는 구성과 기능상 특징에 관하여 개괄하고 있는 것에 불과하여 보유자가 경쟁 상의 이익을 얻을 수 있는 정보라고 할 수 없다는 점에 비추어 볼 때 유출된 자료는 영업비밀의 성립요건인 비공지성과 경제적 유용성을 가진다고 할 수 없는 것이므로 영업비밀에 해당하지 않아 원심판결을 파기하고 무죄를 선고하였다.

<표 6> 영업비밀 침해 관련 피고인의 행위유형별 무죄 사유(특허청)

행위유형		비공지성	경제적 유용성	비밀관리성	부정한 목적	기타	합계
국외 침해	취득	-	-	-	1	-	1
	사용	2	4	4	-	-	10
	누설	2	4	2	-	-	8
국내 침해	취득	20	15	45	6	7	93
	사용	31	29	84	4	10	158
	누설	14	14	34	5	4	71
총계		69	66	169	16	21	341

또한 영업비밀로 인정을 받았으나 '부정한 이익을 얻거나 대상 기관에 손해를 입힐 목적'이 충분히 증명되지 않은 사유로 인한 무죄가 16건(4.69%)을 차지했는데 영업비밀성을 인정받지 못한 무죄에 비해 비율 자체가 높지는 않으나 유죄 판결을 위해서는 결국 영업비밀임을 입증하는 동시에 피고인의 부정한 목적까지 충분히 증명해야 한다는 점에서 그 어려움이 배 이상 가중된다고 볼 수 있다. 그 외 단순 반출 및 사용으로 혐의 자체가 인정되지 않거나 압수수색절차 과정에서의 위법으로 인해 증거능력이 부정되는 등 기타 사유로 인한 무죄가 21건(6.16%)을 차지하였다.

2.3 기술유출 형사사건 무죄 유형별 사례

판결의 적정성은 단편적인 통계 수치만을 가지고 일률적으로 논의하기는 어려운 영역이므로 무죄가 선고된 기술유출 사건의 일부 판결을 검토해 보고자 한다.

2008도3435 사건에서는 피고인들이 피해회사의 기술 자료를 개인 노트북 등을 이용하여 유출한 사실과 관련하여 유출된 자료의 일부가 외부에 공개된 보고서 및 학회에 발표된 논문을 구성하는 내용이거니와 해당 자료들을 보관함에 있어 보관책임자가 지정되거나 별다른 보안장치 또는 보안관리 규정이 없었으며 해당 파일들을 중요도에 따라 대외비 또는 기밀자료라는 표시도 하지 않았고 연구원뿐 아니라 생산직 사원들도 자유롭게 접근이 가능한 파일서버 내에 저장되어 열람, 복사가 자유로웠던 사실 등에 비추어 볼 때 해당 파일들이 상당한 노력에 의하여 비밀로 관리되었다고 보기 어려운 점을 종합하였을 때 해당 파일들이 영

업비밀에 해당하지 않는다고 판단, 무죄를 선고하였다.

2008노2107 사건의 경우, 피고인들이 회사를 그만두는 시점에 개인적인 짐을 챙기는 과정에서 회사의 제품 관련 회로도, 부품 리스트, 테스트 매뉴얼 등 다수의 업무자료가 저장되어 있는 컴퓨터에 대해 업무 관련 내용을 삭제하고 반출하라는 지시를 이행하지 않고 반출한 사실과 관련하여 무단 반출한 사실은 인정되나 유출한 자료의 제품들이 이미 공개적으로 판매되고 있는 제품들이어서 판매 중인 제품을 구입하여 분해하면 부품 리스트를 알아낼 수 있고, 회로도 또한 다른 모듈 판매회사들이 제공하는 표준 회로도와 유사한 수준이며 제품 운영에 필요한 소프트웨어 자체도 해당 제품을 구입하면 복제할 수 있는 점 등을 고려하였을 때 독립적인 경제적 가치를 가지고 있다고 인정할 수 없으며 해당 자료들에 대한 관리적인 측면에서도 컴퓨터에 저장된 해당 파일들을 프린트로 출력하거나 USB 등에 저장하는 것을 방지할 수 있는 보안장치가 없었던 사실, 하청업체에게 제공한 회로도 등을 다른 곳에 유출하지 말라고 요구하거나 제품 생산이 종료된 이후 회수하는 등의 조치를 취하지 않은 사실들을 비추어 보았을 때 상당한 노력에 의하여 비밀로 관리되었다고 볼 수 없는 점을 종합하여 볼 때 해당 자료들은 영업비밀에 해당하지 않는다고 판단, 무죄를 선고하였다.

2017노2162 사건에서는 피해회사에서 근무하던 직원들이 피해회사의 제품 관련 원재료 및 제조기술을 유출한 이후 동종 회사를 설립한 사실과 관련하여 법원은 원재료를 절취한 점에 대해서는 절도죄로 유죄가 인정되나 유출된 제조기술에 대해서는 해당 정보가 포함된 문서들이 전자파일로 생성, 보관되면서 별도의 암호나 방화벽 없이 열람이 가능했던 점, 출력에 대해서도 별도 제한이 없었던 점, 출력본에 대외비 표시도 미흡한 점, 팀장들은 별도 제한 없이 타 부서의 문서를 열람할 수 있었던 점 등을 미루어 볼 때 영업비밀이라고 객관적으로 인식될 수 있는 정도로 통제되고 있었다고 보기 어렵다고 판단하여 무죄를 선고하였다.

