개인 및 기업의 정보 수집을 위한 산업기술보안법제 정비 방안

김 용 진*

차 례

* 충남대학교 법학전문대학원 교수, 법학박사
접수일자 : 2015. 10. 30. / 심사일자 : 2015. 11. 25. / 게재확정일자 : 2015. 11. 30.

Ⅰ. 산업기술보호 법제의 현황과 예방적 보호법제 구축 및 개인정보 보호법제와의 공조의 필요성

오늘날 산업기술은 기업의 생존조건을 넘어 국가안보와 국민경제에 커다란 영향을 미친다. 그런데 첨단기술이 발전하는 속도에 비례하여 첨단기술의 유출범죄도 비례하여 증가하고 있다. 특히 불법적인 방법에 의하여 첨단기술이 유출되거나 기술보유 국내기업이 해외인수합병 또는 외국기업과의 합작투자 등의 방법으로 국가핵심기술이 유출되는 경우도 적지 않다. 이에 따라 각국은 산업기술, 특히 첨단기술의 유출을 방지하고자 법적, 제도적 체제를 정비하고 있다. 법제도적 규율형태에는 불법유출에 대한 형사벌적 처벌을 강화하는 방법과 핵심기술을 보유하고 있는 국내기업의 해외인수 합병 또는 외국기업과의 합작투자 등에 대한 승인이나 사전신고 제도 채택 등 행정법적 규율방식이 주를 이룬다. 이는 산업기술보호 법제가 사후적 구제조치를 넘어 사전적 예방제도로 발전해 가고 있음을 보여준다.

그런데 산업기술의 불법유출에 대한 사전예방적 조치가 여전히 미흡하다. 2011년 개정「산업기술의 유출방지 및 보호에 관한 법률」(이하 "산업기술보호법")은 산업기술침해행위를 하거나 하려는 자에 대하여 그 행위로 인하여 영업상의 이익이 침해되거나 침해될 우려가 있는 경우에는 법원에 그 행위의 금지 또는 예방을 청구할 수 있도록 하는 내용의 침해행위에 대한 금지청구권제도를 신설하였다(같은 법 제14조의2). 이는 사전적 대응방안임은 분명하나, 문제는 산업기술을 침해하거나 하려는 자를 특정지우는 일이 쉽지 않고, 또 유출위험과 관련된 자에 대한 개인정보를 수집할 수 없다면 법원에의 금지청구권은 무의미하며 사전적 예방조치도 불가능에 가깝게 되고 만다. 이러한 사정은 우리나라의 경우 산업기술을 유출한 자를 신분별로 조사한 결과 현직직원 27%, 퇴직직원 65% 등으로 나타난 통계[1]에 비추어 크게 문제된다. 현직직원은 물론 퇴직직원 등에 대한 개인정보 수집 및 그 동향 파악이 필요할 것인데, 이는 개인정보보호법제에 의하여 커다란 제약을 받는다. 이와 같은 사실은 산업기술 유출방지를 위한 법제를 단지 산업기술에 대한 보호를 강화하는 방안만으로는 부족하고,

1) 국가정보원, 첨단 산업기술 보호 동향, 제8호, 5쪽.

다른 법 영역, 특히 개인정보보호 법제와의 공조를 통하여 해결하여야 할 문제임을 알려준다.

위와 같이 산업기술 유출방지를 위한 개인정보 수집의 필요성이 점증하고 있음에도 불구하고 현행「부정경쟁방지 및 영업비밀보호에 관한 법률」(이하 "부정경쟁방지법")은 물론 산업기술보호법 또한 넓은 의미에서 사후적 구제수단일 뿐 보호가치 있는 기술유출을 예방하는 제도로는 미흡하다. 산업기술보호법 제5조에 따라 산업통상부장관이 산업기술의 유출방지 및 보호에 관한 종합계획을 세우고, 같은 법 제37조의 예비·음모죄 처벌을 실효성 있게 운영하게 하여 산업기술보안을 확보하기 위해서는 잠재적으로 유출우려가 있는 자에 대한 개인정보를 수집할 수 있도록 하여야 할 것이다. 아래에서는 종래 산업기술 보호 문제가 개인정보 수집을 통한 사전적 유출방지에 관한 연구가 거의 없다는 점에 착안하여, 개인에 대한 정보수집이 가능한 방향으로 개인 및 기업의 정보를 수집할 수 있는 방향으로 산업기술보호법 정비 방안을 제안하고자 한다.

II. 현행법상 산업기술 유출(우려)자에 대한 개인·기업 정보 수집 가능 여부

1. 현행 산업기술법제의 사전적 예방기능의 미비점

우리나라 현행 산업기술에 대한 법적 보호는 이원적 체제로 이루어져 있다. 국내산업기술의 유출규제에 관한 법제는 부정경쟁방지법과 산업기술보호법이 있다. 다음으로는, 부정경쟁방지법은 기술이 유출되고 난 뒤에 피해기업을 구제하고 산업기술을 이미 유출한 자의 처벌에 치중하여 산업기술의 사후적 구제제도로서 기능하고 있는 반면에, 산업기술보호법은 국내 산업기술의 보호를 위한 제도적 기반의 구축을 위한 법적 근거를 마련하여 보호에서 보안체제로 격상시켰다고 평가할 수 있다. 현행법은 산업기술을 보호하기 위하여 기술유출행위에 대하여 형사처벌을 강화하고 있을 뿐 아니라 예비·음모에 대해서도 처벌하는 규정을 두고 있으며(부정경쟁방지법 제18조의3, 산업기술

보호법 제37조), 이와 함께 산업기술의 침해행위에 대한 금지청구권(산업기술보호법 제14조의2) 제도를 두고 있을 뿐 아니라 국가핵심기술 및 국가연구개발사업으로 개발한 산업기술에 대한 침해행위가 발생할 우려가 있거나 발생한 경우 기관장이 이를 신고토록 하고, 이에 기하여 정보수사기관장이 필요한 조치를 취할 수 있도록 하고 있다(산업기술보호법 제15조).

그러나 기술유출행위에 대한 처벌을 강화하는 것만으로 적절한 대응방안인지 의문이다. 산업기술에 대한 보호 강도가 높을수록 기술과 지식의 확산과 활용이 제한되어 산업전체적으로 볼 때 기술개발활동의 제약은 물론 혁신자원의 활용과 네트워킹에 장애사유로 작용할 수 있으며, 이러한 제약은 결국 해외연구소 및 IT 다국적 기업의 연구센터 유치에 걸림돌로 작용할 위험이 크다.[2] 그러나 무엇보다 현행법상의 처벌제도는 사후적 보호방안이라는 점에서 유출을 차단시키는 사전적 보호방안에 미치지 못한다. 산업기술을 유출우려가 있는 자에 대한 관리시스템이 없는 한, 사적적 대응이나 구제는 사실상 어렵기 때문이다. 특히 사이버공간에서의 국외유출의 시도를 차단하기 위하여 유출위험자들에 대한 동향의 감시와 자료수집 및 포렌직 시스템도 갖추어야 할 것이다.[3] 그럼에도 불구하고 현행 산업기술보호 법제는 물론 개인정보 법제에 이에 관하여 아무런 규정을 두고 있지 않다. 이와 같이 기술유출우려자에 대한 개인정보 및 자료수집에 대한 필요성은 2002년 미국 외국인투자위원회가 엑슨-플로리어법(Exon-Florio Act)에 따라 국가안보의 우려를 이유로 산업기술을 보유한 미국회사를 인수하려는 홍콩기업에 대해 미국인을 임원으로 임명하고, 통신보안 관련 종사자에 대한 정보제공을 조건으로 하여 승인한 사건을 통해서도 확인할 수 있다.[4]

---

2) 황철, "핵심기술유출의 현황 및 대응",「지식재산권연구센터 포럼」 자료, 2005, 6쪽; 황인표, "IT분야기술유출방지에 관한 법제도적 연구",「연세대학교 일반대학원 석사학위논문」, 2004, 81쪽.

