

## 미국 영업비밀보호법(DTSA)의 주요내용 검토 및 시사점

김 윤 정\*

### 〈국문초록〉

기업의 보안시스템이 과거 대비 고도화 되고 있음에도 불구하고 산업계의 기술 유출사태는 증가하고 있다. 문제는 단순히 기술유출 사례가 증가하는 흐름인 것뿐만 아니라 그 경로가 점차 지능화·고도화되고 있다는 점이다. 이러한 기술유출의 증가는 국내 산업을 이끄는 기업들의 재무적인 손실 및 기술개발 위축 등의 내부적인 우려뿐만 아니라 글로벌시대에서 우리 기술의 해외로의 유출 가능성도 높아지고 있다는 것이다.

부정경쟁방지법 개정과 정부의 산업기술 유출 근절대책 발표 등의 노력에도 불구하고 이해 당사자가 많아진 현 산업 시대에서 기술유출을 막기란 쉽지 않고 우리나라 기술보호 체계가 M&A 시도에 취약하고 유출피해의 심각성에 비해 국내 기술유출에 따른 처벌이 해외국가보다 약해 그 실효성이 떨어진다는 지적도 지속적으로 제기되고 있다.

특히 IT강국인 우리나라의 경우 영업비밀 중에서도 기술정보에 대한 위협에 대비하고 침해가 발생했을 시에 강력한 대응이 필요할 것이다. 따라서 현재 경쟁기업체들의 빈번한 영업비밀 절취 시도에 대해 적절한 대응을 할 수 있는 법제를 갖추어 우리나라의 경제안보는 물론 국가안보의 보호를 위한 노력을 꾸준히 진행해나가야 할 필요가 있다.

현재 영업비밀보호 법제를 가장 탄탄하게 갖추고 있는 미국에서도 늘어나고 있는 자국 기업의 영업비밀에 대한 위협에 대해 예의주시하고 있으며, 입법개선을 통해 영업비밀보호의 강화를 도모하고 있다. 따라서 우리나라도 미국의 영업비밀 보호법제를 검토하여 우리나라의 영업비밀보호 법제의 정비 및 강화를 꾀할 필요가 있다. 따라서 부정경쟁방지법에 영업비밀의 정의에 대한 구체적인 예시규정 마련, 영업비밀 도용에 대한 일방적 민사압류제도 도입, 기술유출의 조직범죄에 대한 법인의 중과규정 마련, 내부고발자 면책규정 마련 등을 통해 영업비밀 보호제도의 규제 개선이 필요하다.

주제어 : 영업비밀, 영업비밀보호법, 통일영업비밀보호법, 경제스파이법, 부정경쟁방지 및 영업비밀 보호에 관한 법률

• 투고일 : 2020.06.26. / 심사일 : 2020.07.22. / 게재확정일 : 2020.07.23.

\* 충북대학교 법학연구소 전임연구원.

## I. 서론

오늘날 기술은 기업의 가치 창출을 넘어 기업의 흥망을 좌우하고 있으며 국가 경쟁력 강화에 영향을 미치는 핵심 요소로 작용하고 있어 기업간 그리고 국가간 기술보호의 중요성이 증대되고 있다. 기업 및 국가는 특허권 등 지식재산권제도와 영업비밀 보호제도를 통해서 자사 또는 자국의 핵심 기술을 보호하고자 노력하고 있다.<sup>1)</sup>

영업비밀은 일반적으로 외부에 알려지지 않은 회사의 모든 생산방법, 판매방법 기타 영업활동 등의 정보로서 특허와는 다르게 공개되지 않는 이점이 있어 기업들은 기술상·경영상 정보를 비밀로 관리하고 있다. 기술혁신은 기업의 발전과 존속에도 막대한 영향을 미치며, 기업들은 기술을 보호하고 그 정보를 보호하기 위하여 많은 역량을 기하고 있으나 기술의 발달, 산업의 전문화 및 세분화, 기업 간 기술적 우위 확보를 위한 경쟁 심화 등으로 기술유출 및 영업비밀 침해로 인한 막대한 손해와 법적 분쟁도 많이 발생하고 있다.<sup>2)</sup>

글로벌 기술 강국인 미국은 자국기업의 영업비밀보호를 위해서 연방차원의 강력한 법률인 영업비밀보호법(Defend Trade Secrets Act, 이하 'DTSA'라 함)을 2016년 제정하여 시행중이다. 그동안 영업비밀 분쟁이 발생했을 경우 민사적 조치는 주(州)영업비밀보호법으로 형사적 조치는 연방 경제스파이방지법(Economics Espionage Act, 이하 'EEA'라 함)으로 이원화 되어 있었으나 동 법률의 제정으로 연방차원의 영업비밀보호를 형사적 제재에서 민사적 구제로까지 확대하게 되었다. 동 법률은 영업비밀의 범위를 대폭 확대하고 민·형사적 각종 조치를 강화함과 동시에 내부고발자에 대한 면책도 규정하였다는 특징이 있다.

2019년 중국 화웨이가 미국의 T모바일의 영업비밀을 유출한 혐의로 연방법원에 제소되었고 이 사건은 미-중 간 무역분쟁을 넘어 정치문제로까지 확대된 바가 있으며, 미국은 연방법원 제소와 별개로 동맹국들에게도 화웨이 제품에 대한 보이콧을 요청하였다.<sup>3)</sup> 우리나라에서도 2019년 중국 화웨이와 에릭슨LG

1) 김혜정, “미국 영업비밀보호법(Defend Trade Secrets Act)의 주요내용 검토 및 시사점”, Issue & Focus on IP, 2016. 12. 29, 2면.

2) 이경민, “영업비밀 요건으로서 비밀관리성에 대한 비교법적 고찰-미국과 일본의 법률과 판례를 중심으로-”, 법이론 실무연구 8권 1호, 한국법이론실무학회, 2020. 2, 323면.

3) 최근에는 코로나19로 인하여 미국이 2019년 ‘국가안보우려’로 블랙리스트에 올린 화웨이에 대해 새로운 규제책 즉 미국 반도체 제조 장비를 사용하는 외국기업은 화웨이에 반도체를 공급하려면 사전에 미국으로부터 허락을 받아야 하며, 화웨이는 미국 또는 미국의 장비를

와의 영업비밀 분쟁이 발생하여 이와 유사한 사건이 발생한 바 있다.<sup>4)</sup> 이처럼 영업비밀을 둘러싼 국가 간 소송이 최근 증가하고 있으며, 우리나라도 기업 간·국가간 영업비밀 침해에 대비하기 위해 미국의 영업비밀보호법을 참고하여 부정경쟁방지 및 영업비밀 보호에 관한 법률(이하 ‘부정경쟁방지법’이라 함)의 개정을 적극적으로 검토할 필요가 있다.

따라서 이하에서는 미국의 영업비밀보호법의 법제화 배경 및 영업비밀보호법의 주요 내용에 대해 살펴보고, 우리법제에서의 시사점을 제시하고자 한다.

## II. 미국 영업비밀보호법의 법제화 배경

미국의 경우 특허권, 상표권 및 저작권과 달리 영업비밀은 오로지 주법(state law)에 의하여 보호되고 있었다. 1979년 전국주법통일위원회(National Conference of Commissioners on Uniform State Law)에 의하여 완성된 통일 영업비밀보호법(Uniform Trade Secrets Act, 이하 ‘UTSA’라 함)은 뉴욕 주, 노스 캐롤라이나 및 메사추세츠 주를 제외한 47개 주에서 채택되었다.<sup>5)</sup> 그러

---

사용하는 외국기업으로부터 반도체를 계속 공급받거나 미국의 특정 소프트웨어와 기술이 들어간 반도체 설계를 사용할 때 미 상무부로부터 허가를 받도록 하여 미-중간의 무역전쟁 2차전에 돌입하였다(조민수, “미-중, 화웨이 둘러싸고 전면전 치달아”, IT DAILY, 2020. 5. 18자.

(<http://www.itdaily.kr/news/articleView.html?idxno=101138>))

- 4) 코로나19 팬데믹 여파가 확산되는 가운데 코로나19에 대응할 수 있는 핵심기술에 대한 탈취시도가 잇따르고 있다. 한국이 방역 우수 국가로 주목을 받고 한국 제약기업 등이 월등한 기술력을 보유하고 있다는 인식이 퍼지면서 불법적인 수단을 통해서라도 이를 확보하는 것이다. 실제로 코로나19 진단키트 제조사 대표 A씨는 중국시장 진출을 위해 중국식품의약품안전처(CFDA)의 위생허가증을 발급받아야 한다며 접근한 브로커에게 속아 자료기술을 보냈고 얼마 후 한 중국업체에서 유사한 진단키트를 만들고 있다는 사실을 알게 되었다. 또한 코로나19 치료약을 개발하고 있던 B사는 첨단 의료기술을 보유하고 있다고 주장하는 미국 스타트업으로부터 공동연구개발 프로젝트를 제의받았으나 이 스타트업은 갑자기 자금난을 호소하다 결국 프로젝트를 포기하였으나 이미 B사의 고급기술 자료는 미국으로 건너간 이후였다. 그리고 한 중국회사는 코로나19 백신을 개발하고 있는 국내 제약사 연구원 C씨에게 접근해 기존 연봉의 5배를 제시하며 영입을 제안했고 C는 일하던 회사에서 빼돌린 자료의 유용성에 따른 보상을 약속받고 중국회사에 약품 원가정보와 회사가 진행 중인 프로젝트 정보 등을 지속적으로 제공하다 적발되었다(강한, “코로나 대응 국내 핵심기술 보호 비상”, 법률신문, 2020. 4. 23자(<https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=161058>)).
- 5) 김양실, “미국 연방의회의 영업비밀보호법(Defend Trade Secrets Act) 제정·공포”, IP Insight 보고서, 한국지식재산보호원, 2016. 5. 13, 1면.