2.3.2 산업기술 부정

2011도1614 사건의 경우, 선박을 건조하는 피해회사에서 건조 중이던 ‘드릴쉽(Drillship)’에 대한 선급검사 업무를 담당하던 피고인(중국 국적)이 동료 선급검사관으로부터 전달받은 USB에 드릴쉽 기술 관련 파일들이 저장되어 있는 것을 발견하고 이를 피고인의 노트북 및 외장하드에 무단 저장하여 유출하였으나 유출된 파일과 관련하여 산업통상자원부 고시에 의거하여 해양특수선의 한 종류로 드릴쉽이 규정되어 있으나 이는 첨단제품의 하나로 고시된 것으로 볼 수 있을 뿐 관련된 어떠한 기술이 함께 고시된 것으로 볼 수는 없는 바 해당 고시에서 첨단제품으로 드릴쉽을 정하고 있다고 해서 드릴쉽 설계기술이나 건조기술 등 드릴쉽과 관련된 모든 기술이 산업기술보호법상 산업기술에 해당한다고 볼 수 없으며 국가핵심기술에는 ‘고부가가치 선박 및 해양시스템 설계기술’이 명시되어 있고 고부가가치 선박에 드릴쉽이 포함되어 있으므로 드릴쉽 설계기술은 산업기술에 해당하나 설계기술 상의 정보를 제외한 나머지 정보들은 산업기술에 해당하지 않는다고 판단, 산업기술 유출 관련해서는 무죄를 선고하였다.

2.3.3 부정한 목적 부정

2015도464 사건에서 법원은 피해회사의 장비업체 직원(엔지니어)이 피해회사의 국가핵심기술 관련 자료 일부를 카드 형태의 USB에 담아 무단 반출하여 협력업체의 외국(이스라엘) 본사 직원에게 해당 자료를 전달한 사실과 관련하여 유출한 자료가 핵심기술의 일부이며 보안규정을 알면서도 위반한 사실에 대해서는 인정되나 유출 및 해외 본사 직원과 자료를 공유한 목적이 해당 장비의 문제점 파악 등을 통한 성능 향상에 도움이 되기 위함이었으며 이는 궁극적으로는 피해회사의 이익으로 환원된다는 점, 해당 자료들이 경쟁 업체에 유출되거나 업무와 관련 없는 직원들에게까지 전달되는 등 다른 불법적인 용도로 사용되었다는 증거가 충분치 않다는 점을 고려하였을 때 부정한 이익을 얻거나 그 대상기관에게 손해를 입힐 목적 및 외국에서 사용하거나 사용되게 할 목적이 있었

음이 합리적 의심의 여지가 없을 정도로 증명되지 않았다고 판단, 무죄를 선고하였다.

2018노777 사건에서 법원은 피해회사의 고위 임원이었던 피고인이 국가핵심기술을 포함한 다량의 기술 자료를 집으로 유출한 사실에 대해 피고인이 헤드헌터와 접촉하기는 하였지만, 이직에 대한 구체적인 논의가 있었다고 볼 만한 증거가 없는 점, 피고인이 사무실에서 출력한 자료를 집에 가져가서 공부하고 폐기한 행위가 약 7년간 꾸준히 계속되어 온 점, 회사 이메일을 출력한 사유가 사내 보안 프로그램에 의해 이메일이 정기적으로 삭제되기 때문에 이에 대비하기 위한 것이라는 점, 회사의 보안검색이 본래 규정과는 달리 임원용 차량에 대해서는 완화되어 있었기 때문에 특별히 악의를 가지고 보안검색을 무력화시켰다고 보이지 않는 점, 피고인이 다소 긴 병가를 냈다는 사정이 이직을 위하여 다량의 기술 자료를 유출하였음을 의심하게 할 만한 사정으로 보기도 어려운 점, 피고인이 업무에 참고하기 위해서 종전에 근무했던 사업부의 자료를 활용할 여지도 있다고 보이는 점 등을 고려하였을 때 피고인이 부정한 이익을 얻거나 피해회사에게 손해를 입힐 의도로 산업기술을 유출하였다는 목적이 충분히 증명되었다고 보기 어렵다고 판단, 무죄를 선고하였다.

이처럼 기술유출 범죄의 주요 무죄 판결 사례를 살펴보면 영업비밀 또는 산업기술 자체에 대한 객관적 구성요건이 부정되는 것이 1차적인 무죄 사유이고 기술 자체의 중요성 및 가치가 인정된다 하더라도 2차적으로 주관적 구성요건인 기술유출 행위자의 부정한 목적성 즉 '부정한 이익을 얻거나 대상기관에게 손해를 입힐 목적'을 의심의 여지가 없을 정도로 입증하지 못하면 무죄로 판결될 가능성이 높은데 이 모든 증명책임이 기술 전문성이 상대적으로 부족할 수밖에 없는 검사에게 있다는 점에 비추어 볼 때 기술유출 형사사건의 무죄 비율이 일반 형사사건 대비 높은 것은 어쩌면 지극히 당연한 결과라고 보인다.

3. 기술유출 사건 무죄율이 높은 이유

3.1 객관적 구성요건 부정

3.1.1 비공지성 관련

수사 과정에서 피의자가 자료를 제출하면서 적극적으로 다투지 않으면 외부에 공지된 정보의 범위가 어디까지인지 수사기관 스스로 확인하기 어렵고, 이는 피해자 입장에서도 마찬가지이다.