3) 조광훈, "첨단기술 유출범죄의 발생원인과 대응방안",「지식재산21」, 2010/4, 13쪽.

4) 상세는, 손승우, "2011년 개정 산업기술의 유출방지 및 보호에 관한 법률안의 분석",「경원법학」 4권, 2011, 237-238쪽 참조.

2. 현행 개인정보보호에 관한 법규에서 정보수집이 가능한 경우 및 그 한계

(1) 개인정보와 기업정보의 수집 가능성

1) 개인정보보호법

개인정보의 기본법이라 할 수 있는「개인정보보호법」은 개인정보처리자(공공기관, 법인, 단체 및 개인 등)가 스스로 처리하는 개인정보를 보호하도록 하기 위한 법률이다. 이 경우 개인정보는 '성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보'를 말한다(개인정보보호법 제2조 제1호).

산업기술유출가능성은 산업기술에의 접근성을 전제로 하기 때문에, 개인정보는 산업기술 유출우려자의 범위를 정하는데 유용할 것이다. 예컨대 국가적으로 중요한 산업기술을 보유하고 있는 기업에서 당해 기술을 취급하여오던 자가 퇴직 등의 사유로 직장을 떠나게 된 경우 그 기업으로부터 그러한 사람들의 인적사항을 파악할 수 있다면, 산업기술 유출우려자의 대상 범위를 쉽게 파악할 수 있게 될 것이다.

위와 같이 산업기술을 유출하려는 정황은 파악되었는데, 그 당사자가 누구인지 알기 어려운 때에는 개인정보보호법을 활용할 수 있을 것이다. 다만, 산업기술의 보안이 이미 특정된 자를 전제로 하여 그의 유출우려행위를 사전에 탐문하는 것을 주된 내용으로 하는 경우에는 개인정보보호법이 제공할 수 있는 정보제공은 제한적일 수밖에 없을 것이다. 이와 같은 경우에는 개인의 신상정보보다는 산업기술을 유출할 우려가 있는 특정의 자가 유출을 예비하거나 음모하는 과정에 관한 정보를 입수하는 것이 보다 효과적이기 때문이다.

물론 위와 같은 개인정보를 입수하기 위해서는 개인정보처리자가 개인정보를 제3자에게 제공할 수 있는 법적 근거가 있어야 하는데, 이와 관련하여 개인정보보호법은 다른 법률에서 이에 관한 특별한 규정을 두고 있거나(개인정보보호법 제18조 제2항 제2호), 범죄의 수사나 공소의 제기 등 공공기관이 필요한

경우에 한하여 허용하고 있다(같은 조 같은 항 제5호 내지 제9호).

2) 기업정보 수집 및 활용 가능성 검토

나아가 산업기술보안을 위한 기업정보 수집의 필요 또한 시급한 시대상황을 맞이하고 있다. 산업기술의 유출을 방지하기 위해서는 보호대상인 산업기술 자체에 대한 정보와 그 기술을 다루는 사람에 대한 관련 정보를 수집할 수 있어야 한다. 특정한 산업기술이 유출방지 등으로부터 보호를 받아야 할 만한 가치가 있는가를 판단하기 위한 정보에는 산업기술의 내용은 물론, 그 기술을 제품에 활용하여 판매된 매출데이터 등에 관한 정보 등도 수집되고 활용되어야 한다. 유출주체와 관련하여서는 당해 기업에서 문제의 기술을 다룬 사람에 대한 정보가 필요한데, 이는 결국 개인정보보호법에 따라 규율될 사항이다. 여기에 속하는 사항으로 직원의 출퇴근, 근무기록 데이터, 인사기록 데이터 등이 있다.

기업의 매출데이터 등 기업이 보유한 산업기술관련정보와 기업의 직원 정보 등에 대한 정보를 입수할 수 있는가의 여부는 양자를 분리하여 그 법적 근거를 검토하여야 한다. 개인정보보호법의 보호대상은 살아있는 개인이므로(개인정보보호법 제2조 제1호), 기업의 산업기술관련정보의 보호 내지는 제3자 제공에 관한 규정 등이 적용될 여지가 없다. 산업기술관련정보는 산업기술보호법 또는 부정경쟁방지법에 따라 보호받게 될 것인데, 이들 법은 기업정보에 대한 수집 및 활용에 관한 규정을 두고 있지 않다. 기업정보 중 직원의 출퇴근, 근무기록데이터, 인사기록데이터 등 기업의 직원정보는 기업이 개인정보처리자로서 개인정보보호법에 따라 보호하고, 이 법이 정하는 바에 따라 그 처리정보를 제3자에게 제공할 수 있다. 다만, 산업기술보호법 제15조 및 개인정보보호법 제18조 제2항 제5호에 따라 보호위원회의 심의·의결을 거쳐 그 직원에 관한 개인정보를 제3자에게 제공할 수 있는 개인정보처리자가 공공기관인 경우에 한하므로(개인정보보호법 제18조 제2항 단서), 기업의 경우에는 개인정보법 제18조 제2항 제5호를 이용할 수 없을 것이다.

(2) 정보통신망 이용 및 정보보호 등에 관한 법률(이하 “정보통신망법”)

정보통신망법의 목적은 정보통신서비스를 이용하는 자의 개인정보를 보호하고 정보통신망의 건전한 이용에 그 목적이 있으므로(정보통신망법 제1조 참조), 정보통신망에서의 개인정보보호법인 동시에 다른 이용자에 의한 사생활침해나 명예훼손을 방지하는 것을 주된 내용으로 한다. 이에 따라 정보통신망을 통하여 일반에게 공개되는 정보에 의하여 사생활 침해나 명예를 훼손당한 자는 정보통신서비스제공자에게 삭제 등을 요구하거나(제44조의2) 침해이용자의 정보제공을 청구할 수 있다(같은 법 제44조의6). 위와 같이 정보통신망법은 건전한 정보통신망 이용이라는 측면에서 프라이버시나 명예훼손 등을 침해받은 자의 권리구제를 위해 이용자 정보의 제공청구권을 인정하고 있으므로, 산업기술유출혐의자에 대한 정보수집 제도로서의 효용성의 거의 없다 할 것이다.