나 UTSA는 영업비밀 침해에 대한 형사적 제재를 규정하고 있지 않았기 때문에 일반적으로 주법 차원의 영업비밀보호는 민사적 구제에 한정된 것으로 이해되어 있었다.<sup>6)</sup> 그리고 UTSA를 채택한 주들은 내용의 변경 없이 동일하게 채택한 주들도 있었지만, 각 주의 환경에 맞게 변경하여 채택한 경우도 있었기 때문에 주별로 그 내용이 상이하여 통일성 문제가 제기되었다.<sup>7)</sup>

미연방의회에서는 1948년 영업비밀보호법(Trade Secrets Act)을 제정하여 연방공무원과 정부를 상대로 계약하는 상대방에게 영업비밀을 포함하여 정부의 기밀정보를 허가 없이 공개하는 것을 금지하였으나, 이는 주 정부나 지방 정부 공무원, 또는 민간부분의 고용인에게에는 적용되지 않았다.<sup>8)</sup>

1996년 연방의회는 경제스파이법(Economics Espionage Act, 이하 EEA라 함)을 제정하였고, 18 U.S.C. Section 1831-Economic espionage와 Section 1832-Theft of trade secrets에서 외국 기업의 이익을 위한 영업비밀의 부정취득(misappropriation)과 타인의 경제적 이익 제공을 위한 영업비밀 부정취득을 각각 범죄로 규정하였으나, 이는 검사의 기소가 있어야만 형사처벌 할 수 있었다.<sup>9)</sup> 즉 영업비밀 침해에 대한 민사적 구제를 위해서는 연방법원이 아닌 주(州)법원에만 소를 제기할 수 있으며, 적용되는 주법에 따라 동일한 사안에서 서로 다른 결과가 도출될 수 있다.

이에 따라 연방법에 의한 영업비밀보호에 관한 필요성은 지속적으로 제기되어 왔고, 영업비밀보호에 관한 입법안은 제113대 연방의회 때부터 꾸준히 발의되어 왔지만 영업비밀에 대한 일방적 압류조치 남용의 문제, 연방법원의 부담증가와 주법에 의한 보호방안이 이미 존재한다는 이유 등으로 반대에 부딪혀 왔다.<sup>10)</sup>

영업비밀보호법(Defend Trade Secrets Act of 2016, 이하 'DTSA'라 함)은 영업비밀보호에 관한 "18 U.S.C. Chapter 90-Protection of Trade Secret"을 개정하고자 제114대 미국 연방의회에서 제정하였다. DTSA는 2015년 7월 29일 Orrin Hatch 상원의원이 발의하여 2016년 4월 4일 상원을 통과하였고, 4월 27일 하원을 통과하여 마침내 2016년 5월 11일 오바마 대통령이 승인함에 따라

6) 다만 캘리포니아 주, 텍사스 주 등 일부 주에서는 관련법에서 영업비밀 침해에 대한 형사 처벌을 규정하고 있다(김혜정, 앞의 보고서, 3면).

7) 김양실, 앞의 보고서, 2016.5.13, 1면.

8) 유계환, "미국의 영업비밀 보호 동향 및 시사점", 한국지식재산연구원, Issue & Focus on IP, 한국지식재산연구원, 2015. 2. 6, 3면.

9) 김양실, 앞의 보고서, 1-2면.

10) 김양실, 앞의 보고서, 2면.

제정·공포되었다.<sup>11)</sup> DTSA는 영업비밀보호에 대한 통일성 확보 및 강화를 꾀하여 영업비밀 침해에 대한 연방차원의 형사적 구제뿐만 아니라 민사적 조치를 허용하고 있다. DTSA는 주법에 우선하는 것은 아니므로, 영업비밀 보유자는 본인의 선택에 따라 종래와 같이 각 주의 영업비밀보호법에 따른 보호를 받을 수 있으며, DTSA의 의한 보호를 받을 수도 있다.<sup>12)</sup>

#### <영업비밀 보호와 관련한 미국의 법률 체계의 변화><sup>13)</sup>



### 1. 통일영업비밀법(UTSA)

종래 미국에서는 각 주마다 서로 다른 내용의 영업비밀보호법을 두고 있어 각 주 영업비밀보호법에 대한 통일성 확보의 필요성이 대두되었다. 이러한 상황을 반영하여 통일법위원회(Uniform Law Commission, 이하 ‘ULC’라 함)는 통일적인 영업비밀보호법제 마련에 착수하였으며, 그 결과로써 1979년에 UTSA가 제정되었다. 동 법은 1985년에 개정된 바 있으며, 2020년 현재 뉴욕주를 제외한 49개주에 의해 채택되었다.<sup>14)</sup> UTSA는 주별로 상이한 영업비밀 관련 규율에 통일성을 갖추도록 하는 가이드라인이다. 즉 UTSA는 개별 주에서 제정하는 영업비밀보호와 관련한 법률의 모델이 되는데, 이는 가이드라인 또는 권고안이지 효력을 발생하는 법률은 아니다.<sup>15)</sup> 따라서 대부분의 주에서

11) 김양실, 앞의 보고서, 1면.

12) 김혜정, 앞의 보고서, 3면.

13) 박재영, “美 영업비밀보호법(DTSA) 제정과 산업분쟁 사례가 주는 시사점”, NARS 제26호, 국회입법조사처, 2020. 2. 5, 3면.

14) 2020년 1월 기준 뉴욕 주도 UTRA 채택안이 발의된 상태이다(美 통일법위원회 홈페이지 참조. (<https://www.uniformlaws.org>)).

15) 박재영, 앞의 보고서, 3면.

UTSA를 채택하였다고 하더라도 주마다 일부 내용이 다른 경우도 있고, 내용이 동일하다고 하더라도 구체적인 사안에 있어서 법률의 해석이나 적용이 달라지는 경우가 있다.

UTSA에서는 영업비밀을 ① 현실적 또는 잠재적으로 독립된 경제적 가치를 가지며, 일반적으로 알려져 있지 않고, 그 공개 또는 이용으로부터 경제적 가치를 얻을 수 있는 제3자에 의하여 정당한 수단으로는 쉽게 획득할 수 없으며, ② 비밀성을 유지하기 위하여 상황에 맞는 합리적인 노력이 기울여지는 정보를 말한다고 하고 있으며, 정보의 비공지성, 경제성, 비밀유지성을 요건으로 하고 있다. 그러한 대상으로 공식, 양식, 편집물, 프로그램, 도안, 방법, 기술, 공정 등을 열거하고 있다.<sup>16)</sup>

UTSA의 주요 내용은 영업비밀 침해에 대한 민사적 구제수단으로써 금지청구, 손해배상, 변호사비용, 비밀유지명령 등에 관해 규정하고 있다.

① 영업비밀이 실제로 침해되었거나 침해될 우려가 있는 때에는 금지청구를 할 수 있고, 예외적인 경우 영업비밀 침해로 인한 합리적 로열티 지급을 명할 수 있다(금지청구). ② 영업비밀 침해로 인하여 실제로 입은 손해, 실제 손해에 대한 손해배상액을 산정하는 것에 있어 고려되지 않았던 영업비밀의 침해로 발생한 모든 부당이득에 대하여 배상받을 수 있다. 또한 고의 또는 악의적인 영업비밀 침해의 경우에는 산정된 손해배상액의 2배를 초과하지 아니한 범위에서 징벌적 손해배상의 지급을 명할 수 있다(손해배상). ③ 법원은 고의 또는 악의로 영업비밀을 침해한 자에 대하여 합당한 변호사비용을 승소자에게 지불할 것을 명할 수 있다(변호사 비용). ④ 소송절차에서 영업비밀이 공개되지 않도록 해당 영업비밀에 대한 비밀유지, 비공개 심리, 소송기록 봉인 등을 명할 수 있다(비밀유지명령).<sup>17)</sup>

## 2. 경제스파이법(EEA)

영업비밀 침해 시 주법에 의한 민사적 구제가 가능하지만, 기업들은 영업비밀 침해에 대한 민사적 구제조치를 취하는 것에 적극적이지 않았다. 그 이유는 기업이 영업비밀 침해를 원인으로 한 민사소송의 비용이 고액이라는 점, 승소 가능성이 보장되지 않는다는 점, 영업비밀 침해를 주창하는 측에서 그 사실을

16) UTSA §1(4).

17) 김혜정, 앞의 보고서, 4-5면.

입증하기 어렵다는 점 등 때문이었다. 대체로 주법에서는 영업비밀 침해에 대한 형사적 제재 규정이 없었으며, 연방법에서는 영업비밀에 대한 형사적 제재 조치가 연방장물법(National Stolen Property Act, 18 U.S.C. 2314), 영업비밀법(18 U.S.C. 1905) 등에 분산되어 규정되어 있었다. 이러한 상황에서 인터넷 등 정보통신기술 발달로 인하여 외국 정부나 외국 기업에 의한 기술유출 내지는 영업비밀 침해가 심화되자, 주와 연방 차원의 영업비밀보호가 충분하지 않다는 인식이 확산되었다. 이에 따라 1996년 미국의회는 영업비밀 침해에 대한 형사적 제재를 위하여 EEA를 제정해 미국 연방형사법(18 U.S.C.) 제90장에 편입하였으며, 이로써 영업비밀보호 수준이 한층 강화되게 되었다.<sup>18)</sup>

EEA의 주요내용은 영업비밀 침해행위에 대한 형사처벌(징역, 벌금, 몰수)의 대상이 되는 행위를 ‘경제스파이(economic espionage)’와 ‘영업비밀절도(theft of trade secrets)’로 구분하여 처벌하고 있다.

<경제스파이와 영업비밀 절도 행위 비교><sup>19)</sup>

구분	적용대상	처벌
경제스파이	영업비밀을 침해하여 외국 정보, 외국 기업 등에 이익을 제공한 자	(개인) 15년 이하의 징역 또는 500만 달러 이하의 벌금
		(단체) 1,000만 달러 또는 침해된 영업비밀로 취득한 이익의 3배 이하의 벌금
영업비밀절도	주(州)간 또는 국제통상에서 사용되었거나 사용될 상품 또는 서비스와 관련된 영업비밀을 침해하여 영업비밀 보유자가 아닌 자에게 이익을 제공한 자	(개인) 10년 이하의 징역 또는 25만 달러 이하 또는 이득과 손실을 고려한 벌금
		(단체) 500만 달러 이하의 벌금, 관련된 재산이나 이득 몰수

EEA는 2012년 말에 경제스파이법에 대한 주요 내용을 개정하였는데, 바로 영업비밀 도용 명확화 법률(Theft of Trade Secrets Clarification Act)을 제정하여 EEA에서 정하고 있는 영업비밀 도용의 범위를 확대하였다. 즉 EEA 제 1832조에서 그 대상을 “주간 또는 외국과의 상거래를 위해 생산되거나 출시된 제품과 관련되거나 그 제품에 포함된 영업비밀” 문구를 “주간 또는 외국과의 상거래에 사용되거나 사용될 목적의 제품 또는 서비스와 관계되는 영업비밀”로 수정하였다.<sup>20)</sup>

18) 김혜정, 앞의 보고서, 5면.