<표 7> 기술유출 형사사건의 주요 무죄 판결 사례

판결번호	적용법령	주요 무죄사유	주요 내용
2006도 9022	부정경쟁방지법	영업비밀성 부정	거래처 등에 제공된 적이 있으며 일부 내용이 홈페이지에도 공개되어 있고 해당 문서의 보유자가 경제적 이익을 얻을 수 있는 정보로 인정되지 않음
2008도 3435	부정경쟁방지법	영업비밀성 부정	공개된 보고서 및 학회에 발표된 논문을 구성하는 내용이고 파일들이 상당한 노력에 의하여 비밀로 관리되었다고 볼 수 없음
2008노 2107	부정경쟁방지법	영업비밀성 부정	판매 중인 제품을 구입, 분해하면 확보할 수 있는 수준의 정보로 독립적인 경제적 가치가 있다고 인정되지 않으며 상당한 노력에 의하여 비밀로 관리되었다고도 볼 수 없음
2017노 2162	부정경쟁방지법	영업비밀성 부정	영업비밀이라고 객관적으로 인식될 수 있는 정도로 통제(관리)되었다고 보기 어려움
2011도 1614	산업기술보호법	산업기술 부정	드릴쉽 설계기술은 산업기술에 해당하나 설계기술 상의 정보를 제외한 나머지 정보들은 산업기술에 해당하지 않음
2015도 464	산업기술보호법	부정한 목적 부정	부정한 이익을 얻거나 그 대상기관에게 손해를 입힐 목적 및 외국에서 사용하거나 사용되게 할 목적이 있었음이 충분히 증명되지 않음
2018노 777	산업기술보호법	부정한 목적 부정	부정한 이익을 얻거나 피해회사에게 손해를 입힐 의도로 산업기술을 유출하였다는 목적이 충분히 증명되었다고 보기 어렵다고 판단

기소된 이후 영업비밀이 특정되면 피고인 측이 공지된 자료를 샅샅이 검색하여 공판 과정에서 제출하는 경우가 많은데 이는 문제가 된 영업비밀과 공개 정보가 동일하지 않다고 하더라도 이를 공판 검사가 소화하여 재판부를 설득시키기 어려운 것이 현실이다.

따라서 피해자가 공판에 적극적으로 개입하여 반박하여야 하는데 절차적으로 피해자의 참여 수단이 제한되어 있어 무죄 판결의 주된 원인이 되고 있다. 예를 들어, 기업들은 관련 기술에 대하여 여러 건의 특허를 취득하고 있는 경우가 많은데, 특허의 경우 그 기술의 범위를 넓게 설정하고(예를 들어 1-10으로) 실제 적용하는 특정 값(예를 들어 3.6)은 공개하지 아니하고 영업비밀로 관리하는 것이 일반적인 전략인데, 피고인이 수많은 특허를 내세우며 공지된 기술이라고 복잡한 주장을 하는 경우, 기술 전문성 등이 부족한 검사가 이에 대응하기 어렵고, 영업비밀 관련 경험이 별로 없는 재판부의 경우 위와 같은 기본적인 사항을 인식하지 못하는 경우가 있다.

3.1.2 경제적 유용성 관련

통상 경제적 유용성 단독으로는 잘 문제가 되지 않는 편이며, 비공지성이 문제되는 경우에 해당 정보가 공개되어 있다는 이유로 경제적 유용성이 동시에 문제가 되는 경우가 많다. 진보의 수준이 낮아 관련 업계에서 비교적 도출이 쉬운 정보에 대해서는 경제적 유용성이 인정되지 않아 무죄가 선고되는 경우가 있는데 특히, 고객정보 등 경영상 정보에 대해서는 피해자 입장에서 생각하는 가치와 법원이 인식하는 가치에 큰 차이가 있는 경우가 종종 있으며, 법원을 충분히 설득하지 못하는 경우 무죄 판결의 원인이 되기도 한다.

3.1.3 비밀관리성 관련

위에서 언급한 바와 같이 기술유출 형사사건의 무죄율은 전체 형사사건 평균의 약 6배에 달할 정도로 높은데, 비밀관리성 결여를 이유로 영업비밀이 불인정 되는 경우가 특히 많다. 다만, 비밀관리성 불인정의 문제는 주로 보안시스템을 충분히 갖추지 못한 중소규모 이하 회사들에게 문제가 되는 무죄 원인으로서 대기업의 경우 비밀관리성으로 인해 영업비밀성이 부정되는 경우가 많지는 않은 편이다. 최근 여러 차례 부정경쟁방지법이 개정되면서 법문상 비밀관리성의 요건을 점차 완화하는 방향은 분명하나, 법원의 판단기준이 실제로 완화되어 가고 있는지는 명확하지 않다.

따라서 아직까지는 비밀관리성 입증 수준이 높고 고려 요소들이 많은 것으로 평가되고 있다. 국민권익위원회(2022)에서 발표한 자료에 따르면 통상 내부 보안규정의 존재 및 영업비밀 등급 분류 여부, 임직원들을 상대로 한 보안교육의 실시 여부, 물리적인 잠금장치 및 CCTV 등 설치 여부, 프로그램에 의한 암호화, DRM 등 설정 여부, 대외비 등 비밀 표시 여부, 보안책임자 지정 여부, 외부 반출 제한 여부 등이 법원에서 고려하는 요소이며 각 항목별로 컴플라이언스 체크가 필요함을 안내하고 있다[20].

3.1.4 산업기술(국가핵심기술) 미해당

산업기술(또는 국가핵심기술) 유출이 문제된 제품 또는 기술 카테고리가 산업기술(또는 국가핵심기술)로 지정되어 있다고 하더라도 산업기술(또는 국가핵심기술)의 문언을 법원이 엄격하게 해석하거나 개별 자료가 산업기술(또는 국가핵심기술)에 해당하는지를 법원이 다시 판단함으로 인하여 무죄가 선고된 사례가 있다. 산업기술(또는 국가핵심기술) 문언이 포괄적이고 이에 대한 구체적인 해설이 존재하지 않아 법관에 따라 주관적인 판단의 여지가 있으며 또한 산업통상자원부의 판정을 받았다고 하더라도 이는 확인적 성격에 불과하다는 이유로 법원이 개별 사례에서 다시 판단하는 경우가 지속 발생하고 있다.