(3) 전기통신사업법

「전기통신사업법」은 통신비밀을 보호하는 동시에, 일정한 경우 전기통신사업자에게 정보수집에 공여할 자료의 열람이나 제출(이하 “통신자료제공”) 요청에 응하도록 규정하고 있다(제83조 제1항 및 제3항). 여기의 통신자료에는, 이용자의 ①성명 ② 주민등록번호 ③주소 ④ 전화번호 ⑤가입일 또는 해지일 뿐만 아니라, ⑥아이디도 포함된다(제83조 제3항 각호). 그런데 정보제공의 근거 사유는 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해방지로 제한적으로 열거되어 있다. 이에 따라 산업기술유출이 수사의 대상으로 된 경우에는 검사 또는 정보수사기관의 장이 전기통신사업자에게 산업기술유출자 내지는 유출우려자에 대한 통신자료(이용자의 아이디 포함)의 제출을 요구할 수 있다. 산업기술의 유출을 국가안전보장에 대한 위해로 볼 수 있는지 의문이나, 국가핵심기술의 경우에는 긍정하여도 무방할 것이다. 물론 이는 어디까지나 개인정보자기결정권이나 익명표현의 자유를 본질적으로 침해하지 아니한 범위 안에서 운영되어야 할 것이다. 예컨대 모색적 내지 탐색적 증거를 확보하기 위한 방편으로 이용할 수는 없다고 보아야 한다. 최근 하급심 법원도 인터넷

포털사이트 게시물 작성자의 인적 사항 일체를 제공하여 달라는 수사기관의 요청에 응한 인터넷 정보제공 사업자의 손해배상책임을 인정함으로써, 무분별한 개인정보제공 관행에 제동을 거는 판결을 선고한 바 있다.[5] 이와 같이 수사기관이 법익침해사실을 구체적으로 적시하는 대신 일단 특정인의 인적 사항 일체를 제공받아 이를 이용하여 범죄사실을 구체화시키려는 모색적 증거 활동은 엄격히 제한되어야 할 것이다.

(4) 통신비밀보호법

「통신비밀보호법」은 예외적으로 통신비밀보호법, 형사소송법 또는 군사법원법의 규정에 의하여 우편물의 검열·전기통신의 감청(이하, "통신제한조치") 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취할 수 있도록 허용하고 있다(통신비밀보호법 제3조). 통신비밀보호법은 범죄수사와 국가안보를 위해 필요한 경우 엄격한 요건 아래에서 보충적인 수단으로 이용할 것을 요구한다(통신비밀보호법 제3조 제1항 및 제2항, 제5조, 제7조). 그런데 산업기술 유출은 형법상 업무상배임죄에 해당하므로(형법 제356조), 통신비밀보호법이 허용하는 통신제한조치의 대상이 되지 아니하며(통신비밀보호법 제5조제1호 참조), 또한 이를 국가안전보장 침해라고 보기 어렵고 설사 이에 해당된다 하더라도 법원(고등법원 수석부장판사)의 허가(통신비밀보호법 제7조 제1항 제1호) 또는 대통령의 승인을 받아야 한다(같은 항 2호). 다만 검사 또는 사법경찰관이 수사를 위하여 전기통신사업자에게 통신사실확인자료는 요청할 수 있다(통신비밀보호법 제13조 제1항, 제15조의2 참조).

(5) 소결

산업기술유출자 또는 유출우려자에 대한 신상정보는 현행 개인정보보호법에 따라 수집하고 이를 활용할 수 있다. 다만, 범죄의 수사나 공소의 제기에 필요한 범위 안에서 가능하므로, 수사 이전의 단계에서는 수집할 수 없는 한계가 있다. 현행법상 기업정보 중 기술 자체에 관한 정보나 판매데이터 등에 관한 정보를

5) 서울고등법원 2012. 10. 18. 선고 2011나19012 판결.

수집할 수 있는 법적 근거가 없다. 정보통신망법은 통신망 운영자와 이용자간, 이용자 상호간의 문제를 규율하므로 산업기술 유출혐의자에 대한 정보수집제도로는 활용하기 어렵다. 정보수사기관의 장은 전기통신을 이용하는 이용자가 산업기술을 유출할 우려가 있는 경우 그의 아이디 등 통신자료를 전기통신사업자에게 요청할 수 있다. 통신비밀보호법이 허용하는 통신제한조치는 범죄수사의 경우에 허용되는 범죄의 유형에 들어 있지 않으며, 국가안전보장의 위해는 국가핵심기술에 한하여 허용할 수 있을 것이다.

3. 현행법의 적극적 해석을 통한 정보수집가능성 검토

(1) 유출우려자의 대상설정 단계 : 산업기술보호법과 개인정보보호법의 해석 문제

산업기술 보유기관의 장은 산업기술에 대한 유출이나 침해의 행위가 발생할 우려가 있거나 발생한 때에는 산업통상자원부장관 및 정보수사기관의 장에게 신고하여 필요한 요청을 할 수 있으며, 산업통상자원부장관 및 정보수사기관의 장이 이와 같은 요청을 받거나 유출이나 침해행위를 인지하면 필요한 조치를 취하여야 한다(산업기술보호법 제15조). 그런데 산업기술보호법에는 필요한 조치의 내용과 그 범위에 대한 규정이 존재하지 아니하나, 첫 단계로 행위자의 인적 사항이 파악되어야 할 것이다. 그런데 인적 사항은 개인정보이며 이는 개인정보보호법에 따라 규율될 것이다. 개인정보보호법은 제18조 제2항 제5호에서 “개인 정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우”에는 개인정보를 제3자에게 제공할 수 있도록 허용한다. 기술유출우려자의 개인정보가 파악되지 않고서는 산업통상자원부장관이나 정보수사기관의 장이 필요한 조치를 취할 수 없을 것이므로, 이들은 개인정보보호법 제18조 제2항 제5호에 따라 공공기관에 해당하는 개인정보처리자에게 개인정보를 청구할 수 있다고 볼 것이다.

(2) 침해행위에 대한 정보의 수집 및 활용 단계

1) 통신자료의 수집

산업기술보호법은 이 법 또는 그 위임입법에서 보호하는 산업기술을 침해하는 행위를 금지하고 있는데(산업기술보호법 제14조), 만약 그러한 행위가 발생할 우려가 있거나 발생한 때에는 산업통상자원부장관이나 정보수사기관의 장은 '필요한 조치'를 취할 수 있다(산업기술보호법 제15조 제2항). 여기의 필요한 조치에는 전기통신사업법상의 통신자료제공의 요청이 포함된다고 해석된다. 따라서 산업기술을 유출할 우려가 있는 자가 침해행위과정에서 전기통신을 이용한 경우, 정보수사기관의 장은 유출우려자(이용자)의 인적 사항이나 그의 아이디에 관한 정보를 제공받을 수 있을 것이다.

2) 우편물의 검열 또는 전기통신의 감청

산업기술 유출우려자와 관련한 우편물을 검열하고 그가 이용한 전기통신을 감청하기 위해서는 통신비밀보호법이 허용하는 경우에 해당하여야 한다. 그런데 통신비밀보호법은 그 자체 또는 형사소송법이나 군사법원법에서 따로 규정한 경우에 한해서만 통신제한조치를 허용한다(통신비밀보호법 제3조). 현행 형사소송법이나 군사법원법은 허용조항을 두고 있지 않고 통신비밀보호법만이 예외규정을 두고 있다. 통신비밀보호법은 '국가안보'와 일정한 '범죄의 수사'를 위한 경우에 한하여 통신제한조치 또는 긴급통신제한조치를 허용한다(통신비밀보호법 제5조 내지 제8조). 산업기술유출은 형법상 업무배임죄를 구성하여 형법상 범죄일 뿐 아니라 산업기술보호법이 금지하는 행위 또한 범죄를 구성할 것이지만, 통신비밀보호법 제5조 제1항 제1호에서 열거하는 형법상 범죄에 업무상 배임죄(형법 제356조)가 포함되어 있지 않으며, 여타의 각 호에도 산업기술보호법에 규정된 범죄를 규정하고 있지 않다. 결국 현행법상 기술유출이라는 범죄의 수사를 위하여 우편물을 검열하거나 전기통신을 감청할 법적 근거가 없다.