19) 김혜정, 앞의 보고서, 6면.

20) 이는 2012년에 선고된 판결(United States v. Aleynikov, 676 F.3d 71, 75(2d Cir, 2012)에서 나타난 문제를 해결하기 위한 것이었는데, 골드만삭스(Goldman Sachs) 투자은행의 직원이었던 자가 회사 내부에서 사용하던 증권거래 관련 소프트웨어 소스코드를 무단 반출

또한 2013년에 제정된 외국 및 경제스파이 처벌 강화법(Foreign and Economic Espionage Penalty Enhancement Act)에 따라 외국과 관련된 영업 비밀을 취득·사용·공개 등의 행위를 한 경우에 EEA의 벌금이 대폭 상향 조정되었다. 이에 따라 개인에 대한 상한액은 기존 미화 50만 달러(약 5억 원)에서 미화 500만 달러(약 50억 원)로 10배 상향되었고, 법인의 경우에는 기존 미화 1천만 달러(약 100억 원)에서 현재의 미화 1천만 달러 또는 영업비밀 가치의 3배 중 큰 금액으로 변경됨으로써 영업비밀을 침해하여 얻은 이득이나 절약한 비용이 클수록 벌금도 그에 비례하여 늘어날 수 있도록 하였다.<sup>21)</sup>

또한 EEA에 의하여 영업비밀을 보호함에 있어서 함정수사의 방법을 적극적으로 채용하고 있으며, 구제수단으로는 벌금, 징역, 그것들의 병과 및 위반에서 얻는 재산의 몰수가 포함되어 있다.<sup>22)</sup>

### 3. 영업비밀보호법(DTSA)

미국에서는 오래전부터 영업비밀 침해에 대한 연방 차원의 민사적 구제수단 도입 필요성 및 타당성을 둘러싸고 활발한 논의가 진행되어 왔으며, 관련 법안도 제출된 바 있으나 입법으로 이어지지는 못하였다. 영업비밀 침해는 미국 경제에 심각한 손실을 끼치고 있음에도 불구하고 해킹 및 종업원에 의한 기밀 누출 등의 위협으로부터 연방 정부 차원의 법적 보호가 미흡하다는 비판이 지속적으로 제기되었고, 이러한 상황하에 발의된 DTSA는 백악관, 미국 상공회의소, 기술 기반 기업이 회원으로 소속된 미국 바이오산업협회 및 소프트웨어 단체 등의 강력한 지지와 미국의회의 초당적 합의에 따라 2016년 4월 4일 상원 통과(87:0), 2016년 4월 27일 하원통과(410:2), 2016년 5월 11일 오바마 대통령의 서명으로 시행되었다.

DTSA는 영업비밀 침해 시 당사자가 연방법원에 직접 제소할 수 있도록 허용한 최초의 법으로 동법에 따라 영업비밀에 대한 연방 차원의 보호가 형사적

하여 기소된 사건에서 항소심 법원은 경제스파이법 제1832조에서 그 대상을 “주간 또는 외국과의 상거래를 위해 생산되거나 출시된 제품과 관련되거나 그 제품에 포함된 영업비밀”이라고 명시하고 있기 때문에 회사 내부에서 사용하던 소프트웨어 소스코드는 ‘제품’에 해당하지 않는다고 하여 1심의 유죄판결을 뒤집는 판결을 선고하였다. 따라서 회사 내부에서의 사용을 위한 영업비밀도 경제스파이법의 보호대상에 포함시키기 위한 법 개정이 필요하였다(특허청, “꼭 알아야 할 해외 영업비밀 분쟁 대응 가이드-미국편“, 2015. 9, 16면).

21) 특허청 산업재산보호정책과, 앞의 책, 16면.

22) 전용태, “미국기업의 영업비밀 보호현황에 대한 실무적 연구”, 법이론실무연구 제6권 3호, 한국법이론실무학회, 2018. 8, 16면.



조치뿐만 아니라 민사적 조치로 확대되었다. 또한 ‘영업비밀의 정의’와 ‘영업비밀 부정이용 행위’ 확대를 통해 영업비밀의 보호 범위를 넓히고, 영업비밀 침해로 인한 민·형사상 제재 수위도 상향하는 등 결과적으로 영업비밀의 보호 수준이 크게 강화되었다.<sup>23)</sup>

DTSA의 제정으로 주(州)별 영업비밀보호법의 기능이 상실되는 것은 아니며, 영업비밀을 보유한 자가 침해당했을 경우 병존하는 양 법률 중 선택하여 연방법원 또는 주법원에 제소할 수 있고 경우에 따라서는 동시에 제소하는 것도 가능하다.

### Ⅲ. 미국 영업비밀보호법(DTSA)의 주요내용

#### 1. 영업비밀의 정의 및 침해행위(18 U.S.C. §1839)

##### (1) 영업비밀의 정의

DTSA는 UTSA와의 정합성을 위해 영업비밀의 정의를 UTSA와 유사하게 수정하고 영업비밀 부정이용(misappropriation)을 정의 조항(§1839)에 포함시켜 영업비밀 정의 및 침해행위의 범위를 확대하였다.

DTSA는 EEA상의 영업비밀에 대한 정의를 UTSA와 조금 더 유사한 방향으로 수정하였지만, DTSA와 USTA 간에는 아래 정의 비교와 같이 상당한 차이가 존재한다.

<UTSA와 DTSA의 영업비밀 정의 규정 비교>

UTSA상 영업비밀 정의 규정	DTSA상 영업비밀 정의 규정
제1조(정의) 동법에 사용되는 용어는 문맥상 달리 요구되지 않는 한 다음을 뜻한다. (4) 영업비밀은 공식, 패턴, 편집물, 프로그램, 도안, 방법, 기술 또는 과정을 포함한 정보로서 다음의 요건을 갖춘 것을 의미한다. (i) 현실적 또는 잠재적으로 독립된 경제적 가치를 가지고 있으며, 일반적으로 알려져 있지 않고, 그 공개 또는 이용으로부터 경제적 가치를 얻을 수 있는 타인이 정당한 수단에 의해 쉽게 알아볼 수 없고,	§1839 정의 동법에서 사용되는 용어는 다음을 뜻한다. (3) 영업비밀은 패턴, 계획, 편집물, 프로그램 장치, 공식, 디자인, 프로토타입, 방법, 테크닉, 절차, 프로그램 또는 코드를 포함한 모든 형태와 유형의 재정적, 상업적, 과학적, 기술적, 경제적 또는 공학적 정보로서 그 정보가 유형물이든 무체물이든, 어떠한 물리적, 전자적, 그래픽, 사진, 문서로 저장, 편집, 기억되었는지는 불문한다. (A) 영업비밀의 보유자는 비밀 정보를 유지하기

23) 김혜정, 앞의 보고서, 6면.

(ii) 비밀유지를 위하여 상황에 따른 합리적인 노력을 하여야 한다.	위하여 적절한 조치를 취하여야 하고, <sup>24)25)</sup> (B) 그 정보가 현실적 또는 잠재적으로 독립된 경제적 가치를 가지고 있고, 일반적으로 알려져 있지 않으며, 적절한 수단에 의해 쉽게 알아볼 수 없어야 한다.
--	--

DTSA는 영업비밀의 정의와 범위를 기존 UTSA와 EEA에서 규정하는 것보다 대폭 확대하여 권리자 또는 영업비밀 보유자에 대한 보호를 크게 강화하였다.

## (2) 처벌범위의 확대

영업비밀의 침해행위에 대해 “일반대중”을 삭제하고 “정보의 공개 혹은 사용으로부터 경제적 가치를 얻을 수 있는 다른 사람”으로 개정하여 영업비밀 절도나 경제스파이의 처벌범위를 확대하였다. 이로 인해 반드시 일반대중이 아니어도 침해를 인정받을 수 있게 되었다.

## (3) 도용(misappropriation)의 의미 명확화

도용은 영업비밀이 부정한 수단으로 얻어졌다는 것을 알거나 알 수 있었을 것으로 판단되는 사람이 다른 사람이 소유하고 있는 영업비밀을 취득 또는 이하와 같은 사람에 의해 명시적 혹은 묵시적 동의 없이 다른 사람의 영업비밀을 공개 또는 사용하는 것을 의미한다.

- ① 영업비밀의 지식을 취득하기 위해 부적절한 수단을 사용한 자
- ② 공개 혹은 사용시에 영업비밀의 지식이 다음과 같다는 것을 알았거나 알고 있었을 것으로 판단되는 자
  - 영업비밀을 취득하기 위해 부적절한 수단을 사용했던 사람으로부터 혹은

24) 적절한 조치를 취하는 것은 영업비밀 소유자의 책임이지만, 법원은 DTSA 이전의 소송에서 적절한 조치를 해석하면서 영업비밀의 법적인 보호를 위해 ‘난공불락의 요새’를 건설할 필요는 없다고 판시(Boston Scientific Corp. v. Dongchul Lee, No. 1:13-cv-13156-DJC (D. Mass.), Memo. and Order at 7, Dkt. 95 (citations omitted))한 바 있다(Bill McCabe/Gene Lee, “The New “Defend Trade Secrets Act”: What It Means And How It Can Be Utilized To Defend Against Trade Secret Misappropriation”, 2018. 12. 21). (<https://lotnet.com/the-new-defend-trade-secrets-act-what-it-means-and-how-it-can-be-utilized-to-defend-against-trade-secret-misappropriation/>)

25) 2009년부터 2018년까지 영업비밀 관련 소송사건을 분석한 결과, “영업비밀”의 정의를 충족시키기기 위해 원고가 도난당한 정보를 보호하기 위한 ‘합리적 조치’를 취하지 않아 영업비밀 관련 분쟁 사건에서 11%가 청구를 기각당했다(Winston&Strawn LLP, “Reasonable Measures’ For Protecting Trade Secrets: A Primer”. Feb 27, 2019 (<https://www.winston.com/en/thought-leadership/reasonable-measures-for-protecting-trade-secrets-a-primer.html>)).