3.2 주관적 구성요건 부정

실무상 피의자/피고인 측이 영업비밀 자료의 취득 및 사용 경위에 대해 업무상 목적으로 취득 내지 사용한 것이므로 부정한 목적이 없었다고 주장하는 경우가 많은데 그 결과, 명백히 권한이 없는 제 3자에게 자료가 유출되었거나 정당한 목적 범

위를 명백하게 벗어난 부정사용 사실이 확인되지 않은 사건에서는 규정이나 계약에 위반하여 영업비밀 자료를 취급하더라도 부정한 목적이 부인되어 무죄가 선고되는 사례가 있다. 특히 사내 규정이나 계약에도 불구하고 이를 위반한 채 실무가 진행되고 직원들도 이를 묵인해 온 사실관계가 인정되면 무죄 가능성이 커진다.

부정한 목적에 대한 입증이 부족하여 제대로 형사처벌이 이루어지지 않는 문제를 개선하기 위하여 절취, 기망, 협박, 그 밖의 부정한 수단으로 영업비밀을 취득한 경우에는 부정한 목적을 요구하지 않도록 2019년 부정경쟁방지법 개정이 이루어졌지만, 대법원 판례상 업무상 목적에 따라 보유한 자료의 경우 나중에 유출이 되더라도 별도의 영업비밀취득죄 성립을 인정하지 않으므로 위의 개정된 규정이 적용될 수 있는 범위는 제한적이다.

3.3 수사/공판 과정 절차 및 구조 한계

3.3.1 압수물 선별절차 시 피해자 참여권 미보장

압수 후 이루어지는 선별 절차는 기술 및 영업비밀의 유출 및 부정사용 증거를 확보하는 데 있어 가장 중요한 절차이다. 그런데 피해자 참여 없이 선별을 진행하게 될 경우, 기술 내용에 대한 전문적 지식이 부족한 수사팀만으로는 유출된 자료, 특히 부정 사용된 흔적을 확인하기 어려운 것이 현실이다. 현재 수사 실무의 입장은 피압수자(피의자)의 동의를 전제로 수사관이 피해자의 참여가 필요하다는 재량적 판단이 있을 때 비로소 피해자의 선별 절차 참여가 허용되고 있다. 만일 이러한 선행 조건 없이 피해자를 선별에 참여시키게 되면 절차 위법 또는 반대 방향의 비밀 침해 문제가 발생할 수 있다.

3.3.2 수사 과정에서 피해자 조력의 절차적 한계

기소 전 수사 기록은 수사 보안 등을 이유로 그 등사 범위가 본인 진술서류 또는 본인 제출서류로 제한됨이 원칙이다. 그 이외의 서류에 대해서는 피해 회복을 목적으로 하는 범위로 한정되나 실무상 수사기관이 등사를 허락하는 경우는 매우 예외적이다. 따라서 피해자 회사 소속 엔지니어에 대한 참고인 신문을 통해 압수물을 제시하며 피해를 진술하는 방식 이외에는 피해자가 기술적 측면에서 조력을 제공하기 어렵고, 이는 높은 무죄율 및 낮은 형량의 실질적인 이유로 작용한다.

3.3.3 공판 단계에서 피해자 참여의 절차적 한계

우리나라 재판 실무상 공판 검사는 6개월 내지 1년마다 교체되며, 해당 사건은 공판 검사가 담당하는 여러 사건 중 하나에 불과하므로, 법원에 수사 기록을 제출하는 절차에 집중하고 기술 및 증거 설명을 하는 데에는 한계가 존재한다. 특히 앞서 언급한 바와 같이 영업비밀성 관련 쟁점은 공판 과정에서 새롭게 제기되는 경우가 많은데 적절한 대응이 사실상 불가능한 경우가 많다. 더불어, 영업비밀 형사사건은 단독판사가 담당하고 있는데, 수많은 사건을 처리해야 하는 형사 단독 재판부의 특성상 그 처리에 많은 시간과 노력이 투입되어야 하는 영업비밀 사건은 매우 부담이 될 수밖에 없고, 더욱이 영업비밀 사건을 처음 처리해 보는 재판부도 많아 관련 법리나 실무에 익숙하지 못할 수도 있다.

따라서 실체적 진실의 발견을 위해서는 피해자가 긴밀하게 절차에 관여하는 것이 필요하나 원칙적으로 피해자에 대한 증인신문이라는 제한된 절차를 통해서만 공소사실에 대한 진술이 가능한데(형사소송법 제294조의2) 앞서 언급한 바와 같이 영업비밀 재판을 주재하는 판사나 검사 등의 전문성이 부족한 현재 실무 상황에서는 전문성으로 무장한 피고인의 변호인들 주장에 휘둘릴 수밖에 없는바 이를 보완하기 위한 영업비밀 관련 전문성을 가진 피해자 대리인의 참여가 매우 필요한 상황임에도 형사소송법상 피해자 대리인의 절차 참여권의 존재 및 범위가 명시적으로 규정되어 있지 않다. 이처럼 실무상 기술 설명, 엔지니어에 대한 증인신문은 기술적인 전문성과 영업비밀 사건에 대한 전문성을 가지지 않으면 수행이 힘든 부분이 있으므로 피해자 또는 피해자 대리인의 참여가 필요하나, 제도적으로 명확히 보장되어 있지 않으며

이에 따라 재판 시마다 다툼의 대상이 되고 재판장의 소송지휘권에 맡겨져 있는 상황이다.

3.3.4 피해자 증거 제출의 어려움

영업비밀성이나 부정사용의 입증을 위해 수사과정이나 공판 단계에서 피해자의 증거 제출이 필요한 경우가 많이 있으나, 피고인 또는 변호인의 열람 내지 등사로 인한 추가적인 영업비밀 누설의 우려로 피해자는 증거 제출에 소극적인 입장을 가지게 된다.

실무적으로 민감한 부분을 삭제 또는 보이지 않게 편집하여 제출하거나, 보안 USB를 사용하여 제출하는 방식을 사용하기도 하나, 첫 번째 방법의 경우 입증이 필요한 부분과 관련이 있는 부분의 내용이 가려져 있다면 문서의 의미가 달라진다는 반박이 있을 수 있고, 두 번째 방법인 보안 USB를 사용하는 경우에도 피의자/피고인 측의 임의 협조를 전제로 하는 것이므로 피의자/피고인 측 입장에 따라 진행할 수 없을 수 있다.