산업기술의 유출, 특히 해외유출이 국가안전보장에 위해가 되는지 여부도 문제이다.

헌법 제18조가 보장하는 통신비밀의 자유는 국가안전보장, 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있다. 통신비밀보호법은 통신제한조치의 사유로 국가안전보장과 질서유지를 들고 있으며, 통신비밀자유의 본질적인 내용이 침해되지 않도록 하기 위하여 가중요건을 부가하고 있다(헌법 제37조 제2항 후단, 통신비밀보호법 제5조 제1항 및 제7조 제1항 참조). 산업유출에 대해서는 이를 인정하는 견해와 부정하는 견해가 있을 수 있지만, 경우를 나누어 살펴야 할 것이다. 통상의 기술은 기업의 사익에 관한 사항이므로 그 유출을 국가안보와 결부시키는 것은 무리라고 보아야 할 것이지만, 국가핵심기술이 해외로 유출되는 경우에는 사익을 넘어 공익에 대한 침해라고 보아야 할 것이다. 현행 산업기술보호법도 국가핵심기술이 해외로 유출될 경우 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 미치는 것으로 평가하고 있기 때문이다(산업기술보호법 제2조 제2호). 나아가 국가핵심기술이 국내에 유출되는 경우에도 국가안전보장에 대한 상당한 위험이 예상된다고 보아야 할 것이다. 오늘날 통신의 발달로 지구촌시대가 도래한 상황에서 국내유출은 잠재적인 해외유출로 간주하여도 무방할 것이기 때문이다. 결국 산업기술의 유출은 통신제한조치를 정당화할 사유가 되지 못하는 것이 원칙이고, 다만 국가핵심기술이 유출되거나 유출될 우려가 큰 경우에는 통신비밀보호법 제7조에 따라 통신제한조치를 취할 수 있고, 이 경우 고등법원 수석부장판사의 허가(내국인 경우) 또는 대통령의 승인(외국인 경우)을 얻어야 한다.

3) 온라인서비스제공자의 정보제공의무

가. 문제점

산업기술침해를 이유로 침해우려가 있는 자에 대한 개인정보를 인터넷포털 운영자에게 요구할 수 있는지 문제이다. 산업기술 유출이 인터넷을 이용하여 행해지는 경우가 빈번하므로, 이를 허용할 경우에는 사후적 구제는 물론 유출을 사전에 방지시킬 수 있게 되어 기술유출에 대한 매우 유용한 대응책이 될 수 있을 것이다. 이 문제는 결국 인터넷에 접근한 개인의 정보에 관한 문제이므로 인터넷에 의하여 개인의 명예가 훼손된 경우에 유저의 개인신상 정보를 제공하게 할 수 있느냐의 문제와 궤를 같이 한다.

나. 비교법적 검토

미국의 경우, 1986년 사생활보호에 관한 법률(ECPA) 중 제2편의 일명 저장통신법(Stored Communications Act; SCA)은 인터넷서비스제공자(ISP)가 익명의 인터넷 사용자의 신원을 파악할 수 있는 정보를 공개할 수 있는 반면에, 인터넷 통신 내용의 공개는 수정헌법 제4조를 위반한 것으로 허용되지 아니한다. SCA에서는 공개가 가능한 '기타 정보'가 무엇인지에 대한 구체적인 정의규정을 두고 있지는 않지만, 판례는 "이용자의 이름, 주소, 시내 및 시외전화연결기록 또는 기타 이용자의 번호나 신분과 서비스이용요금지불 현황" 등을 여기에 포함시킨다.[6]

독일의 경우 인터넷서비스제공자는 전기통신사업법(TKG) 제100조에 따라 고객이 인터넷서비스에 접속한 때로부터 7일 동안 고객의 아이피주소를 저장할 수 있다고 판결하였다.[7] 이에 따라 독일의 형사소추기관은 위 7일의 저장기간 안에 인터넷서비스제공자가 보유하고 있는 개인정보에 대해 접근할 수 있다. 물론 이에 대한 법원의 재판절차를 거쳐야 하므로 7일 이내에 신속하게 법원에 정보청구권을 신청하여야만 가능하다. 예컨대 저작권법 제101조 제9항이 규정하고 있는 정보제공절차에서는 저작권이 침해되었다고 주장된 특정기간 동안 인터넷을 이용한 유저에 대한 권리자의 정보청구권을 인정하고 있는데, 권리자가 이 정보청구권을 활용할 수 있기 위해서는 7일 이내에 법원에 신청을 하지 않으면 안 된다. 또한 독일 연방대법원은 2012. 4. 19, 판결을 통하여 최초로 인터넷서비스제공자는 이용자의 정보를 권리자 또는 그 소송대리인에게 제공하여야 할 의무가 있다고 판결하였다.[8]

---

6) Patrick Collins, Inc. v. Does 1-38, 941 F. Supp. 2d 153 (D. Mass. 2013); United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999); United States v. Wheelock,. 772 F.3d 825, 829 (8th Cir. 2014).

7) BGH III ZR 391/13 vom 03. 07. 2014.

8) BGH I ZB 80/11.

다. 우리나라의 현행법 제도

온라인서비스제공자의 정보제공의무는 저작권법과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 규정되어 있다. 저작권법의 보호를 받는 권리가 침해된 경우 권리자는 저작권법 제103조의3에 따라 온라인서비스제공자에게 복제·전송자의 성명과 주소 등 민사상 소제기 또는 형사상 고소에 필요한 정보제공을 요청할 수 있다. 이는 물론 침해행위에 대한 사후구제 제도이다. 저작권법의 적용을 받지 아니하는 권리침해의 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 정보통신서비스제공자가 개인정보를 제3자에게 제공할 수 있는 경우를 규정하고 있다. 이 법에 따르면 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우이거나 또는 법률에 특별한 규정이 있는 경우 이외에는 이용자의 개인정보를 수집·이용하거나 또는 그 이용자의 동의가 없는 이상 이를 제3자에게 제공하지 못하며(같은 법 제24조의2 제1항), 이에 위반한 경우에는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처하도록 규정한다(같은 법 제71조 제3호).

4. 주요국가의 입법례

(1) 미국

1978년 국내에서의 첩보활동을 제한하기 목적으로 해외정보감시법(Foreign Intelligence Surveillance Act ; FISA)이 제정된 것과 동시에 FISA 법원이 설립되었고, 이 법원은 국가안보기관이 미국 내에서 하는 감청에 대한 사전승인권을 행사할 수 있게 되었다. 그 후 2001년 이른바 9.11.사태의 발발을 계기로 의회는 FISA에 대한 재검토 작업에 착수하며 안보와 프라이버시를 보다 심도 있게 균형을 맞추고자 노력하였다. 그 결과물이 2001년의 애국자법(Patriot Act)인데, 이 법에서도 여전히 감청은 FISA 법원이 관할하는 사법적 통제 하에 두는 것을 원칙으로 하였다. 다만, 이 애국자법에서 예외적으로 인정하는 대부분의 감시규정(surveillance provisions)을 한시규정으로 하였으나, 오늘날 가장 큰 쟁점사항이 된 조사규정인 '국가안전소환장'(National Security Letters)[9]은 애국

자법 제정 당시부터 한시규정화하지 않아 이 제도는 현재에 이르기까지 영구적이고 가장 강력한 조사수단으로 활용되고 있는 실정이다.

