财经法学 No. 3，2021
pp. 144 - 160

商业间谍刑事规制的美国经验与我国的借鉴应对

曹　波　杨　婷*

内容提要：《经济间谍法》系美国首部专门为侵犯商业秘密提供刑事规制路径的联邦法律，一改长期以来由各州普通法保护商业秘密的司法传统，奠定了美国商业秘密犯罪规范体系的基础，引领着商业秘密法律保护的国际立法趋势。美国对商业间谍进行刑事规制的罪名主要有商业间谍罪与普通商业秘密窃取罪，前者配置更高的法定刑以威慑并严惩有外国政府因素介入的商业秘密窃取行为，兼顾商业秘密保护与国家安全保障。当前该法日渐异化为美国遏制中国的法律工具，特别是美国法院确立的以创造性证据实施诱捕以证立犯罪的判例规则，给美国商业竞争对手恶意打压甚至扼杀中国企业大开方便之门；其经济间谍条款未排除其他商业秘密补救措施的规定，意味着被卷入商业秘密刑事案件的当事人将面临联邦或州的双重甚至多重控诉。开展涉美业务的中国企业、个人抑或中国政府仅依赖法庭上的抗辩并无太大胜算，最佳措施应是事前“防御”，如出入境美国时携带“清洁”电子产品，相关企业在人才流动频繁的经济市场中应特别重视合规管理等。

关键词：商业间谍法　商业秘密　刑事规制　事前防御　合规管理

一、引　言

中国共产党第十八次全国代表大会以来，我国不断深入推进以总体国家安全观为导向的国家安全工作并取得瞩目成绩。作为国家安全工作的重要保护性机制，刑事法律往往根据经济社会发展的现实需要调整或者增设相关罪刑条款以维护与保障国家安全。2021 年 3 月 1 日正式施行的

* 曹波，贵州大学法学院副教授，中国社会科学院法学所暨贵州省社会科学院联合培养博士后；杨婷，贵州大学法学院硕士研究生。

本文为中国博士后科学基金第 67 批面上资助项目“刑事治理现代化内在逻辑与推进路径研究”（2020M673298）的阶段性成果。

《刑法修正案（十一）》以总体国家安全观为旨归，对现行《刑法》进行多达47处的实质性修正。《刑法修正案（十一）》第22条修改侵犯商业秘密入罪门槛，并进一步升格侵犯商业秘密罪法定刑，强化对既有侵犯商业秘密行为的刑法惩治力度；第23条新增为境外窃取、刺探、收买、非法提供商业秘密罪作为独立罪名，将为境外机构、组织或人员窃取、刺探、收买以及非法提供商业秘密的商业间谍行为直接犯罪化并配置明显高于普通侵犯商业秘密罪的法定刑，以期对商业间谍行为给予专门且严厉的刑事惩治。

在竞争激烈的商业“战场”中，商业秘密早已突破私权属性，既成为企业经济交往制胜的核心关键，也成为推动国家经济发展的重要动能。然而境外人士侵犯我国商业秘密的事件频现报端，严重危及我国企业的生存与发展，诱发商业间谍犯罪化之客观需要。例如2009年澳大利亚力拓公司驻上海办事处首席代表胡士泰等人刺探、窃取我国钢铁企业商业秘密所引发的“力拓间谍门案”，给有关钢铁企业和我国国家经济安全造成特别严重后果，胡士泰等人因涉嫌侵犯商业秘密罪被提起公诉。〔1〕诚然，罪名的选择反映出我国司法机关在办案过程中避免将案件政治化的审慎态度，但也深刻凸显我国现行刑事法律体系对商业间谍行为规制乏力：以“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”追诉，将面临商业秘密并非本罪犯罪对象涵摄范围而抵触罪刑法定原则的批驳；适用“侵犯商业秘密罪”等其他罪名追究刑责，则出现所判处之刑罚与行为的社会危害性及行为人的主观犯意程度严重不匹配的罪刑失衡现象。商业间谍刑事规制罪名选择上的无所适从，给针对我国总体经济安全、具有间谍性质的商业间谍活动带来可乘之机。