3.3.5 전문적인 기술 사항에 대한 심리의 한계

증거의 증명력에 대해서는 자유심증주의가 적용되고 양형기준이 존재하기는 하지만 양형은 법관의 재량사항이다. 그런데 기술적 의미 파악에 한계가 있는 상황에서 심리를 진행하는 경우 잘못된 사실관계를 인정하거나 그렇지 않더라도 확신의 부족으로 인하여 상대적으로 낮은 형량이 선고될 가능성도 있다. 전문심리위원 제도가 존재하기는 하나 기술유출 형사사건에서는 단독판사의 업무 부담 등으로 인하여 거의 활용되고 있지 않으며, 특허와는 달리 영업비밀의 경우 피해자 회사에 특유한 부분이 있고 일반적으로 공개된 내용이 아니므로 적절한 전문심리위원을 선정하기 어려운 측면도 있다.

또한 현재 제도상 전문심리위원의 의견이 소송기록에 첨부되는 것이 아니라 공개되지 않는 재판부와의 커뮤니케이션에 의해 전달되므로 검사 측뿐만 아니라 피고인 입장에서도 예측 가능성이 떨어지는 문제가 있다. 전국에서 가장 많은 기술유출 사건을 다루는 수원지방법원에 지식재산권 전담 재판부가 설치되는[21] 등 긍정적인 변화가 일고 있으나 법원 인사 구조상 통상 형사 단독은 2년(빠르면 1년) 근무를 넘지 않으므로 추후에도 꾸준한 제도적, 실무적 개선이 필요한 상황이다.

4. 부당한 무죄를 위한 개선 고려사항

4.1 법령 개정 내지 해석상 고려 필요사항

‘부정한 이익을 얻거나 대상기관에게 손해를 입힐 목적’이라는 주관적 구성요건이 범죄구성요건으로 반드시 필요한 것인지에 대한 검토가 필요하다. 허락된 범위 외의 영업비밀 사용이나 허락된 장소 외로 영업비밀 자료를 옮기는 행위 자체로 가벌성이 있는 것으로 보되 업무상 목적이 개입된 경우라면 양형에서 고려하도록 하는 방안을 고려해 볼 수 있을 것이다.

또한 비밀관리성 관련하여 현재의 ‘비밀로 관리된’에서 추가적인 법령 개정이 필요할 것으로 보이지는 않으나, 비밀관리성 문구는 비밀관리성 불인정으로 인한 무죄율 증가에 대한 반성적 고려에서 개정된 것이므로 이러한 취지를 법원에서 충분히 고려하여 영업비밀로서 보호 가능한 정보의 범위를 판단할 필요가 있다는 공감대가 형성되어야 할 필요성이 있다.

마지막으로 산업기술, 특히 국가핵심기술 지정고시를 개정함에 있어 해당 여부를 보다 명확하게 구분할 수 있도록 문구를 정비하고, 필요한 경우 산업통상자원부 또는 유관 기관에서 해설 자료를 배포하는 방안도 고려할 수 있을 것이다.

4.2 수사 과정 기술유출 피해자의 절차 참여

현행 제도하에서는 전국 검찰청으로부터 기술유출, 특허법 위반 등 특허범죄사건을 이송, 자문의뢰 받아 처리하고 있는 대전지방검찰청의 특허기술변론절차(수사 초기에 검사 및 수사관의 기술에 대한 이해도를 높이기 위해 고소인을 상대로 기술설명회 형식으로 변론절차를 진행하는 제도로 2017년 2월 최초 도입) 및 수원지방검찰청의 첨단산업기술변론절차(대전지검의 특허기술변론절차를

벤치마킹하여 2020년 11월 도입되었으며 조서 작성 대신 구두 변론절차를 통해 기술에 대한 변론을 심도 있게 진행할 수 있고 수사팀도 기술에 대한 이해도를 제고할 수 있도록 마련하였으나 기술유출 사건의 특성상 실무적으로는 양 당사자가 참여하는 기술변론절차는 거의 진행되지 않고, 송치 사건의 수사 마무리 단계에서 진행되는 경우가 일부 있음)의 활용을 보다 적극적으로 고려할 수 있을 것이다. 다만, 특별히 마련되어 진행되는 절차에서 설명이 부족하게 되면 되려 수사 의지를 약해지게 할 수도 있으므로 사전에 철저한 준비가 필요하다는 점을 고려해야 할 것이다.

제도 개선사항으로서는 압수물 선별 절차의 중요성에 비추어, 일정한 요건 하에서는 피해자의 절차 참여를 넓게 보장하는 방안이 마련될 필요가 있다. 예컨대 피압수자의 동의가 없어도, 검사의 사전승인 하에 외부 전문가 등 객관적인 제 3자와 함께 피해자 참여를 보장하는 방법이 있을 것이다. 또한 현재 검찰이 구속영장신청 사건에 대해 필수적으로 피의자를 면담하도록 하고 있는바, 기술유출 형사사건의 경우에는 기록만으로 단시간 내에 실체를 파악하기 힘든 부분을 고려하여 피해자의 진술을 필수적으로 청취하도록 하는 방안도 고려할 수 있을 것이다.

4.3 공판 단계 피해자 조력 범위, 절차 법제화

기술유출 형사사건에서 검사의 공판 유지를 지원하기 위하여 피해자, 피해자 대리인, 또는 기술전문가가 공판 과정에서 검사를 보좌할 수 있는 제도적 근거를 마련할 필요가 있다. 검사의 공판 절차 진행을 보조하는 한도에서 당사자적 지위를 부여하고, 다만 사인이라는 점을 고려하여 엄격한 비밀유지의무를 법률상 부과하는 방안을 고려할 수 있을 것이다. 또한 현재 운영되고 있는 첨단산업 보호 중점 검찰청 등에 파견된 특허청 파견 인력이 공판 과정에서 검사를 보좌할 수 있는 법적 근거가 추가되는 것도 바람직한 방향이라고 할 수 있겠다.