정보통신이용자의 통신자료의 제출의무에 대해서는 18 U.S. Code § 2703에서 규정하고 있다. 이 규정에 따르면 모든 국가기관은 전기통신사업자 또는 인터넷서비스제공자에게 90일 이내의 일정한 기간 동안 이용자의 통신자료정보를 저장할 것을 요구할 수 있으며, 그 기간을 90일 더 연장할 수도 있다. 이는 사업자의 유저개인정보 저장과 관련하여 유럽의 경우보다 비교적 폭넓게 허용되는 것인데, 그 배경으로는 사적 영역에 속하는 개인정보를 법률로 규정하는 것을 꺼리는 미국법의 특징이 지적된다.[10] 물론 이와 같이 저장된 정보에 접근하기 위해서는 법원의 허가가 필요하다. 그런데 법원의 사전승인 없이 소환이 가능한 이른바 국가안전소환장에 의하여 FBI 기타 연방정부첩보기관 등은 아무런 제한을 받지 않은 채 전기통신사업자, 인터넷서비스제공자 및 기타 기업들에게 인적 사항이 들어있는 (거래) 정보를 저장하고 특정한 사람에 대한 정보를 제공할 것을 요구할 수 있다.[11] 국가안전소환장은 일종의 행정적 소환으로, 연방수사국(FBI)이 사법적 심사를 받지 않고 재량으로 발령한다. FBI는 국가안전소환장에 의하여 조사대상자가 스파이라든가 테러리스트임을 증명하는 증거를 제시할 필요도 없이 그 사람의 통신기록(communication records), 은행영수증(banking receipts) 및 예금정보(credit information) 등을 수집할 수 있다. 수사기관은 위 소환장을 자유로이 임의의 사람을 선택하여 그에 관한 정보를 수집하는데 사용하고 있기 때문에, 죄가 없는 자에 대한 정보를 무턱대고 수집하여 이를 영구히 보관하는 일도 드물지 않게 발생한다.[12] 이러한 이유로 이 제도를 제한하여야 한다는 목소리가 높아지자,[13] 2009년 미국 연방의회는

9) 미국 연방정부는 저장정보법(The Stored Communications Act), 신용보고공정법(Fair Credit Reporting Act), 재정프라이버시접근법(Right to Financial Privacy Act)에 따라 국가안전에 중요한 정보를 탐지할 수 있는데, 이를 위해 연방정부가 발하는 소환장을 국가안전소환장이라 하는데, 애국자법에 의하여 그 적용범위가 크게 확대되어 시행되고 있다.

10) Max-Planck-Institut, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, S. 184.

11) Max-Planck-Institut, a.a.O.

12) Charles Doyle, "National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments", Congressional Research Service (September 8, 2009).

13) William Bendix/ Paul J. Quirk, "Institutional Failure in Surveillance Policymaking: Deliberating the Patriot Act", Issues in Governance Studies, 2013, 13-14.

국가안전소환장 제도를 제한하는 내용의 법안을 제출하는 등 법개정 노력을 계속하고 있으나, 9. 11. 사태의 충격은 이 제도를 계속 유지시키는 가장 든든한 버팀목으로 작용하고 있다.

(2) 독일

독일에서의 통신감청 및 통신사실확인자료는 독일 형사소송법과 「서신, 우편, 통신 비밀제한에 관한 법률」이 정하는 예외적인 경우에 한하여 인정되는데, 일정의 범죄에 대한 범죄혐의가 있고, 사실관계의 조사나 피의자의 소재수사가 다른 방법으로는 매우 곤란하거나 불가능한 경우로 제한하고 있다. 이와 같은 예외적인 경우가 아닌 한, 감청이나 통신자료의 제공의무는 형사소송법이 정하는 압수, 수색의 절차에 따라야 한다.[14] 독일의 전기통신사업법에는 사업자가 통신자료를 제공할 수 있는 근거규정이 있으나, 이는 의무조항이 아니므로 일체의 통신자료는 물론 감청은 수사기관이 압수와 수색이라는 전통적인 방법으로 입수하여야 한다.[15]

(3) 일본

일본의 경우에도 감청을 하거나 통신이력 및 통신자료를 제공받기 위해서는 형사소송법에 의한 수색 및 압수의 절차를 거쳐야 한다. 다만, 「범죄수사를 위한 통신방수에 관한 법률」은 수인이 공모하여 실행하는 조직적 살인, 약물 및 초기의 부정거래에 관한 범죄 등 중대범죄에 있어서 범인간에 상호연락 등에 사용된 전화, 기타 전기통신을 감청하지 않으면 사안의 진상을 해명할 수 없는 경우에 한하여 통신감청을 허용하는 예외를 인정하고 있다(같은 법 제1조). 다른 한편, 개인정보보호법의 예외를 인정하는 통신이력과 통신자료에 대한 제공의무와 관련하여서는 총무성의 가이드라인 즉, 「전기통신사업에서

14) 상세는, 박희영, "독일 형사소송법상 통신데이터 수집권과 한국 통신비밀보호법상 통신사실 확인자료 제공 요청권의 비교 및 시사점", 「경찰학연구」 제9권 제3호, 경찰대학, 2009. 참조.

15) 이성기, "통신사업자의 통신사실 확인자료 및 통신자료 제공의 요건과 절차에 관한 비교법적 연구 : 미국, 영국, 독일, 프랑스, 일본 제도 비교를 중심으로", 「법과 정책연구」 제14집 제1호, 2014, 53쪽.

의 개인정보보호에 관한 가이드라인」 제15조는, 전기통신사업자는 이용자의 동의가 있는 경우, 재판관이 발부한 영장에 의한 경우, 정당방위 또는 긴급피난에 해당하는 경우, 기타 위법성조각사유가 있는 경우를 제외하고는 통신이력(이용자가 전기통신을 이용한 일시, 당해 통신의 상대방, 기타 이용자 통시네 관한 정보로서 통신내용 이외의 것을 말한다)을 타인에게 제공해서는 안 된다고 규정하고 있으며(제1항), 제2항은 전기통신사업자는 법령에 근거가 있는 경우 등을 제외하고는 본인의 동의 없이 개인정보를 제3자에게 제공하여서는 안 된다고 규정하고 있다. 다만 이 경우 일본 형사소송법상 제197조 제2항의에 따른 사실조회에 전기통신사업자가 응하여야 하는가 문제와 관련하여, 실무에서 통신자료에 대한 조회에는 응하여야 하는 반면에 통신이력에 대한 조회에는 응할 필요가 없다고 한다.[16]

5. 기술유출에 대한 사전방지조치와 관련한 비교법적 시사점

현행법은 기술유출의 경우 정보제공의무를 규정하는 특별한 규정을 두고 있지 않다. 정보통신망법에 따르면 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우이거나 또는 법률에 특별한 규정이 있는 경우 외에는 이용자의 개인정보를 수집・이용하거나 또는 그 이용자의 동의가 없는 이상 이를 제3자에게 제공하지 못한다(정보통신망법 제24조의2 제1항). 그러나 세계적 추세는 적어도 범죄행위와 관련하여 개인정보를 수집할 수 있도록 하는 방향으로 발전하고 있다. 산업기술정보의 보안과 개인정보의 보호를 균형 있게 발전시키려는 각국의 노력이 계속되고 있으며, 오늘날 종래 안보적 스파이의 개념에는 경제스파이가 포함된다는 것은 널리 알려진 사실이다. 미국의 안전소환장 제도는 조사대상자가 경제스파이라는 근거를 제시하지 않고서도 그의 통신기록을 수집할 수 있도록 하고 있으며, 압수의 대상으로서의 '재산'에 정보를 포함시키고 있다. 최근 유럽평의회는 「사이버범죄방지협약」을 마련하여 개인에게 컴

16) 상세는, 이성기, "통신사업자의 통신사실 확인자료 및 통신자료 제공의 요건과 절차에 관한 비교법적 연구 : 미국, 영국, 독일, 프랑스, 일본 제도 비교를 중심으로", 「법과 정책연구」 제14집 제1호, 2014, 57쪽, 59쪽.