随着世界经济重心东移，中国等新兴经济体和发展中大国群体性崛起并逐渐赢得国际社会的认可，美国国内部分右翼政治势力与极端学者却普遍敌视中国，将中国视为潜在威胁和战略竞争对手，运用复杂的竞争手段企图遏制中国的崛起。〔2〕新世纪初，美国为保护本国产业，悍然发动“337调查”，将矛头直指中国，对我国电子、通信、机械等产业展开猛烈的“专利围剿”与“商标围攻”，我国因此成为“337调查”最大受害国。〔3〕近年来，我国更是被美国冠以商业秘密“头号威胁”之污名。〔4〕2018年11月，美国司法部启动“中国行动计划”（China Initiative）优先对涉华商业间谍案件提起诉讼，进一步加剧两国经贸与外交关系的紧张局势。2020年2月6日，美国联邦调查局在《有效应对中国经济间谍的威胁》中再次指出，中国的商业间谍是美国国家信息、知识产权与经济活力最大的威胁。〔5〕中美两国在知识产权领域展开的“攻防战”以及美国政府长期倡导的敌视思想反映出美国对涉华商业间谍活动的政策导向，特别是专门规制商业间谍、极富特色的联邦刑事法律《经济间谍法》（Economic Espionage Act，EEA）（《美国法典》第18编第90章第1831—1839条）的司法实务明显呈现出直接针对中国的政治化倾向。

---

〔1〕 参见沈爱民、张智聪：《简评美国惩治经济间谍犯罪的司法实践》，载《中国检察官》2011年第6期。

〔2〕 参见邵峰：《美国敌视中国的国际背景和逻辑根源》，载《人民论坛》2020年第16期。

〔3〕 参见田力普主编：《中国企业海外知识产权纠纷典型案例启示录》，知识产权出版社2010年版，第113－114页。

〔4〕 See Michael L. Rustad, The Negligent Enablement of Trade Secret Misappropriation, 22 *Santa Clara Computer & High Tech. L. J.*, 455, 463 (2006).

〔5〕 See Department of Justice China Initiative Conference, Center for Strategic and International Studies Washington, D.C., Responding Effectively to the Chinese Economic Espionage Threat (Feb. 6, 2020), available at https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat, last visited on Apr. 7, 2021.

二、美国商业间谍法律规制的基本概况

冷战后，情报与反情报工作的重心逐渐从军事政治领域向科技经济领域迁移。频繁发生的商业秘密窃取事件严重危及美国企业生存发展利益、社会公共利益以及国家安全。〔6〕美国 1996 年《经济间谍法》正是在企业信息安全面临越来越大的威胁以及国际国内经济间谍活动日益增多的背景下产生的。〔7〕

（一）美国反商业间谍活动之背景简析

两次世界大战所带来的创痛以及近半个世纪相对和平的冷战状态促使各国纷纷转变对外发展思维，开始寻求多角度国家安全维护策略。各国之间商业经济交往日益频繁的同时，经济竞争也日趋激烈。越来越多的国家与企业意识到掌握竞争对手各方面信息对自身发展和获取更多商业机遇极为重要，商业间谍业应运而生，〔8〕成为“当今世界的又一新热点”〔9〕。

各国决策领导层大力寻求开展商业间谍业务的正当化依据，由此催生出一系列商业间谍机构。诚如美国官员罗伯特·科勒所言：“既然可以为军事安全保障进行间谍活动，自然可以为维护经济安全而开展间谍活动。”〔10〕商业间谍主要由两部分力量组成：一是非官方的企业层面，或通过雇佣专业的竞争情报机构，或通过设立自己的情报部门从事相关工作；二是政府层面，如战后为谋求特殊经济优势，美国中央情报局承担起商业间谍的新职责，欧盟则在秘密筹划设立网络委员会，并借此组建一个国际性的电话拦截网络。〔11〕与此同时，以美国为中心的全球窃听卫星网络——梯队系统（Echelon），能够对接入或发出美国的电话、传真与电子邮件进行拦截窃听与分析，因其极易被参与国用于实施犯罪而招致诸多批评。〔12〕例如，有论者指责梯队系统已沦为借反恐之名，行监视其他国家经济活动以及各大经济体动向之实的“窃贼”。〔13〕沙特阿拉伯 60 亿美元客机案即被认为系参与国利用梯队系统从事国家性质的商业间谍活动之典型事例。〔14〕

随着经济发展日益全球化，企业在生产经营活动中所掌握的信息和技术，成为其在竞争中生存和发展的关键核心，经济情报的窃密与反窃密斗争日趋激烈。〔15〕因之，如何在经济“战场”

---

〔6〕 See Thierry Oliver Desmet, The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously? 22 *Hous. J. Int'l L.*, 93, 97 (1999).