그 사람을 통하여 유래되었다는 것을

- 영업비밀의 기밀성을 유지해야 하는 혹은 영업비밀의 사용을 제한해야 하는 의무가 있는 상황 하에서 취득되었다는 것을
- 영업비밀의 기밀성을 유지하기 위한 혹은 영업비밀의 사용을 제한하기 위한 구제조치를 추구하는 사람에게 의무를 진 사람으로부터 혹은 사람을 통하여 유래되었다는 것을
- 담당자의 직책에서 중대한 변경이 있기 전에 그 영업비밀에 해당하는 것 및 영업비밀이 사고 혹은 실수로 취득된 것을 알았거나 알 이유가 있었을 것으로 판단되는 자로부터 취득한 것을 의미한다.

영업비밀의 도용(부정이용)에 대한 정의는 기존 UTSA와 크게 다르지 않지만 피고 또는 제3자에 의한 기존 의무인 도난에서 위반까지 광범위한 행위가 포함되고<sup>26)</sup> 연방차원에서 영업비밀의 침해행위를 정의하였다는데 의미가 있다.

#### (4) 부적절한 수단(improper means)

부적절한 수단은 도난, 뇌물, 허위진술, 비밀유지의무의 위반 또는 위반유혹, 전자 혹은 다른 수단을 통한 스파이 행위 그리고 역설계(reverse engineering), 독자적 개발 또는 다른 합법적인 취득수단을 포함하지 않는 방법으로 획득하는 행위를 의미한다.

## 2. 소송절차에서 영업비밀 유지를 위한 조치 강화(18 U.S.C. §1835)

DTSA 시행 전에도 법원이 소송절차에 있어 영업비밀의 기밀성 유지를 위해 필요하고 적합한 명령 또는 조치를 취할 수 있도록 하는 내용의 규정이 있었으나 DTSA에서는 이를 보다 세밀하게 규정하여 소송절차에서 영업비밀이 포함된 자료가 제출될 경우 영업비밀 유지를 보장하기 위한 법원의 의무를 강화하고 있다.

법원은 영업비밀 보유자가 관련 자료에 대한 영업비밀 유지의 필요성에 대해 소명하여 봉인한 진술서를 제출할 수 있도록 허용하고 있으며, 영업비밀 보유자의 명백한 동의가 없는 한 소송절차에서의 영업비밀 공개가 영업비밀에 대한 보호를 포기하는 것이 아님을 명시하고 있다.<sup>27)</sup>

26) Peter J. Toren, "Misappropriation of a Trade Secret Under the DTSA", 2016. 6. 10.  
(<https://www.ipwatchdog.com/2016/06/10/misappropriation-trade-secret-dtsa/id=69826/>)

27) 18 U.S.C §1835(a)(b).

### 3. 민사적 구제방안(18 U.S.C. §1836)

일반적으로 영업비밀 침해에 대한 민사적 조치는 주법에 의해, 형사적 조치는 연방법에 의하는 것으로 이해되었으나 연방법인 EEA에도 침해행위 방지를 위한 민사소송 절차에 관한 규정을 두고 있었다. 다만, EEA에서는 법무부 장관이 민사소송을 통해 영업비밀 침해에 대한 금지청구를 할 수 있도록 하고, 연방법원이 그 민사소송에서 전속관할을 갖는 것으로 규정하였다. 즉 영업비밀 보유자는 연방법원에 대하여 영업비밀 침해를 근거로 한 민사소송을 직접 제기할 수는 없었다.<sup>28)</sup>

DTSA는 영업비밀이 주간 또는 국제통상에서 사용되었거나 사용될 예정인 상품이나 서비스와 관련된 것이라면 침해된 영업비밀의 보유자가 연방법원에 직접 제소할 수 있도록 허용하고 있다.<sup>29)</sup>

#### (1) 일방적 압류명령(18 U.S.C. §1836(b)(2))

법원이 당사자 일방의 신청에 따라 영업비밀 침해의 확산을 방지하기 위해 필요한 재산의 압류를 명할 수 있도록 하는 일방적 민사상 압류 조항을 두어 압류명령의 요건, 압류명령송달 등을 명확히 하고 있다.<sup>30)</sup>

영업비밀의 확산 또는 전파를 방지하기 위하여 예외적으로 “특별한 경우 (extraordinary circumstances)”에 해당할 때에 침해혐의자의 관련 자산을 압류할 수 있다. 이러한 압류명령은 침해혐의자에게 별다른 공지가 없이도 이루어질 수 있다.

#### 1) 압류명령 발동을 위한 요건

압류명령을 구하는 자는 다음의 요건을 충족시켜야 한다.

- ① 다른 형법상의 구제수단이 충분하지 않다는 점
- ② 압류조치가 취해지지 않으면 즉각적이고 회복할 수 없는 손해가 발생된다는 점
- ③ 영업비밀 보유자에게 발생하는 손해가 침해혐의자 등에게 발생하는 손해보다 크다는 점

28) 김혜정, 앞의 보고서, 8면.

29) 18 U.S.C §1839(b)(1).

30) 18 U.S.C §1836(b)(2).

- ④ 영업비밀이 존재하며, 이 영업비밀이 부정한 방법으로 침해되었다는 점
- ⑤ 압류대상자가 실제 영업비밀을 보유하고 있으며, 압류 대상물도 보유하고 있다는 점
- ⑥ 압류명령이 적용되는 대상물과 그 대상물의 위치를 파악하고 있을 것
- ⑦ 침해혐의자가 증거를 숨기거나 훼손할 수 있다는 점
- ⑧ 영업비밀 보유자가 압류 명령을 알리지 않았을 것

## 2) 압류명령의 내용

압류명령이 조문내용에 근거하여 발행될 경우, 그 명령은 다음의 사항을 포함하여야 한다.

- ① 명령을 위해 요구되는 사실에 대한 조사결과와 법률의 결론을 명시할 것
- ② 본 조항의 목적을 달성하는데 필요한 최소한 범위의 재산 압류를 제시해야 하며, 압류는 제3자의 영업활동방해를 최소한으로 하는 방법으로 실시되도록 지시해야 하고, 영업비밀을 남용한 것으로 고소당한 자의 합법적인 영업활동에 지장을 주지 않아야 함.
- ③ 그 당사자들이 법정에서 청문회를 가질 때까지 그 명령이 발행되는 당사자 혹은 다른 사람들에 대한 부당한 손해를 방지하기 위해 압류재산이 신청자 혹은 그 명령을 받은 사람에 의한 접근을 금지함으로써 그리고 전부 혹은 부분적 압류재산에 대한 복사를 금지함으로써 압류재산이 공개되지 않도록 보호하는 명령이 수반되어야 함.
- ④ 압류를 집행하는 법집행관에게 다음의 상황을 포함하여 집행관의 권한을 명확히 기술한 지침을 주어야 함.

- 압류가 진행될 수 있는 시간
- 봉쇄구역에 접근하게 위해 물리력을 사용할 수 있는지 여부

## 3) 청문회 마감기한

압류명령을 받은 당사자와 명령에 의해 해를 입은 사람들이 청문회의 다른 날짜에 동의하지 않는 한 가능한 한 가장 빠른 시일 내에 그리고 그 명령이 발행된 지 7일 이전에 청문회 날짜를 잡아야 한다. 다만 명령을 받은 당사자 혹은 명령에 의해 해를 입게 되는 사람은 명령을 승인 받은 신청자에게 통지가 제공된 후 그 명령을 폐기 혹은 수정해달라고 어느 때고 법원에 신청할 수 있다.

#### 4) 담보금의 공탁

법원은 본 조항에 따라 초과압류 혹은 잘못되었거나 과도하게 시도된 압류의 결과로서 보상받을 수 있는 손해배상을 위해 적절하다고 판단된 담보를 제공받을 수 있도록 요구할 수 있다.

#### 5) 공개방지 보호

법원은 명령을 승인 받은 사람에 의해 혹은 그 사람의 명령에 의해 본조항에 의거한 명령을 받는 사람이 그러한 명령과 그에 따른 압류와 관련하여 공개되는 것으로부터 보호하기 위한 적절한 보호조치를 취하여야 한다.

#### 6) 법원의 압류물 보관

##### ① 원칙

본 조항에 따라 압류된 모든 물건은 법원의 관리하에 두어야 하며, 법원은 압류 동안 그리고 보관기간 동안 압류물건에 물리적 및 전자적 접근되는 것을 막아야 한다.

##### ② 저장매체

압류물건이 저장매체를 포함하고 있거나 또는 압류물건이 저장매체에 저장되어 있을 경우 법원은 해당 매체가 청문회 때까지 양 당사자의 동의가 없는 한 네트워크 혹은 인터넷에 연결되지 않도록 보호해야 한다.

##### ③ 기밀유지보호

법원은 명령을 받은 자가 물건 공개에 동의하지 않는 한 압류명령을 받은 영업비밀 정보와 무관한 압류물건의 기밀성을 보호하기 위한 적절한 조치를 취해야 한다.

##### ④ 특별관리인 임명

법원은 모든 납용된 영업비밀 정보를 파악 및 분리하면서 재산을 압류한 자에게 무관한 재산 및 데이터의 반환을 용이하게 하기 위하여 특별관리인을 임명할 수 있다. 법원에 의해 임명된 특별관리인은 법원에 의해 승인된 상호 비밀유지 계약(non-disclosure agreement)에 의거하여 법적 구속력을 받기로 동의해야 한다.

#### 6) 명령서의 전달 및 전문가의 참여 결정

법원은 명령서 사본제시 및 집행, 그리고 명령서를 획득하기 위한 신청인의 신청서 제출을 명령서에 따라 압류를 수행하게 될 법집행관이 하도록 명령해야 한다. 법원은 주 또는 지방 법집행관이 참여할 수 있도록 허용할 수 있으나 신청자 혹은 신청자의 대리인에게 압류과정에 참여하도록 허용할 수 없다.

법집행관의 요청에 따라 법원은 전문가 참여로 인해 효과적인 압류진행과 압류부담이 최소화 된다고 판단되는 경우 신청자와 아무 관계가 없으면서 법원이 승인한 비밀유지계약에 의해 구속을 받게 되는 전문가를 압류과정에 참여하는 것을 허용할 수 있다.

#### 7) 압류청문회

##### ① 일자

압류명령을 발부하는 법원은 법원이 정한 일자에 청문회를 개최해야 한다.