퓨터 자료를 제출하거나 컴퓨터 시스템의 기능이나 자료 보호를 위한 수단에 관한 정보를 제공할 것을 명령할 수 있는 권한을 법집행기관에게 부여하는 입법적 조치 등을 취할 것을 협약 당사국에게 요구하고 있다.[17] 인터넷서비스운영자가 국가기관 또는 피해자에게 산업기술을 유출하거나 유출할 우려가 있는 유저에 대한 정보를 제공할 의무를 지는가의 여부에 관하여는 외국의 법을 비교하여 보아도 이를 인정하는 방향으로 나가야 할 것이다. 다만, 법원의 정보제공명령절차를 거치도록 하는 것은 정보유출의 시급성에 비추어 그 실익이 크지 않을 것이다. 따라서 기술유출우려가 있는 경우 정보제공의무를 부여하는 내용을 법률로 정하는 것이 바람직할 것이다.

III. 산업기술보안 입법 방안

1. 제도 도입 형식에 대한 검토

(1) 별도의 단행법률 제정 방안

산업기술 유출방지와 보호에 관한 일체의 내용을 담은 단일한 단행법을 제정하는 방안은 옳은 정비방안은 아니라고 생각한다. 오히려 기존의 산업기술보호법을 내실화 있게 개정하여 이를 활성화시키는 것이 바람직하다. 따라서 대안은 결국, 기술유출방지와 관련한 일체의 사항을 통합적으로 현행 산업기술보호법에 도입하든가, 아니면 산업기술보호법에 규정되어 있지 아니한 사항을 산업기술보호법과 여타의 관련법에 부분적으로 도입하는 방안 중 하나를 선택하는 문제로 남는다.

(2) 기존의 산업기술보호법에의 도입 방안

2006년 제정시부터 적용 범위, 구체적인 규율 내용, 부정경쟁방지법과의 규제 중복성 등에 의문이 제기되어 왔던 현행 산업기술보호법을 차제에 기술보

17) Sec. 19 (1) Convention on Cybercrime.

호의 실효성이 담보된 단행법률로 재정비할 필요가 있는지 문제이다. 산업기술보호법을 부정경쟁방지법과 차별화하기 위해서는 독자적 규율체제를 갖추어야 할 것인데,[18] 이는 기술유출에 대한 사전적이고 구체적인 예방적 조치를 가능케 하는데서 찾아야 할 것이다. 산업기술보호법에 기술유출에 대한 구체적인 예방적 규정을 도입한다면 사후적 구제수단인 부정경쟁방지법과의 차별성을 명확히 할 수 있을 것이다.

2. 개개법률의 관련 규정을 산업기술보호법에 수용하는 방식에 대한 검토

(1) 정보수집단계

1) 개요

우선 개인정보와 관련하여서는 현행법을 개정할 필요는 없어 보인다. 기술유출(우려)자의 개인정보는 현행 기술유출방지법 제15조 제2항 및 개인정보보호법 제18조 제2항 제5호에 의하여 수집・활용이 가능하기 때문이다. 물론 이는 개인정보처리자가 공공기관인 경우에 한하여 적용된다. 다음으로, 기업정보 중 직원정보는 개인정보보호법에 따라 규율될 것이고, 이를 제외한 기술 자체 또는 매출데이터 등에 관한 정보는 개인정보보호법의 적용대상이 아니므로 산업기술보호법에 추가신설할 필요가 있다.

2) 개인정보의 수집

개인정보의 제3자 제공의무를 규정하는 제도 도입은 불필요하다. 산업기술보호법 제15조 제2항의 필요한 조치를 취하기 위해서는 개인정보가 필요하고, 개인정보보호법 제18조 제2항 제5호에 따라 개인정보처리자에게 이를 제공하도록 요구할 수 있기 때문이다. 여기의 개인정보에는 기업의 직원정보가 포함된

18) 이에 대한 상세는, 현대호, "최근 산업기술 보호법제의 동향과 과제", 「연구보고서」 현안분석 2012-01, 2012. 13쪽 이하 참조.

다고 보아야 하며, 이 경우 해당기업은 개인정보처리자로서의 지위를 가진다.

3) 기업정보의 수집

기업정보 중 기술 자체와 이를 활용하여 생산한 제품의 매출에 관한 정보를 제공받을 수 있게 함으로써 해당 산업기술의 산업상 중요성과 보호가치성 여부를 판단할 수 있게 하기 위하여, 다음과 같은 내용으로 산업기술보호법 제15조의 제3항을 신설할 것을 제안한다.

『산업자원통상부장관 및 정보수사기관의 장은 제1항의 대상기관의 장에게 기업의 제품에 대한 매출 데이터 등 기업이 보유한 산업기술관련 정보의 제공을 요구할 수 있다. 정보제공요구는 서면으로 하여야 하며, 당해 기업의 산업기술 보호와 관련된 것임을 소명하여야 한다.』

<현행법규정과 비교>

산업기술의 유출방지 및 보호에 관한 법률 제15조	개정시안
① 생략 ② 산업통상자원부장관 및 정보수사기관의 장은 제1항의 규정에 따른 요청을 받을 경우 또는 제14조에 따른 금지행위를 인지한 경우에는 그 필요한 조치를 취하여야 한다.	① 생략 ② 생략 **③ 산업자원통상부장관 및 정보수사기관의 장은 제1항의 대상기관의 장에게 기업의 제품에 대한 매출 데이터 등 기업이 보유한 산업기술관련 정보의 제공을 요구할 수 있다. 정보제공요구는 서면으로 하여야 하며, 당해 기업의 산업기술 보호와 관련된 것임을 소명하여야 한다.**

(2) 통신자료수집단계

1) 개정취지

현행 산업기술보호법 제15조 제2항의 조치에 전기통신사업법 제83조 제3항의 조치가 포함될 수 있는가의 해석 문제를 남기고 있으므로, 이를 명확히

하기 위하여 산업기술보호법 제15조 제2항의 조치에 전기통신사업법 제83조 제3항의 조치가 포함됨을 명정하며, '필요한 조치'에 전기통신사업법 제83조 제3항의 조치내용을 포함시킴으로써 정보제공의 법적 근거를 마련하는 방안을 제안한다. 현행 산업기술보호법의 선언적인 산업기술보안 제도를 구체화시킬 필요가 있고 또 이를 통해 부정경쟁방지법과의 차별성을 부각시키고 내실 있는 기술보호체제를 갖추도록 하여야 할 것이다.