4.4 증거제출을 위한 비밀유지제도 법제화

민사 사건에서의 비밀유지명령 제도, 일본 부정경쟁방지법상의 비닉결정 제도(당사자 신청 시 법원이 영업비밀의 전부 또는 일부의 사항을 공개 법정에서 밝히지 않는다는 결정을 할 수 있으며 변호인이 검사 신청 증거서류 열람 시 범죄의 증명 혹은 범죄의 수사나 피고인의 방어에 관해 필요하다고 인정될 때를 제외하고는 관계인에게 알려지지 않도록 비닉요청을 할 수 있도록 하는 규정), 미국 연방형사소송규칙상의 Protective order 제도(연방소송규칙 제 16조에 의거, 법원에 영업비밀 자료의 전부 또는 일부를 비공개하는 '보호 또는 수정 명령'을 신청할 수 있는 제도)를 벤치마킹하여 기술유출 형사사건에서의 비밀유지제도를 법제화할 필요가 있다. 다만 현재 도입되어 있는 민사 사건에서의 비밀유지명령 제도는 상대방 당사자 본인에게도 비밀이 제공되는 문제점이 있으므로, 이 부분에 대한 보완이 필요할 것으로 보인다. 이와 관련하여 미국에서는 대리인인 변호사만 해당 정보를 볼 수 있는 Attorney's Eyes Only 제도를 운용함으로써 피해자 회사의 정보가 피의자/피고인 측에 전달되는 것을 방지하고 있는바 이러한 제도의 도입을 고려할 수 있을 것이다. 또한 민사 사건에서의 비밀유지명령 제도보다 더 나아가 실무적으로 수사 과정 및 공판 단계에서 피해자의 영업비밀 유출 우려를 줄일 수 있도록 이미 피고인들에게 유출된 영업비밀 자료 이외의 자료에 대해서는 변호인에 한해서만, 비밀유지명령 하에 특수한 전자적 조치(보안 USB 등)를 거쳐 열람 내지 등사하도록 하는 등의 구체적인 절차 규정이 필요할 것이다.

4.5 사이버보안 측면의 기업 보안체계 전환

전통적으로 대다수 기업에서는 외부로부터의 불법적인 침입 및 외부에서 발생하는 보안 위협으로부터 내부 자산을 방어하는 형태의 경계(Perimeter) 기반 보안체계를 주로 채택하였는데[22] 경계 기반의 보안체계는 관련 보안솔루션을 운영함에 있어 운영 효율성을 높이고 외부로부터 발생하는 침입 및 위협을 차단하기에는 효과적이지만 정상적으로 인가받은 내부자에 의한 불법적인 행위

를 탐지하고 차단하기에는 한계가 있다[23][24]. 더군다나 COVID-19 이후 급격하게 증가한 재택근무 등 업무환경 및 방식의 변화로 인해 사내와 외부의 경계가 점차 불분명해지고 있는 상황에서 기존 보안체계의 취약한 부분을 노린 내부자에 의한 기술유출 시도 및 보안 위협은 날이 갈수록 증가하고 있다[25][26].

최근 이러한 전통적인 경계 기반 보안체계의 한계점을 극복하는 모델로 'Never Trust, Always Verify'라는 표어의 제로 트러스트(Zero Trust) 보안체계가 주목받고 있다[27]. 제로 트러스트 보안체계는 2010년 포레스터(Forrester) 리서치의 존 킨더백(John Kindervag)이 최초로 제안한 개념으로 기업의 환경에 따라 실제 구현 방식이나 형태는 다소 차이가 있으나 지향하는 방향은 내부자와 외부자 그 어떤 누구도 신뢰하지 않는다는 전제를 기반으로 기업의 데이터 및 자산을 중요도에 따라 세분화하여 분류하고, 자산 및 데이터에 접근하는 사용자의 신원을 다양한 방식으로 철저하게 검증하며, 검증된 사용자일지라도 업무에 필요한 최소한의 권한만 허용함으로써 불필요한 자산 및 데이터에 대한 접근을 일체 차단할 뿐 아니라 사용자의 모든 행위(접근시간, 접속기기, 데이터 조회, 파일 다운로드 등)들에 대한 모니터링을 실시간으로 수행하여 이상행위가 발견될 경우 즉시 차단하는 등의 과정이 유기적으로 수행될 수 있도록 기업의 내·외부를 구분하지 않는 통합 보안체계를 갖춘다는 것이다[28][29].

하지만 이런 보안체계의 전환은 대규모의 비용투자가 요구될 뿐 아니라 실제적으로 업무환경에 맞게 적용하고 정착시키는 데까지 오랜 시간이 소요되는 작업이다. 제로 트러스트 보안체계의 개척자라 불리는 구글(Google)의 경우에도 기존의 VPN(Virtual Private Network) 환경을 자체적으로 구현한 제로 트러스트 환경인 'BeyondCorp'으로 전환하는데 6년 이상이 소요되었다고 한다[30]. 그러나 국가핵심기술 등과 같이 유출될 경우 그 피해가 막심한 첨단기술을 보유한 기업이라면 내부자 등에 의한 기술유출 자체를 철저하게 방어하는 동시에 그럼에도 불구하고 발생하는 유출사고에 대해서는 유출경로를 면밀하게 추적하고 관련 증거를 보다 확실하게 수집할 수 있는 제로 트러스트 기반 보안체계로의 전환을 하루빨리 검토하고 점진적으로 전환해 나가는 노력을 수행해야 할 것이다.