〔7〕 See United States v. Hsu, 155 F. 3d 189, 194 (3d Cir. 1998).

〔8〕 参见〔美〕亚当·L. 佩恩伯格、马克·巴里：《经济间谍探秘》，史明明等译，机械工业出版社 2002 年版，第12 页。

〔9〕 曹中轩：《经济情报战：当今世界新热点》，载《现代情报》1994 年第 2 期。

〔10〕 David E. Sanger, Tim Weiner, C. I. A.'s New Role: Spying on Allies and Their Economics, 145 *New York* Times, 12 (1995).

〔11〕 参见〔英〕约翰·帕克：《全民监控：大数据时代的安全与隐私困境》，关立深译，金城出版社 2015 年版，第 146 页。

〔12〕 参见〔美〕吉姆·马尔斯：《美国怎么了》，姚艳萍译，浙江人民出版社 2013 年版，第 232－233 页。

〔13〕 参见亚诺：《NSA 美国国家安全局全传》，凤凰出版社 2010 年版，第 165 页。

〔14〕 沙特阿拉伯 60 亿美元客机案的缘起：1994 年，法国与沙特阿拉伯经过长期的谈判，终于就法国向沙特阿拉伯出售军火及欧洲空中客车飞机达成初步协议。与此同时，美国国家安全局利用梯队系统掌握了交易的所有内情，其中包括空客公司向沙特官员行贿的事实。借助这一情报，美国拿到了与沙特阿拉伯的 60 亿美元合同。（参见隋岩：《美国国家安全局秘史》，中国法制出版社 2014 年版，第 231 页。）

〔15〕 参见王知津：《竞争情报》，科学技术文献出版社 2005 年版，第 397 页。

上维持强势地位成为美国当务之急。美国政府断然不会坐以待毙，被动地等待他国的竞争情报机构将触角伸向本国企业的商业秘密，而是通过包括开展官方和非官方层面的经济竞争情报业务在内的各种途径主动出击，以获取竞争对手的商业秘密。此外，美国政府还重视从多方面加强防范措施以筑牢本国商业秘密保护体系，极力将商业秘密的保护纳入国家法治轨道，构筑较为完善的法律保护机制。

（二）美国反商业间谍活动之动因透析

美国商业间谍的犯罪化系多重因素共同作用的结果。出于保护本国企业商业秘密与高新技术资源的现实考量以及科技发展在某种程度上的“助纣为虐”，美国向来强调从法律层面强力规制商业间谍行为。然而，美国传统联邦与州法难以对商业秘密侵害行为实现完整且准确的评价，制定专门规制商业秘密侵犯行为的联邦刑事法律，形塑国家相关犯罪行为规范体系确有其必要。

1. 经济因素

20 世纪中后期，促进经济社会发展的资产内部构成经历了深刻变革，无形资产尤其是知识产权对经济增长的贡献率与日俱增。虽然 1996 年之前，美国联邦法律体系中就已有对专利权、著作权等知识产权的专门保护，但对于同样具有经济价值的商业秘密却缺乏相同等级之规范。〔16〕美国工业安全协会的调查显示，1996 年大约 1300 家美国公司发生了 1100 多起非法工业秘密刺探事件，被窃取信息的潜在商业价值可能高达 3000 亿美元。〔17〕时任联邦调查局局长路易斯·弗里赫称，全球至少有 50 个国家和地区已经将商业间谍活动之触角伸向美国的经济机密，外国政府和公司对美国的商业间谍案件正成倍增加且手段愈发高明，美国企业每年因此遭受高达 1000 亿美元的经济损失。〔18〕维护商业资讯一定程度上的私有化与秘密状态，维持商业秘密所有人及利益相关者在国内国际自由贸易市场上的竞争优势，预防与制裁相关侵害行为诚为时势所趋。〔19〕

2. 科技因素

科技领域的重大突破推动社会生产关系变革并带领人类历史实现质的飞跃，但科技也可能因人们主观要素的渗入而具有潜在的破坏性，理应辩证地看待科技发展因素在商业秘密保护立法中的作用。与此同时，发达的科技资源客观上也促使美国成为外国商业间谍战的主要目标，以法律抗制商业间谍活动契合国家维护这一优势资源的现实之需。