2) 산업기술보호법 개정 내용

현행 산업기술보호법 제15조 제2항의 필요한 조치에 전기통신사업법 제83조 제3항의 조치를 포함시킨다.

3) 신구개정안 비교

산업기술의 유출방지 및 보호에 관한 법률 제15조 제2항	개정안
산업통상자원부장관 및 정보수사기관의 장은 제1항의 규정에 따른 요청을 받을 경우 또는 제14조에 따른 금지행위를 인지한 경우에는 그 필요한 조치를 취하여야 한다.	산업통상자원부장관 및 정보수사기관의 장은 제1항의 규정에 따른 요청을 받을 경우 또는 제14조에 따른 금지행위를 인지한 경우에는 그 필요한 조치**(전기통신사업법 제83조 제3항의 조치 포함)**를 취하여야 한다.

(3) 우편물 검열 또는 전기통신 감청 단계

1) 개정시안

가. 개정취지

산업기술보호법에 규정된 금지행위를 통신비밀보호법의 적용을 받는 범죄행위로 취급하여 통신제한조치의 대상에 추가하고자 한다. 다만 현행 통신비밀보호법상의 통신제한조치를 산업기술보호법에 포함시킬 수 있는지 문제이다. 그러한 내용을 담기 위해서는 먼저 통신비밀보호법 제3조의 예외사유에 산업기

술보호법의 규정을 추가한 후에, 구성요건을 구체화시켜야 할 것이다. 그런데 이 경우 구성요건을 구체화시킴에 있어서 나타날 수 있는 위헌의 문제를 피하기 위해서는 결국 통신비밀보호법에 규정된 요건에 따르지 않을 수 없을 것이다. 따라서 통신비밀보호법상의 관련 내용을 그대로 기술유출방지법에 수용하는 방식보다는, 산업기술보호법이 통신비밀보호법에 반영될 수 있는 방향으로 개정하는 방식이 보다 안전하고, 효율적이며, 경제적이라고 생각한다.

나. 규정내용 : 통신비밀보호법 제5조 제1항 제4호에 산업기술보호법을 추가한다.

다. 신구개정시안 비교

통신비밀보호법 제5조 제1항 제4호	개정시안
군사기밀보호법에 규정된 범죄	군사기밀보호법·**산업기술보호법에** 규정된 범죄·**금지행위**

2) 상위법 저촉 여부

산업기술보호법에 의하여 보호를 받는 기술의 범위가 대통령령 등 명령에 따라 지정되거나 인증되는 점에 비추어, 통신비밀의 원칙을 제한할 사유를 인정하는 것이 법적 불안정이나 예견가능성을 침해하여 죄형법정주의의 명확성 원칙에 위배되지 않는가 하는 문제제기와 위헌주장이 있을 수 있다. 그러나 위와 같은 내용의 법개정을 하더라도 상위법에 저촉하는 문제는 나타나지 않을 것으로 판단된다. 첫째, 기술의 범위를 법률 또는 그 위임에 의하여 명확히 정하고 있으므로 보호대상 명확성의 원칙에 반하지 아니하며, 둘째, 산업기술보호법 제14조가 금지행위를 열거하고 있을 뿐 아니라 이를 위반한 경우 벌칙규정을 두고 있으므로(같은 법 제36조) 정보의 수집 및 활용이 요구되는 범죄에 준하여 평가할 수 있으며, 셋째, 법정정책적인 면에서 볼 때 다양성과 변동가능성을 그 특징적 요소로 하는 산업기술을 행정규칙적인 지정 또는 고시에 위임하고 이를 침해하는 행위에 형사벌을 과하더라도 죄형법정주의에 반하지 않는다고 본다.

IV. 결론

정보통신사회의 도래는 서로 엇갈리는 두 가지의 법적 문제를 발생시켰다. 한편으로는, 현대 정보기술사회에서 개인정보는 도처에서 그 침해의 위험에 노출되고, 그 결과 개인정보와 관련하여 전통적으로 정보보호의 문제가 주요 과제로 등장하였다. 다른 한편으로는, 개인정보의 보호만을 강조하여 사권 내지 공권을 침해한 자의 인적 사항에 관한 적절한 정보를 얻을 수 없다면, 법이 보호하는 개인 및 사회의 권리는 현실 사회에서 실현되지 못하고 법문의 틀 안에 갇혀 죽은 권리로 전락하고 만다. 산업기술이 사권을 넘어 국가안전보장은 물론 국민경제적 관점에 볼 때 그 보호의 필요성이 점증하고 있는 상황에서, 개인정보의 보호 범위의 한계를 설정하여 개인정보 제공법리를 발전시키는 일에 못지않게, 시급히 정보수집 제도 내지는 정보제공의무 제도를 도입하여야 할 필요성이 크다. 이를 바탕으로 위에서 제안한 산업기술보호법제 정비방안을 정리하면 다음과 같다.

먼저, 법개정 형식과 관련하여, 별도의 단행법률이 아닌 기존의 법률에 새로운 규정을 신설하거나 추가하는 방안이 타당하다. 다음으로, 법개정의 주된 내용은 다음 사항을 포함하여야 한다.

첫째, 개인정보의 수집면에서, 산업기술유출자 및 유출우려자에 대한 개인정보의 수집은 현행법에서도 가능하지만, 수사 이전의 단계에서는 개인정보를 수집할 수 없음은 개인정보보호법에 비추어 자명하다. 기업정보를 요구하는 경우에도 개인정보보호법의 제한에 따라야 한다.

둘째, 기업정보의 수집면에서, 기업정보 중 직원정보에 대해서는 개인정보보호법이 정하는 바에 따라 정보수집이 가능하다. 기업정보 중 직원정보가 아닌 기업정보, 특히 기술 그 자체나 매출데이터 등에 대해서는 현행법상 유출방지 목적의 정보수집을 위한 법률적 근거가 없으므로, 산업기술보호법에 기업정보를 수집하고 활용할 수 있는 근거 규정을 신설하여야 할 것이다.

셋째, 통신자료의 수집과 관련하여, 산업기술보호법 제15조 제2항의 필요한 조치에 전기통신사업법 제83조의 제3항에 따른 조치인 자료의 열람이나 제출이 포함된다고 해석된다. 다만, 그 법적 근거를 명확히 하기 위하여 위 '필요한

조치'에 통신자료제공에 관한 내용을 포함시키는 방향으로 관련 조항을 개정하여야 할 것이다.