##### ② 입증책임

본 조항에 따른 청문회에서 명령을 승인받은 당사자는 해당 명령서를 지지하는데 필요한 법적 판단과 결론을 입증해야 하는 부담을 가지며, 당사자가 그 같은 입증부담을 충족시키지 못할 경우에는 압류명령은 종료되거나 적절하게 변경되어야 한다.

##### ③ 명령의 종료 또는 변경

명령을 받은 당사자 혹은 그 명령으로 인해 해를 입는 자는 언제든지 그 명령을 승인받은 당사자에게 통지를 한 후 명령의 종료 혹은 변경을 해달라고 법원에 신청할 수 있다.

##### ④ 압류물 발견시간 제한

법원은 본 조항에 따른 청문회 목적의 훼손을 방지하기 위해 필요한 때에는 민사소송에 관한 연방규칙에 따라 발견을 위한 시간제한을 변경하는 명령을 할 수 있다.

#### 8) 잘못된 압류로 인한 손해배상청구

잘못된 혹은 과도한 압류로 인해 손해를 입은 자는 그러한 압류가 결정된

해당 명령의 신청자를 상대로 손해배상을 청구할 수 있으며, 연방 상표법 (Trademark Act of 1946)에 따른 구제조치에 대한 권리를 갖는다.<sup>31)</sup> 조문에 따라 법원에 맡겨진 담보금은 제3자의 손해보상을 제한하지 않는다.

#### 9) 암호화 신청

압류물건에 이해관계가 있다고 주장하는 자는 일방적 청문이 가능하며, 저장매체에 저장되어 있는 것으로서 압류되었거나 압류될 물건을 암호화 해달라는 신청은 언제나 요구할 수 있다. 이러한 요청은 가능한 경우에 암호화 방법을 포함해야 한다.

#### (2) 민사소송으로 인한 피해구제책(18 U.S.C. §1836(b)(3))

영업비밀 남용과 관련하여 영업비밀 도용 물품들을 압류당하여 입는 피해를 최소화하기 위하여 민사소송에서 법원은 다음의 조치를 취할 수 있다.

##### 1) 금지명령 및 침해금지 가처분(Injunction)

법원은 영업비밀이 실제로 침해되었거나 침해될 우려가 있는 때에는 금지명령을 할 수 있고, 예외적으로 금지명령이 부적절한 경우 영업비밀 침해로 인한 합리적 로열티 지급을 명할 수 있다.<sup>32)</sup>

영업비밀 보유자는 침해금지 가처분 신청을 통하여 영업비밀의 부정취득과 그 위협을 예방할 수 있다.

법원은 합리적이라고 간주하는 조건하에 실제 혹은 그럴 위험성이 있는 남용을 방지하기 위해 금지명령을 할 수 있으나 다음 사항을 포함하지 않아야 한다.

- 개인이 고용관계를 체결하지 못하게 하는 것(그러한 고용조건은 단순히 개인이 알고 있는 정보에 기반하지 않고 가능성이 있는 남용의 증거에 기반하여야 함)
- 합법적인 직업, 거래, 또는 사업의 실행에 제한을 금지하는 주법과 충돌되는 경우
- 예외적으로 금지가 불공평한 경우, 미래에 영업비밀을 합리적인 로열티를 지불하고 사용하기로 하고 그 기간 동안인 경우

31) 15 U.S.C. §1116(d)(11).

32) 18 U.S.C §1836(b)(3)(A).



그러나 DTSA상에서 “노동자와 사용자 간의 고용계약 체결에 대한 금지(prevent a person from entering into an employment relationship)”는 명령할 수 없다. 고용과 관련된 제한은 단지 영업비밀을 알고 있다는 사실만으로는 부족하며 “부정취득 위협의 증거(evidence of threatened misappropriation)”가 있어야 한다. 그러나 DTSA는 “부정취득 위협”에 대하여 정의하고 있지 않으므로 다툼의 여지가 있다.

## 2) 손해배상

법원은 영업비밀 침해로 인하여 실제로 입은 손해, 실제 손해에 대한 배상액을 산정하는 데 있어 고려되지 않았던 영업비밀 침해로 발생한 모든 부당이득에 대한 배상을 명할 수 있으며, 다른 방법으로는 손해배상을 대신하여(in lieu of damages) 합리적 로열티를 명할 수 있도록 하였다. 고의 또는 악의적인 영업비밀의 침해의 경우에는 산정된 손해배상액의 2배를 초과하지 아니한 범위에서 징벌적 손해배상의 지급을 명할 수 있다.<sup>33)</sup>

손해배상의 범위에 대해 구체적인 금액을 정하는 기준은 다음과 같다.

- 영업비밀의 도용으로 인해 야기된 실제 손해
- 실제 손실에 대한 손해배상을 계산하는데 다루어지지 않은 영업비밀의 도용으로 야기된 부당이득
- 다른 방법으로 측정된 손해 대신에 도용자에 의한 영업비밀의 불법공개 또는 사용에 대한 합리적인 로열티 책임 부과로 측정된 도용에 의한 피해액
- 영업비밀이 고의로 그리고 악의적으로 도용된 경우 보상할 금액의 2배 이하의 피해액
- 영업비밀이 고의로 또는 악의적으로 도용된 경우에는 승소한 당사자에게 합리적인 변호사비용보상

## (3) 소멸시효(18 U.S.C. §1836(d))

민사소송은 관련된 도용이 발견되거나 또는 합리적 주의를 기울였으면 발견될 수 있었던 날부터 3년 이내에 개시될 수 있다. 이 조항의 목적을 위해 계속적인 도용은 하나의 도용행위로 본다.

33) 18 U.S.C §1839(b)(3)(C).

#### 4. 형사적 구제방안(18 U.S.C. §1832)

그동안 영업비밀 침해에 대한 형사적 제재는 기본적으로 EEA를 통해 이루어졌는데 DTSA에서는 영업비밀 침해의 형사처벌이 되는 두 가지 행위 중 하나인 영업비밀 절도(theft of trade secrets) 행위에 대해 그 처벌수위를 강화시켰다. 다만 경제스파이(economic espionage) 행위는 DTSA에 의하여 개정되지 않았다.

기업 등 단체가 영업비밀을 탈취하였을 경우 EEA에서는 최고 500만 달러 이하의 벌금을 부과하도록 규정하였으나, DTSA에서는 영업비밀 절도에 해당하는 행위를 한 단체에 대해 500만 달러 또는 침해된 영업비밀로 취득한 이익의 3배에 해당하는 금액 중 더 큰 금액에 해당하는 벌금을 부과하도록 하고 있다.<sup>34)</sup> 영업비밀로 취득한 이익의 산정에는 침해한 그 영업비밀을 이용하여 피할 수 있었던 연구 및 디자인 비용과 해당 영업비밀을 재현하는 데에 필요한 비용 등이 포함된다.

또한 단체 외의 자가 영업비밀을 유용하였을 때에는 10년 이하의 징역 또는 벌금(정해진 상·하한액은 없음)에 처하거나 이를 병과할 수 있다.<sup>35)</sup>

#### 5. 내부고발자에 대한 면책(18 U.S.C. §1833)

DTSA는 내부고발자가 위법한 사실을 알리기 위한 목적으로 자신이 속한 단체의 영업비밀을 연방기관, 주 정부, 법원에 공개한 경우에는 DTSA 또는 주(州) 영업비밀보호법에 따른 민·형사상 책임을 지지 않도록 하고 있다.

면책이 허용되는 경우는 영업비밀 공개가 ① 직접 혹은 간접적으로 연방, 주 또는 지방 정부의 관리 혹은 변호사에게 비밀리에 이루어진 경우나 ② 오로지 법 위반 혐의를 보고·조사할 목적으로만 이루어진 경우이다. 또한 영업비밀의 공개가 소송이나 기타 법적절차를 위해 제출된 공소장이나 다른 문서를 통해 이루어졌으며 그러한 문서가 봉인되어 제출된 경우에 해당된다.<sup>36)</sup>

보복금지 관련 소송에서 영업비밀 공개를 허용하고 있다. 위법행위의 혐의를 보고했다는 이유로 고용주로부터 보복을 당해 소송을 제기한 자는 관련 영업비밀을 자신의 변호사에게 공개할 수 있고 일정한 요건을 갖춘 경우<sup>37)</sup> 법정

34) 18 U.S.C §1832(b).

35) 18 U.S.C §1832(a).

36) 18 U.S.C §1833(b).

절차에서도 관련 정보의 사용이 허용된다.<sup>38)</sup>

고용주는 영업비밀 또는 기타 기밀정보의 사용과 관련해 직원(여기에는 계약관계에 있는 개인 또는 컨설턴트도 포함됨)과 체결하는 모든 계약이나 합의서에 동 조항에서 규정하고 있는 면책특권에 대해 고지하여야 한다.<sup>39)</sup> 영업비밀과 관련된 계약에 이를 명시하지 않는 경우, 해당 계약을 체결한 직원을 상대로 하는 소송에서 법원은 사용자 측에 징벌적 손해배상 또는 변호사비용 부담을 명할 수 있다.

한편, 다른 법률과의 해석문제를 규정하고 있는 동법 제1838조에 따라 내부 고발자 면책조항은 주법에 대해 우선하여 적용된다.<sup>40)</sup>

#### IV. 우리 법제에의 시사점

우리나라에서 영업비밀은 주로 부정경쟁방지법에 의해 보호되고 있다. 부정경쟁방지법의 개정을 통해 영업비밀에 대한 보호가 점차 강화되어 왔으나 우리 정부와 기업이 영업비밀침해에 적절하게 대응하지 못하고 있다는 비판은 지속적으로 제기되어 왔으며, 이러한 상황을 반영하여 우리나라도 영업비밀을 실효적으로 보호하기 위한 제도의 개선을 추진하여 왔다. 2016년 4월 6일에 중소기업의 기술유출 원인을 종합적으로 분석한 후 범정부차원의 종합적인 기술대책 마련을 위한 “중소기업 기술보호 종합대책(안)”을 발표하였으며, 2016년 8월 부정경쟁방지법 개정을 통해 ① 영업비밀 정의규정을 정비하여 구성요건을 완화하고 영업비밀의 침해유형을 확대하여 영업비밀보호를 강화, ② 영업비밀을 악의적으로 침해한 경우 3배 이내의 손해배상액을 인정하는 징벌적 손해배상제도의 도입, ③ 영업비밀 침해행위 등의 범죄에 대한 양형기준을 강화하는 내용으로 입법예고를 하였으나 개정에 이르지 못하였다.<sup>41)</sup> 2019년 1월 8일에 부정경쟁방지법 개정안이 통과되었고 2019년 7월 9일부터 시행되어 영업비밀보호를 강화하고 있다. 그 주요 내용은 ① 보호대상이 되는 영업비밀의 요건

37) 해당 영업비밀이 포함된 문서를 봉인된 상태로 제출하였을 것, 법원의 명령에 따른 경우를 제외하고는 해당 영업비밀을 공개하지 않을 것을 요구하고 있다(18 U.S.C §1833(b)).