5. 적합·타당성 및 신뢰도 검증

앞서 도출한 개선 고려사항들에 대한 적합·타당성 검증을 위해 법조인, 수사관, 기업 및 기관 보안 담당자 등 기술유출 관련 업계 전문가 75명을 대상으로 설문조사를 실시하였다. 설문조사는 2022년 9월 16일부터 18일까지(3일간) 진행하였으며 설문지는 도출된 각 개선 고려사항이 부당한 무죄사건을 줄이는데 필요한지 여부를 리커트(Likert) 5점 척도에 기반하여 응답하는 방식으로 구성하였고 온라인을 통해 설문지를 전송하여 응답을 회신받는 방법으로 진행하였다.

<표 8> 설문조사 개요

구분	주요 내용
목적	기술유출 관련 부당한 무죄를 줄이기 위해 도출한 개선 고려사항에 대한 타당성 검증
대상	기술유출 관련 업계 전문가 75명
기간	2022. 9. 16 ~ 2022. 9. 18 (3일간)
응답 방식	선행연구를 통해 도출한 개선 고려사항에 대한 필요성을 리커트 5점 척도로 응답
방법	온라인 설문(구글 서베이 폼 활용)

설문조사 결과는 타 논문[31]에서와 같이 각 개선 고려항목의 평균값(기준 타당성)은 3.5점을 기준으로 하여 적합 여부를 구분하였다. 이에 따라 <표 9>와 같이 5개 개선 고려항목 모두 평균값이 3.5점 이상으로 적합·타당함이 검증되었으며 해당 결과를 기준으로 각 항목에 대한 우선순위도 정하였다(동점 항목의 경우 표준편차 값이 작은 항목을 선순위로 선정).

또한, 신뢰도 측정을 위해 크론바흐 알파(Cron

bach's α) 값을 계산한 결과 0.715로 산출됨에 따라 기준(0.7) 이상의 신뢰도를 확보하는 것을 확인하였다.

<표 9> 적합·타당성 검증 결과

연번	개선 고려사항 항목	평균 (표준편차)	우선순위
1	법령 개정 및 해석상 고려 (주관적 구성요건 제외 등)	4.04 (1.03)	5
2	수사 과정상 기술유출 피해자 절차 참여 확대	4.09 (0.87)	4
3	공판 단계 피해자 조력 범위 및 절차 법제화	4.24 (0.82)	3
4	적극적 증거제출을 위한 비밀유지제도 법제화	4.24 (0.75)	2
5	기업의 보안체계 전환 (경계기반 → 제로 트러스트)	4.27 (0.92)	1

이러한 검증 결과는 앞서 제시한 개선 고려사항들이 부당한 무죄사건을 줄이는데 상당 부분 기여할 수 있을 것이라는 결론을 도출할 수 있지만, 실제 부당한 무죄율을 얼마만큼 낮출 수 있는지 정량적으로 도출하는 데는 한계가 존재하며 이를 위해서는 더욱 심도 깊은 추가적인 연구가 필요하다.

6. 맺음말

기술이 고도화됨에 따라 기술유출 범죄는 더 이상 피해기업만의 문제가 아닌 국가 전반에 악영향을 미치는 중대한 범죄이며 기술의 특성상 한번 유출되고 나면 다시 동일한 수준의 기술격차를 벌리는 데 막대한 비용과 노력이 수반되어야 한다는 점에서 기술유출 범죄로의 유인 자체를 근절시킬 수 있는 효과적인 방안이 그 어느 때보다 절실한 때임이 분명하다.

이러한 사회적 상황에 맞추어 법정형을 대폭 상향하는 등 국회 및 정부 차원의 제도적 보완이 이루어지고 있는 것은 사실이나 국가핵심기술을 보유한 기업의 현직 임직원 502명을 대상으로 기술유출 관련 설문조사를 자체적으로 실시해 본 결과, “우리나라의 기술유출 관련 법 처벌 수준이 어느 정도라고 생각하는가?“ 라는 질문에 응답자의 73.9%가 ”처벌 수준이 강하지 않다(보통 이하).”라고 답변하였으며, “미국 등 해외 다른 국가와 비교하였을 때 우리나라의 기술유출 처벌 강도는 어떠한가?”라는 질문에는 응답자의 76.1%가 “해외가 더 강력하다.”라고 답변하였는데 실제 법정형만을 기준으로 볼 때 해외 주요국들과 비교해도 부족하지 않은 수준임에도 불구하고 위와 같은 설문 결과가 도출된 것은 언론매체 등을 통해 보도되는 기술유출 범죄에 대한 처벌 결과 대다수가 무죄로 판결 나거나 유죄로 판결이 나더라도 사회통념상 범죄를 억제할 정도로 강력한 수준이라고 인식되지 않았기 때문이라 판단된다.

결국 기술유출 범죄에 대해 국민들의 인식이 전환될 수준으로 억제력을 갖추기 위해서는 법정형과 같이 기준이 되는 처벌 규정을 상향하는 것과는 별개로 실질적인 처벌의 확실성을 높이기 위한 노력이 필요한 상황이라 할 수 있겠다. 부당하게 유죄를 선고받는 피해자가 발생하면 안 된다는 것이 국민 대다수가 공히 인정하는 절대적 가치인 것처럼 기술유출 범죄에 있어서는 잠재적 기술유출을 야기할 수 있는 부당한 무죄가 발생하면 안 된다는 것을 국민 대다수가 이해하고 이를 실현하기 위한 사회적이고 제도적인 개선 노력이 앞으로 지속적으로 이루어지기를 바라며 본 연구가 그런 노력을 실천함에 있어 조금이나마 보탬이 되기를 기대한다.

참고문헌

[1] 산업통상자원부, ‘제1차 부정경쟁방지 및 영업비밀 보호 기본계획(안) [2022~2026]’, 2021.

[2] 산업통상자원부, ‘제4차 산업기술의 유출방지 및 보호에 관한 종합계획’, 2021.