넷째. 우편물의 검열 또는 전기통신의 감청에 대한 위헌성 문제와 관련하여, 먼저 헌법상 기본권의 제약사유인 공공복리를 통신비밀의 자유에 대한 제한사유로 삼을 수 있을 것인지 문제되나, 이를 허용할 수 있다고 본다. 산업기술이 오늘날 사회에서 점하고 있는 국민경제적 중요성에 비추어 산업기술의 보호는 공공복리의 실현에 필수불가결한 요소라고 볼 수 있으며, 공공복리를 위한 제한은 여타의 많은 기본권과 달리 국가에 대한 개인의 대항적 자유의 범주에 해당하지 않아 정치적인 악용의 위험이 크게 떨어지기 때문이다. 다음으로, 그 규정 형식과 관련하여 산업기술보호라는 공공복리를 이유로 통신비밀의 자유를 제한할 수 있다고 보는 한, 그 규정형식은 별도의 단행법에서 규율할 수도 있고, 아니면 현행 통신비밀보호법이나 산업기술보호법에 추가하여 신설하는 방식도 가능할 것이다. 현행 산업기술보호법을 이용하지 않고 또 다른 법률을 제정하는 것은 규정의 중복성이나 경제적 관점에서 바람직하지 않다. 따라서 별개의 단행법률의 제정 대신에 현행법에 관련 제도를 신설하는 방안이 타당하다. 현행법에 도입하는 방안 중 통신비밀보호법에 도입할 경우에는 공공복리 대신에 범죄수사를 위한 통신제한조치로 규율하는 것이 합리적이며, 산업기술보호법에 도입할 경우에는 공공복리를 이유로 통신제한조치 및 그 허용요건 등에 대한 규정을 신설하여야 할 것이다. 산업기술의 중요성이 점증해가고 현행 산업기술보호법의 내실화를 중요시한다면, 산업기술보호법에 "공공복리를 위한 통신제한조치의 허가요건"에 관한 규정을 신설하는 동시에 통신비밀보호법 제3조에 열거된 "이 법과 형사소송법 또는 군사법원법"에 "산업기술유출방지 및 보호에 관한 법률"을 추가하여야 할 것이다. 다른 한편, 헌법상의 공공복리가 산업기술의 보호에 적용될 수 있는가에 대한 논쟁 및 위헌의 위험을 피하는 것을 염두에 둔다면, 위에서 제안한 바와 같이 통신비밀보호법상의 법죄수사에서의 범죄에 "산업기술유출방지 및 보호에 관한 법률에 규정된 금지행위"를 추가하면 될 것이다.

참 고 문 헌

(국내 문헌)

박희영, “독일 형사소송법상 통신데이터 수집권과 한국 통신비밀보호법상 통신사실확인자료 제공 요청권의 비교 및 시사점”, 경찰학연구 제9권 제3호, 경찰대학, 2009.

손승우, “2011년 개정 산업기술의 유출방지 및 보호에 관한 법률안의 분석”, 「경원법학」 4권, 경원대학교 법학연구소, 2011.

이성기, “통신사업자의 통신사실 확인자료 및 통신자료 제공의 요건과 절차에 관한 비교법적 연구 : 미국, 영국, 독일, 프랑스, 일본 제도 비교를 중심으로”,「법과 정책연구」 제14집 제1호, 한국법정책학회, 2014.

조광훈, “첨단기술 유출범죄의 발생원인과 대응방안”,「지식재산21」, 2010년 4월.

현대호, “최근 산업기술 보호법제의 동향과 과제”,「연구보고서」 현안분석 2012-01, 한국법제연구원, 2012.

황인표, “IT분야기술유출방지에 관한 법제도적 연구”,「연세대학교 일반대학원 석사학위논문」, 2004.

황철, “핵심기술유출의 현황 및 대응”, 「지식재산권연구센터」 포럼 자료, 2005.

(외국 문헌)

Charles Doyle, "National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments", Congressional Research Service (September 8, 2009).

Max-Planck-Institut, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, 2011.

William Bendix/ Paul J. Quirk, "Institutional Failure in Surveillance Policymaking: Deliberating the Patriot Act", Issues in Governance Studies, No. 40, 2013

<국문초록>

퇴직직원에 의한 산업기술 유출 비율이 65% 이상을 점하고 있다는 조사결과는 산업기술보호법제의 충실화를 위해서는 개인정보보호법과의 균형적인 조화를 통한 정비 방안을 요구한다. 이를 조화시킬 수 있는 방안의 하나로 먼저, 현행법의 해석을 통하여 개인정보에 대한 수집이 가능한지 검토하였다. 그러나 각국의 입법례를 비교한 결과, 산업기술유출 우려를 이유로 형사소송절차에 의하지 않고 감청을 하거나 통신자료를 요구할 수 있게 하는 방향은 타당하지 않다고 본다. 다만 미국의 경우 국가안전소환장 제도를 운영하고 있으나, 이는 2011년의 9.11.사태에 따른 부득이한 조치로 이제 폐지하여야 한다거나 한시적으로 운영하여야 한다는 견해 등이 우세해지고 있는 점을 감안하면 해석론적 한계는 명백하다.

다음으로, 첨단기술 내지는 국가핵심기술을 중대범죄수사에 준하여 개인정보 및 기업정보를 수집할 수 있는 근거법률로 산업기술보안입법을 위한 법정비 방안을 제안하였다.

첫째, 기술을 보유하고 있는 기업에 대한 정보가 있어야 국가적으로 보호가치 있는 기술인가의 여부 등을 판단할 수 있도록 기업정보를 수집할 수 있는 법적 근거를 제안하였다. 현행「산업기술의 유출 방지 및 보호에 관한 법률」제15조에 제3항을 신설하여 기업이 보유하고 있는 기술의 내용과 이를 이용한 결과물인 제품의 매출에 관한 정보를 제공받을 수 있는 법적 근거를 만련하고자 하였다.

둘째, 현행「산업기술의 유출 방지 및 보호에 관한 법률」제15조 제2항에 규정된「필요한 조치」에 통신자료에 관한 전기통신사업법 제83조 제3항의 내용을 포함시킴으로써 정보수사기관의 장이 통신자료제공을 요청하고 전기통신사업자가 이를 수용할 수 있는 법적 근거를 마련하고자 하였다.

셋째, 국가핵심기술의 유출 등 침해행위에 대해서도 통신제한조치를 취할 수 있는 법적 근거를 마련하기 위하여 통신비밀보호법 제5조 제1항 제4호의 “군사기밀보호법에 규정된 범죄”에 “산업기술보호법에 규정된 국가핵심기술에 대한 범죄”를 추가하는 방안을 제안하였다.

주제어 : 산업기술보호, 통신자료, 개인정보보호, 기업정보, 해외정보감시법, 애국자법, 국가안전소환장

Protection of Industrial Technology by way of Access to Communication Records

Kim, Yong-Jin*

The World face difficult choices between striving for higher protection level for industrial technology and protecting civil liberties. Without judicial approval, the criminal investigators could not access to wiretaps, communication records, and so on. In our judicial viewpoint american style of National Security Letters is not available to us. Whether to provide investigation authorities with communication data without court's order lies therefore in the discretion of the person or the company. This result is, however, not enough to protect industrial technology, of which competitiveness enhances dramatically national resources in each country.

Based on this idea the paper recommends as follows. First of all the lawful position of high technology should be equivalent to that of national security. In this regard the paper suggests some legislative recommendations. They would allow investigators to seize a person's communications record and credit information, without having to obtain judicial approval. But as relatively lax rules for seizing private records and conducting electronic surveillance could lead to fishing expedition and violations of privacy rights, the concrete requirements of such control should be strictly examined and fulfilled. Such suggestions are ambitious institutional reforms. But as divulgence of industrial technology increasingly devastating and surveillance technologies become ever more sophisticated, to maintain a healthy balance between security and privacy will depend on overcomming the institutional weaknesses in law mechanism.

Key Words : Protection of Industrial Technology, communication records, privacy rights, business records, Foreign Intelligence Surveillance Act, Patriot Act, National Security Letters

* Professor, Chungnam National University Law School