38) 18 U.S.C §1833(b)(2)(A)(B).

39) 18 U.S.C §1833(b)(3).

40) 18 U.S.C §1838.

41) 산업통상자원부공고 제2016-422호, “부정경쟁방지 및 영업비밀 보호에 관한 법률 일부개정법률(안) 입법예고”, 2016. 8. 18.

완화(제2조 제2호),<sup>42)</sup> ② 영업비밀 침해행위에 대해 손해액의 3배 범위내에서 징벌적 손해배상제도 도입(제14조의2 제6항, 제7항),<sup>43)</sup> ③ 영업비밀 침해행위의 유형 확대, ④ 영업비밀 침해행위에 대한 벌칙수준 상향(제18조 제1항, 제2항),<sup>44)</sup> ⑤ 영업비밀 침해 예비·음모범에 대한 벌금을 상향(제18조의3)<sup>45)</sup>하는 등 현행 제도의 운영상 나타난 미비점을 상당 부분 보완하였다. 또한 2019년 1월 정부는 ‘산업기술 유출 근절대책’을 발표하였고 그 주요 내용은 ① 국가 핵심기술 보유기업을 대상으로 해외 인수·합병시 사전승인제를 도입하고, ② 산업기술 유출시 징벌적 손해배상제도를 도입하여 최대 3배의 손해를 배상하게 하며, ③ 범죄수익환수 대상을 확대하는 등의 제도 개선에 나선다는 내용을 담고 있다.<sup>46)</sup>

부정경쟁방지법의 개정과 정부의 산업기술 유출 근절대책의 발표에도 불구하고 업계에서는 해외 국가의 처벌 수준에 비해 국내 기술유출에 따른 처벌이 약해 그 실효성이 떨어진다는 평가를 하고 있으며 이는 최근에 있었던 기술유출 판례에서도 드러나고 있다.<sup>47)</sup> 실제로 2015년 국가 핵심기술인 ‘힘센엔진(HiMSEN)’주요부품 설계도면 유출하려 했던 현대중공업의 하청업체 대표는 징역 1년 6개월, 하청업체 회사 법인은 벌금 5000만원을 선고받았고,<sup>48)</sup> 현대중

42) 2019. 7. 9. 이전의 영업비밀 정의 규정에는 ‘공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서 합리적인 노력에 의하여 유지된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보’로 되어 있었으나 이 규정을 ‘공언히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 비밀로 관리된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보’로 변경하였다.

43) 영업비밀 침해행위가 고의적인 것으로 인정되는 경우에는 손해로 인정된 금액의 3배를 넘지 아니하는 범위에서 배상액을 인정할 수 있도록 하면서, 영업비밀의 침해행위가 고의적인지 판단할 때에는 침해자의 우월적 지위 여부, 고의의 정도, 침해행위의 기간 및 횟수, 침해행위로 인하여 침해자가 얻은 이득의 정도 등을 고려하도록 영업비밀 침해에 따른 피해구제를 강화하였다.

44) 부정한 이익을 얻거나 영업비밀 보유자에게 손해를 입힐 목적으로 영업비밀을 지정된 장소 밖으로 무단유출하거나 영업비밀 보유자로부터 영업비밀의 삭제 또는 반환을 요구받고도 이를 계속 보유하는 행위 등도 영업비밀 침해행위로서 처벌하도록 하고, 영업비밀 침해행위에 대한 벌칙을 종전에는 원칙적으로 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알면서도 한 경우에는 10년 이하의 징역 또는 1억원 이하의 벌금, 그 밖의 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금으로 하던 것을, 앞으로는 각각 15년 이하의 징역 또는 15억원 이하의 벌금, 10년 이하의 징역 또는 5억원 이하의 벌금으로 상향하였다.

45) 기존 영업비밀 침해 예비·음모범의 경우 3년 이하의 징역 또는 2천만원 이하의 벌금에 처하던 것을 3년 이하의 징역 또는 3천만원 이하의 벌금으로 상향하였다.

46) 산업통상자원부, “산업기술 유출 근절대책 발표”, 2019. 1. 3 보도자료 참고.

47) 김재민, “날로 복잡해지는 기술유출 사고, 법국가적 해결책 마련돼야”, 뉴스락, 2019. 5. 30자. (<http://www.newslock.co.kr/news/articleView.html?idxno=19003>)

공업과 현대건설기계는 하도급업체의 기술을 유용하여 다른 하청업체에게 넘긴 혐의로 공정위원회의 시정명령과 과징금 4억 3100만원의 처분을 받았을 뿐이어서<sup>49)</sup> 미국의 처벌기준에 비하면 그 규모가 작은 편이다.

영업비밀보호에 관한 해외 주요국의 보호강화 동향 및 영업비밀 침해로 인한 산업상의 피해를 고려할 때 영업비밀에 대한 보다 강력하고 실효적인 보호를 위한 관련법의 개정이 필요하다.

## 1. 영업비밀 정의에 대한 개선필요

부정경쟁방지법 제2조 제2호는 “‘영업비밀’이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 비밀로 관리된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.”라고 규정하고 있다. 영업비밀로 성립되기 위해서는 ① 공공연히 알려져 있지 아니한 것(비공지성)으로서 공개된 간행물 등에 게재되지 않고 비밀상태이며, 보유자를 통하지 않고서는 입수할 수 없는 것을 의미하며, 다만 비밀유지의무자(보안서약서)에 대한 공개는 제외한다. ② 기술상·경영상 경제적 가치가 있는 것(경제적 유용성)으로서 경영상의 이익을 얻을 수 있거나 또는 정보의 취득이나 개발을 위해 상당한 비용이나 노력이 필요한 경우를 의미한다. ③ 비밀로 관리되는 것(비밀 관리성)으로서 정보가 비밀이라고 인식될 수 있는 표시를 하거나 고지를 하고, 정보에 접근할 수 있는 대상자나 접근방법을 제한하고 비밀준수의무를 부과하는 등 객관적으로 정보가 비밀로 유지 및 관리되고 있다는 사실이 인식 가능한 상태를 의미한다.<sup>50)</sup> 즉 영업비밀로 인정되기 위해서는 비공지성, 경제적 유용성, 비밀 관리성의 세 가지 요건을 만족하여야 한다.<sup>51)</sup>

48) 김선호, “국가핵심기술 ‘힘센엔진’ 도면 빼돌린 부품업체 대표 실형”, 연합뉴스, 2019. 3. 17자. (<https://www.yna.co.kr/view/AKR20190315089900051?input=1195m>)

49) 안종호, “공정위, ‘기술자료 유용’ 현대건설기계·현대중공업 제재” 아시아투데이, 2019. 5. 29자. (<http://www.asiatoday.co.kr/view.php?key=20190529010017891>)

50) 영업비밀보호센터 홈페이지 참조(<https://www.tradesecret.or.kr/institution/requirement.do>)

51) 특히 비밀 관리성에 대한 명확한 기준을 정하고 있지 않아 실제 분쟁에 있어서는 법원의 판단에 의할 수밖에 없다. 이번 개정에 의하여 부정경쟁방지법에서 비밀 관리성에서 합리적 노력을 삭제하고 비밀로 관리로 그 요건을 완화시켜서 기존 판례에서 요구되었던 접근제한과 객관적 인식가능성을 위한 기업의 합리적 노력의 수준까지는 요구되지 않고 대상 영업비밀이 기업 내·외에서 비밀이라고 인식할 수 있는 정도(비밀의 표시와 접근제한)에서 인정될 수 있으며 기업이 회사의 일반정보와 영업비밀을 구체적으로 구별하지 않고 어떠한 조치도 취하지 않았을 경우에는 비밀 관리성이 부정된다고 보여진다(이경민, 앞의 논문, 329면).

부정경쟁방지법은 영업비밀을 비공지성, 경제적 유용성, 비밀 관리성의 세 가지 요건을 만족하는 것을 내용으로 하면서 포괄적으로 정의하고 있다.

미국의 경우 DTSA §1839(3)에서 “영업비밀을 패턴, 계획, 편집물, 프로그램 장치, 공식, 디자인, 프로토타입, 방법, 테크닉, 절차, 프로그램 또는 코드를 포함한 모든 형태와 유형의 재정적, 상업적, 과학적, 기술적, 경제적 또는 공학적 정보로서 그 정보가 유형물이든 무체물이든, 어떠한 물리적, 전자적, 그래픽, 사진, 문서로 저장, 편집, 기억되었는지는 불문한다.”라고 정의하여 구체적인 예시들을 제시하고 있다.

기술과 서비스가 발전함에 따라 영업비밀의 범위도 복잡·다양화되고 있으나 부정경쟁방지법은 이를 지나치게 포괄적으로 기술하여 영업비밀 분쟁에서 다툼의 여지가 커지고 있다. 따라서 이를 개선하기 위해서는 영업비밀에 해당하는 종류를 설명하는 예시규정을 법률에 도입하는 방안을 고려해보아야 할 것이다.<sup>52)</sup>

## 2. 영업비밀 도용에 대한 일방적 압류제도 도입 필요

미국은 영업비밀을 도용당한 영업비밀보유자가 신청할 경우 극히 예외적인 경우에 한해 법원이 구체적인 확인을 거친 후 영업비밀 유출을 막기 위한 일방적인 민사압류를 허용하고 있다. 이러한 일방적 압류제도는 침해혐의자에게 별다른 공지가 없이도 이루어질 수 있다. 구체적으로는 법원은 ① 다른 형법상의 공평한 구제수단이 충분하지 않을 것, ② 압류명령이 되지 않을 경우 즉각적이고 회복 불가능한 손실이 발생할 것, ③ 압류명령을 받게 되는 자가 영업비밀을 부정한 방법으로 침해하고 있을 것, ④ 압류대상자가 영업비밀 및 압류대상물을 가지고 있을 것 등을 확인하여야 한다. 그리고 법원은 반드시 압류된 물건을 보관하고 보호하여야 하며, 7일 이내에 압류에 대한 청문회를 실시해야 한다. 이 경우 청문회 대상자는 압류물의 암호화를 신청할 수 있다. 만약 잘못되거나 과도한 압류로 인해 피해를 보게 된 당사자는 압류명령의 종료 또는 변경을 요청할 수 있으며, 압류명령의 신청자를 상대로 손해배상을 받을 수도 있다.