[3] 조선비즈, “국정원 5년간 산업기술 유출 시도 99건... 22조원 규모”, 2022. 4. 2.

[4] 허정현, 이채율, “산업기밀 유출범죄 처벌의

실태와 실효성 제고에 관한 논의", 한국산업보안연구, 제12권, 제1호, pp. 263-292, 2022.

[5] 국회입법조사처, '산업·안보기술 관련 해외 입법 동향과 시사점', 2020.

[6] 이승주. "기술과 국제정치: 기술 패권경쟁시대의 한국의 전략", 한국과국제정치, 38권, 1호, pp. 227-256, 2022.

[7] Zak Dychtwald, "China's New Innovation Advantage", Harvard Business Review, Vol. 99, No. 3, pp. 55-60, 2021.

[8] Allison Graham, Kevin Klyman, Karina Barbesino, & Hugo Yen, 'The Great Tech Rivalry: China vs the U.S.', Belfer Center for Science and International Affairs, Harvard Kennedy School, 2021.

[9] Peter Navarro, 'Why Economic Security is National Security?', Real Clear Politics, December 9, 2018.

[10] Roberts Anthea, Choer Moraes Henrique, & Ferguson Victor, 'Geoeconomics: the US Strategy of Technological Protection and Economic Security', Lawfare, December 11, 2018.

[11] Haiyang Sun, "U.S.-China Tech War: Impacts and Prospects", China Quarterly of International Strategic Studies, Vol. 5, No. 2, pp. 197-212, 2019.

[12] 정주호, "산업기술의 보호와 유출방지를 위한 처벌법규의 비교법적 고찰 : 미국, 일본, 중국을 중심으로", 한국국가안보국민안전학회지, 제4호, pp. 8-31

[13] 이장욱, "영업비밀 침해에 대한 형사적 규제 실태 연구 - 처벌의 확실성을 중심으로 -", 한국경찰연구, 제20권, 제1호, pp. 273-300, 2021.

[14] 박강우, "산업스파이범죄의 실태와 법적 규제의 문제점", 형사정책연구, 제23권, 제3호, pp. 129-160, 2012.

[15] 조용순, "2019년 개정 영업비밀보호법 및 산업기술보호법에 대한 검토 : 민·형사적 구제를 중심으로", 시큐리티 연구, 제61호, pp. 333-352, 2019.

[16] 박미랑, "영업비밀침해행위 및 부정경쟁행위 사건 양형요인", 형사법의 신동향, 제62호, pp. 105-132, 2019.

[17] 이순옥, "산업기밀 유출사건의 처리현황 및 판례에 대한 연구 - 양형에 관한 문제를 중심으로 -", 한국형사소송법학회 형사소송 이론과 실무, 제12권, 제2호, pp. 319-363, 2020.

[18] 한지영, "IP 5 국가에서 영업비밀 보호에 관한 최신 입법동향 및 영업비밀 소송전략에 관한 비교법 고찰 - 미국, 유럽연합, 일본, 중국 및 우리나라를 중심으로 -", 한국지식재산학회 산업재산권, 제63호, pp. 189-253, 2020.

[19] 특허청, '2017-2019 부정경쟁방지 및 영업비밀보호에 관한 법률 판결문 분석 연구', 146면, 2020.

[20] 국민권익위원회, '디지털시대의 영업비밀보호와 청렴윤리경영', 15-16면, 2022.

[21] 서울경제, "수원지법, 지식재산권 전담부 설치…기술유출 사건 전문성 제고", 2022. 4. 7.

[22] Saleem, Mubeen Begum, & Venkata Sravya, "Issues with perimeter based network security and a better model to resolve them", European Journal of Molecular & Clinical Medicine, Vol. 7, No. 9, pp. 2437-2444, 2020.

[23] R. Rapuzzi & M. Repetto, "Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter mode", Future Generation Computer Systems, Vol. 85, pp. 235-249, 2018.

[24] Ferretti L, Magnanini F, Andreolini M, &

Colajanni M., “Survivable zero trust for cloud computing environments”, Computers & Security, Vol. 110, 2021.

[25] Rhee K, Won D, Jang S-W, Chae S, & Park S, “Threat modeling of a mobile device management system for secure smart work”, Electronic Commerce Research, Vol. 13, No. 3, pp. 243-256, 2013.

[26] 한성화, 이후기, “제로 트러스트 환경을 위한 보안 정책 배포 방법에 대한 연구”, 융합보안논문지, 제22권, 제1호, pp. 93-98, 2022.

[27] Doug Barth & Evan Gilman, ‘Zero trust networks’, O′Reilly Media, Inc, 2017.

[28] Collier ZA & Sarkis J, “The zero trust supply chain: Managing supply chain risk in the absence of trust”, International Journal of Production Research, Vol. 59, No. 11, pp. 3430-3445, 2020.

[29] Alper Kerman, Oliver Borchert, Scott Rose, Eileen Division, & Allen Tan, ‘Implementing a Zero Trust Architecture’, The MITRE Corporation, 2020.

[30] ITWORLD, “재택근무와 IoT보안의 기대주’ 제로 트러스트의 현황”, 2020. 7. 3.

[31] 김재수, 김자원, 김정욱, 최유림, 장항배 “기술유출행위 군집화를 위한 탐색적 연구”, 융합보안논문지, 제19권, 제2호, pp. 3-9, 2019.

〔저자소개〕

황 경 준 (Kyung-joon Hwang)
2011년 2월 한동대학교 컴퓨터공학과 학사
2021년 3월 ~ 현재 고려대학교 정보보호대학원 융합보안학과 석사과정
email : hkjooni@gmail.com

권 헌 영 (Hun-yeong Kwon)
2005년 2월 연세대학교 법학과 박사
2008년 ~ 2015년 광운대학교 과학기술법학과 교수
2015년 9월 ~ 현재 고려대학교 정보보호대학원 교수
email : khy0@korea.ac.kr