이러한 미국의 일방적 민사압류제도는 부정경쟁방지법에서는 없는 제도이다. 한국의 경우 부정경쟁방지법 제10조에 따라 영업비밀침해 피해에 대한 예방적

52) 박재영, 앞의 보고서, 7면.

차원에서 영업비밀 침해행위에 대한 금지청구권을 활용하고 있다. 부정경쟁방지법 제10조(영업비밀 침해행위에 대한 금지청구권 등)는 ① 영업비밀의 보유자는 영업비밀 침해행위를 하거나 하려는 자에 대하여 그 행위에 의하여 영업상의 이익이 침해되거나 침해될 우려가 있는 경우에는 법원에 그 행위의 금지 또는 예방을 청구할 수 있으며, ② 영업비밀 보유자가 제1항에 따른 청구를 할 때에는 침해행위를 조성한 물건의 폐기, 침해행위에 제공된 설비의 제거, 그 밖에 침해행위의 금지 또는 예방을 위하여 필요한 조치를 함께 청구할 수 있다고 규정하고 있다. 금지 및 예방청구권은 영업상의 이익이 침해되거나 침해될 우려가 있는 경우에 영업비밀 보유에 관하여 정당한 권원을 가지는 자 또는 사실상의 보유자인 영업비밀 보유자가 청구할 수 있으며, 특정한 제품의 생산을 일정기간 중지 또는 완성제품의 배포, 판매금지를 그 내용으로 하고 있다. 다만 ‘영업상의 이익이 침해될 우려’는 단순히 침해될 가능성만으로는 안 되고 침해될 것이 확실히 예상되는 개연성을 의미하기 때문에 사회통념상 객관적으로 영업상 이익이 침해될 가능성이 있어야 하며, 이에 대한 입증책임은 침해금지 청구권자가 입증하여야 한다.<sup>53)</sup>

영업비밀 침해행위의 금지 및 예방 청구권에 관해서는 통상 영업비밀 보유자의 신청에 의해 법원이 제소 전후를 불문하고 본안에 관한 최종심리 이전 단계에서 침해 피의자에게 잠정적으로 침해금지 명령을 내리는 가처분 신청을 제기하는 경우가 많다. 가처분을 제기하면 사안이 복잡하지 않은 경우 약 2-3주 간격으로 2번 정도의 심문기일을 열어 신속하게 재판이 종결되고 가처분이 인정되면 침해 피의자의 생산 및 판매가 중단되므로 가처분신청은 영업비밀 보유자에게는 매우 실효적이고 강력한 공격수단이 될 수 있다.<sup>54)</sup> 이러한 가처분 신청은 민사집행법에 의해서 진행되고 있다. 즉 부정경쟁방지법상 금지 및 예방청구권은 침해행위를 즉시 중지시키거나 예방시킬 수 있는 효과적인 방법이기는 하지만 본 조항에서는 영업비밀 침해금지 가처분이나 압류제도에 대해서는 규정하고 있지 않고 있다.

영업비밀 침해자의 추가적인 공개와 사용, 제품의 생산 및 판매 등 영업비밀의 유출 및 도용 등의 영업비밀 침해를 막지 못한다면 그 피해가 기하급수적으로 증가할 수도 있고 기업의 존폐에도 영향을 미칠 수 있을 것이다. 따라서 보완적인 측면에서 부정경쟁방지법에서 영업비밀 피해자의 보호를 위하여 피해자의 청구가 있을 경우 일방적 민사압류제도를 도입할 필요가 있을 것이다. 이는

53) 특허청, “기술보호의 초석 영업비밀 보호제도”, 2019. 12. 17, 80-82면.

54) 특허청, 앞의 책(각주 48), 129면.

영업비밀 유출에 따른 매출감소, 기업이미지 손상, 막대한 소송비용 등의 피해는 분쟁에서 승소한다고 하더라도 원상복구가 불가능하기 때문이다.<sup>55)</sup>

다만 정상적이고 합법적인 거래나 사업활동이 침해되지 않도록 신중하게 일방적 민사압류제도를 도입하여 운용할 수 있도록 미국의 일방적 압류제도를 참고하여 세밀하게 규정할 필요가 있으며, 악의로 영업비밀이 담긴 정보나 생산물에 대해 민사압류제도를 남발하지 못하도록 담보제공 제도 및 잘못된 압류명령으로 인한 피해를 충분히 보상할 수 있는 조치도 규정에 포함되어야 할 것이다.<sup>56)</sup>

### 3. 기술유출의 조직범죄에 대한 처벌 강화 필요

부정경쟁방지법은 2019년 개정에서 형사처벌의 구성요건을 정비하였다. 부정경쟁방지법 제18조(벌칙)는 영업비밀을 국외유출하는 경우 15년 이하의 징역 또는 15억원 이하의 벌금에 처하며, 벌금형에 처하는 경우 위반행위로 인한 재산상 이득액의 10배에 해당하는 금액이 15억원을 초과하면 그 재산상 이득액의 2배 이상 10배 이하의 벌금에 처하도록 하고 있다(제18조 제1항). 국내유출의 경우 10년 이하의 징역 또는 5억원 이하의 벌금에 처하며, 벌금형에 처하는 경우 위반행위로 인한 재산상 이득액의 10배에 해당하는 금액이 5억원을 초과하면 그 재산상 이득액의 2배 이상 10배 이하의 벌금에 처하도록 하고 있다(제18조 제2항). 또한 영업비밀 침해 예비·음모범에 대한 벌금도 국외유출은 3년 이하의 징역 또는 3천만원 이하의 벌금, 국내유출은 2년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 하고 있다(제18조의3).

기술유출의 경우 법인 등 기업이 적극 가담하여 조직적인 인력매수를 통한 영업비밀탈취 및 인력 스카웃 등을 한 경우 처벌을 강화할 필요가 있다. 영업비밀침해나 기술유출을 통해서 물건이나 서비스를 개발한 기업은 막대한 이익을 얻을 수 있으며, 영업비밀 침해에 있어서도 기획적인 영업비밀을 침탈한 기업의 처벌을 개인과 같은 수준에 두는 것은 형평성이 어긋난다.

미국의 경우 해외로의 영업비밀 유출을 규정한 EEA에서는 외국과 관련된 영업비밀을 취득·사용·공개 등의 행위를 한 경우에 개인에 대한 벌금액은 미화 500만 달러, 법인의 경우 1000만 달러 또는 영업비밀 가치의 3배 중 큰

55) 홍성삼, “미국 영업비밀방어법(DTSA) 배경 및 시사점 연구”, 가천법학 제12권 제4호, 가천대학교 법학연구소, 2019. 12, 68면.

56) 홍성삼, 앞의 논문, 69면 참조.



금액을 지불하도록 하고 있으며, DTSA에서는 영업비밀 절도에 해당하는 행위를 한 단체에 대해 500만 달러 또는 침해된 영업비밀로 취득한 이익의 3배에 해당하는 금액 중 더 큰 금액에 해당하는 벌금을 부과하도록 하고 있으며, 단체 외의 자가 영업비밀을 유용하였을 때에는 10년 이하의 징역 또는 벌금(정해진 상·하한액은 없음)에 처하거나 이를 병과할 수 있다.

그러나 부정경쟁방지법에서는 영업비밀을 침해한 개인과 법인을 똑같이 다루고 있을 뿐 법인에 대한 중과(重課)규정은 두고 있지 않다. 최근의 기술유출은 조직적으로 직원이나 기술자를 매수하는 방식 등으로 이루어지고 있고, 기업 등의 법인은 생산기반을 갖추고 있기 때문에 영업비밀 침해가 훨씬 더 용이할 뿐만 아니라 그 피해액이 크다고 할 수 있다. 따라서 영업비밀보호법에서도 개인과 법인의 처벌을 동일하게 취급할 것이 아니라 기업 등 법인에 의한 영업비밀 침탈행위에 대해서는 더 큰 벌금을 부과하여 기술유출 침해에 대한 억지력을 강화시킬 수 있도록 하여야 할 것이다.<sup>57)</sup>

#### 4. 부정경쟁방지법에 내부고발자 면책조항 도입 필요

공익적 또는 양심적 고발로 영업비밀이 알려진 경우에 이에 대한 면책조항이 부정경쟁방지법에 부재하여 내부고발자는 민·형사 소송을 당할 가능성이 있다. 예컨대 2016년 8월 현대자동차 내부직원이 자사 제품의 ‘세타Ⅱ엔진 등’ 결함 의심 사안 10건에 대해 미국 NHTSA 거래 업체에 제보한 사실에 대해 해당 기업이 직원을 검찰에 형사기소 한 사례가 대표적이다.<sup>58)</sup>

공익신고자 보호법 제14조(책임의 감면 등) 제1항에 따라 공익신고자는 그 형을 감경하거나 책임의 일부를 감면받을 수 있으나 이때에는 국민권익위원회의 감면 요구가 선행되어야 하고 이마저도 의무규정이 아니어서 실효성이 크다고 보기 어렵다. 또한 성광 다단계 사건에서 대법원의 판결에 따르면 공익신고자라 할지라도 공익신고자 보호법상의 형의 감경이나 면제는 필수적인 것이 아니고 법원의 재량에 속한다고 판단하고 있다.<sup>59)</sup>

57) 조용순, “2019년 개정 영업비밀보호법 및 산업기술보호법에 대한 검토 : 민·형사적 구제를 중심으로”, 시큐리티 연구 제61호, 한국경호경비학회, 2019. 12, 345-346면 참고.

58) 1년 후 해당기업은 고소를 취하였으나 검찰은 해당 직원을 기소혐의로 송치하였고 2017년 7월 수원지방법검찰청은 해당 직원에 대해 무혐의 처분을 결정하였다(김경환, “영업비밀 유출사건 최근 판례 등 동향”, 2017년 산업보안 국제 컨퍼런스 자료, 2017). (<https://www.slideshare.net/ssuserbd0159/ss-81138884>).

59) 김덕성, “공익신고자 형 감면은 법원 재량”, Legal Times, 2019. 3. 31자.

미국의 경우 내부고발자가 위법한 사실을 알리기 위한 목적으로 자신이 속한 단체의 영업비밀을 연방기관, 주 정부, 법원에 공개한 경우에는 일정한 요건을 만족하는 경우에 영업비밀보호법에 따른 민·형사상 책임을 지지 않도록 하고 있다. 또한 보복금지 관련 소송에 있어서도 위법행위의 혐의를 보고했다는 이유로 고용주로부터 보복을 당해 소송을 제기한 자는 관련 영업비밀을 자신의 변호사에게 공개할 수 있고 일정한 요건을 갖춘 경우 법정 절차에서도 관련 정보의 사용이 허용된다. 또한 고용주는 영업비밀 또는 기타 기밀정보의 사용과 관련해 직원(여기에는 계약관계에 있는 개인 또는 컨설턴트 포함)과 체결하는 모든 계약이나 합의서에 동 조항에서 규정하고 있는 면책특권에 대해 고지하여야 하며, 영업비밀과 관련된 계약에 이를 명시하지 않는 경우, 해당 계약을 체결한 직원을 상대로 하는 소송에서 법원은 사용자 측에 징벌적 손해배상 또는 변호사비용 부담을 명할 수 있다.

공익목적의 내부고발은 영업비밀 유출에 따른 손해보다는 공정한 거래관계의 확립, 기술 등 지식재산의 건전한 형성이라는 경제·사회적 이익이 더 크므로 미국 DTSA 제1833조를 참고하여 내부고발자에 대한 면책조항을 부정경쟁방지법에 신설하는 것을 검토할 필요가 있다.<sup>60)</sup>

## V. 결론

기업의 보안시스템이 과거 대비 고도화 되고 있음에도 불구하고 산업계의 기술유출사례는 증가하고 있다. 문제는 단순히 기술유출 사례가 증가하는 흐름인 것뿐만 아니라 그 경로가 점차 지능화·고도화되고 있다는 점이다. 이러한 기술유출의 증가는 국내 산업을 이끄는 기업들의 재무적인 손실 및 기술개발 위축 등의 내부적인 우려뿐만 아니라 글로벌 시대에서 우리 기술의 해외로의 유출 가능성도 높아지고 있다는 것이다.

실제로 2018년 국정감사에서 산업통상자원부와 국가정보원이 제출한 ‘산업기술유출 현황 및 적발현황’에 따르면 2013년부터 2018년 8월까지 산업기술 해외 유출 및 시도 적발건수는 152건에 달하며 업종별로는 전기전자 57건, 기계 31건, 조선·자동차 22건 등 주로 주력산업에 집중되어 있다. 이중 중소기업의

(<https://www.legaltimes.co.kr/news/articleView.html?idxno=45328>)

60) 박재영, 앞의 보고서, 7면.

기술 유출·시도는 102건으로 전체의 67%를 차지하며 이는 대기업 해외 산업 기술 유출건수인 35건(27%)의 3배에 달하였다.

부정경쟁방지법 개정과 정부의 산업기술 유출 근절대책 발표 등의 노력에도 불구하고 이해 당사자가 많아진 현 산업 시대에서 기술유출을 막기란 쉽지 않고 우리나라 기술보호 체계가 M&A 시도에 취약하고 유출피해의 심각성에 비해 국내 기술유출에 따른 처벌이 해외국가보다 약해 그 실효성이 떨어진다는 지적도 지속적으로 제기되고 있다. 또한 최근의 영업비밀 침해나 기술유출 유형이 해외 기업이 한국 회사를 속여 정보유출을 시도하는 경우, 협력업체에 정보를 제공하는 과정에서 정보가 유출되는 경우, 전·현직 직원이 내부정보를 유출하는 경우뿐만 아니라 해킹, 디도스 공격, 랜섬웨어 등의 디지털을 기반으로 하는 유출 사례도 적지 않게 발생하고 있다. 특히 IT강국인 우리나라의 경우 영업비밀 중에서도 기술정보에 대한 위협에 대비하고 침해가 발생했을 시에 강력한 대응이 필요할 것이다. 따라서 현재 경쟁국 업체들의 빈번한 영업비밀 절취 시도에 대해 적절한 대응을 할 수 있는 법제를 갖추어 우리나라의 경제안보는 물론 국가안보의 보호를 위한 노력을 꾸준히 진행해나가야 할 필요가 있다.

현재 영업비밀보호 법제를 가장 탄탄하게 갖추고 있는 미국에서도 늘어나고 있는 자국 기업의 영업비밀에 대한 위협에 대해 예의주시하고 있으며, 입법개선을 통해 영업비밀보호의 강화를 도모하고 있다. 따라서 우리나라도 미국의 영업비밀보호법제를 검토하여 우리나라의 영업비밀보호 법제의 정비 및 강화를 꾀할 필요가 있다. 따라서 부정경쟁방지법에 영업비밀의 정의에 대한 구체적인 예시규정 마련, 영업비밀 도용에 대한 일방적 민사압류제도 도입, 기술유출의 조직범죄에 대한 법인의 중과규정 마련, 내부고발자 면책규정 마련 등을 통해 영업비밀 보호제도의 규제 개선을 할 필요가 있다.

[참고문헌]

<논문>

- 이경민, “영업비밀 요건으로서 비밀관리성에 대한 비교법적 고찰-미국과 일본의 법률과 판례를 중심으로-”, 법이론 실무연구 8권 1호, 한국법이론실무학회, 2020. 2.
- 전용태, “미국기업의 영업비밀 보호현황에 대한 실무적 연구”, 법이론실무연구 제6권 3호, 한국법이론실무학회, 2018. 8.
- 조용순, “2019년 개정 영업비밀보호법 및 산업기술보호법에 대한 검토 : 민·형사적 구제를 중심으로”, 시큐리티 연구 제61호, 한국경호경비학회, 2019. 12.
- 홍성삼, “미국 영업비밀방어법(DTSA) 배경 및 시사점 연구”, 가천법학 제12권 제4호, 가천대학교 법학연구소, 2019. 12.

<단행본>

- 특허청, “꼭 알아야 할 해외 영업비밀 분쟁 대응 가이드-미국편“, 2015. 9.
- \_\_\_\_\_, “기술보호의 초석 영업비밀 보호제도”, 2019. 12. 17.

<보고서 등>

- 김경환, “영업비밀 유출사건 최근 판례 등 동향”, 2017년 산업보안 국제 컨퍼런스 자료, 2017.
- 김양실, “미국 연방의회의 영업비밀보호법(Defend Trade Secrets Act) 제정·공포”, IP Insight 보고서, 한국지식재산보호원, 2016. 5. 13.
- 김혜정, “미국 영업비밀보호법(Defend Trade Secrets Act)의 주요내용 검토 및 시사점”, Issue & Focus on IP, 2016. 12. 29.
- 박재영, “美 영업비밀보호법(DTSA) 제정과 산업분쟁 사례가 주는 시사점”, NARS 제26호, 국회입법조사처, 2020. 2. 5.
- 유계환, “미국의 영업비밀 보호 동향 및 시사점”, 한국지식재산연구원, Issue & Focus on IP, 한국지식재산연구원, 2015. 2. 6.
- Bill McCabe/Gene Lee, “The New “Defend Trade Secrets Act”: What It Means And How It Can Be Utilized To Defend Against Trade Secret Misappropriation“, 2018. 12. 21.
- Peter J. Toren, “Misappropriation of a Trade Secret Under the DTSA”, 2016. 6. 10.

Winston&Strawn LLP, “Reasonable Measures’ For Protecting Trade Secrets: A Primer”. Feb 27, 2019.

<기타>

산업통상자원부공고 제2016-422호, “부정경쟁방지 및 영업비밀 보호에 관한 법률 일부개정법률(안) 입법예고”, 2016. 8. 18.

산업통상자원부, “산업기술 유출 근절대책 발표”, 2019. 1. 3 보도자료.

[Abstract]

A Study on the Review and Implication of  
the Defend Trade Secrets Act of United States

Kim, Yun-Jeong\*

Despite the advancement of corporate security systems compared to the past, the number of technology outflow in the industry is increasing. The problem is that not only is the number of technology leakages increasing, but the way is gradually becoming more intellectualization and advancement. This increase in technology outflows has brought internal concerns, such as financial losses and a contraction in technology development by companies leading the domestic industry. In addition, the possibility of overseas outflow of our technology in the global age is also increasing.

Despite the government's efforts to amend 'Unfair Competition Prevention and Trade Secret Protection Act' and announce 'Measures to Eradicate Industrial Technology Leakage', it is not easy to prevent technology leakage in the current industrial era with many stakeholder. And it has been continuously pointed out that the nation's technology protection system is vulnerable to M&A attempts and the punishment for domestic technology leakage is weaker than that of foreign countries compared to the seriousness of the spillage damage.

In particular, in the case of Korea, an IT powerhouse, it is necessary to prepare for threats to technical information among strong trade secrets and to respond strongly when infringement occurs. Therefore, it is necessary to continue efforts to protect national security as well as the nation's economic security with legislation that can properly respond to the current attempts by rival companies to steal frequent trade secrets.

Even in the United States, which has the strongest trade secret protection legislation, it is keeping tabs on the growing threat to trade secrets of US

---

\* Law Research Institute Chungbuk National University, Associate Researcher.

companies, and is seeking to strengthen trade secret protection through improved legislation. Therefore, Korea needs to review the United States Trade Secrets Protection Act to overhaul and strengthen the nation's Trade Secrets Protection Act. In other words, the Unfair Competition Prevention and Trade Secret Protection Act is necessary to prepare specific example rules for the definition of trade secrets, introduce a unilateral civil seizure system for the theft of trade secrets, prepare heavy regulations for corporations for organized crimes of technology leakage, and to prepare exemption rules for whistle-blower.

Keywords : Trade Secrets, Defend Trade Secrets Act,  
Uniform Trade Secrets Act, Economics Espionage Act,  
Unfair Competition Prevention and Trade Secret Protection Act