详言之，世界经济已演变为以高新科技为代表的经济形态。能够为企业带来更大经济价值的资产通常已不再是动产不动产之属，而是企业的核心机密。科技发展极大地便利了企业商业秘密的存储、传输与传播，用以窃取商业秘密的高科技设备也是日新月异，客观上加剧了企业商业秘密资产的流失风险。例如，隐匿于办公场所的迷你触发式摄像机和数码录像机，可以捕捉长达 33 个小时的活动。一支外观与其他书写笔无异的圆珠笔，其内部竟然隐藏足有 2G 存

〔16〕 参见林志洁：《美国联邦经济间谍法之回顾与展望——兼论台湾营业秘密法之刑罚化》，载《台湾科技法学评论》2016 年第 1 期。

〔17〕 参见胡树华等编著：《国家创新战略》，经济管理出版社 2003 年版，第 27 页。

〔18〕 参见李航主编：《竞争优势》，中国对外经济贸易出版社 1998 年版，第 159 页。

〔19〕 参见曾胜珍：《美国经济间谍法初探》，载《台湾中正大学法学集刊》2005 年第 19 期。

储容量的语音激活录音设备。〔20〕当然，先进科学技术本身也是商业秘密的重要内容，因而对美国先进科技的觊觎成为许多国家不断制造商业间谍事件的主要动因。为此，美国政府采取多重商业秘密防范与保护措施，并于 1996 年通过旨在将商业秘密法律保护纳入联邦法律框架的《经济间谍法》。

3. 打击犯罪的现实需要

《经济间谍法》正式颁行之前，美国国内商业秘密窃取行为尚无联邦刑事规范予以规制，遑论外国商业间谍。彼时美国的商业秘密主要依据各州普通法进行保护。虽然理论与实践上也存在联邦刑事法律规制路径，但综而观之，能够涵盖商业秘密侵害行为的联邦法律因其犯罪构成无法涵盖所有行为对象或行为样态而备受司法实践“冷落”。例如，1934 年《州际失窃财产转移法》（Interstate Transportation of Stolen Property Act of 1934）系主要适用于商业秘密泄露盗窃等行为的联邦刑事规范，但依据该法对商业秘密侵害行为进行刑事追诉却面临商业秘密能否归入“货物、物品或商品”的司法困惑。〔21〕该法所保护的对象主要为有体物的“财产”，无体财产权并不在保护范围之内。〔22〕又如，《美国法典》第 2511 条禁止窃听有线、电子或口头通讯以及公开窃听之信息，旨在专门规制、精准打击与有效遏阻滥用监听手段进行的非法窃听行为，〔23〕对于窃听之外的其他侵犯商业秘密的行为样态则缺乏刑事规制。此外，《美国法典》第 1343 条“电报、无线电或电视诈骗”〔24〕虽弥补《州际失窃财产转移法》仅适用于有体物的局限性，但有学者指出该规范在商业间谍规制司法实务中的应用受到以下限制：以电报、无线电或电视诈骗追诉商业间谍实施者的刑责要求行为人主观上“具有诈骗意图”，客观上“利用电报、无线电或电视”。〔25〕我国学者认为，就商业秘密的侵害行为而言，有时简单的信息复制并不必然导致资讯本身永久性的丧失，依据该法追究侵犯商业秘密行为的刑事责任并不妥当。〔26〕

鉴于《州际失窃财产转移法》等联邦刑事规范存在不同形式的局限性，美国启动“统一商业秘密法律保护”的有益尝试。1979 年的《统一商业秘密法》（Uniform Trade Secret Act，UTSA）旨在作为示范法以供各州政府引用、参考。虽然 UTSA 在商业秘密定义、侵害行为样态与民事救济等方面的规定为《经济间谍法》的规范设置奠定了基础，但各州在制定各自州法时大都对其进行了不同程度的修改，〔27〕以致各州的商业秘密保护法仍欠缺统一性，国家统一商业秘密法律保护之初衷未能实现，商业秘密诉讼当事人仍面临各州相互冲突之法律标准与不同诉讼程

---

〔20〕 See Acohido Byron，Tech Gadgets Help Corporate Spying Surge in Tough Times，USA TODAY（Jul. 28，2009），available at https://usatoday30. usatoday. com/tech/news/computersecurity/2009 - 07 - 28-corporate-espionage-recession-tech _ N. htm.，last visited on Apr. 7，2021.

〔21〕 参见储槐植：《美国刑法》，北京大学出版社 1996 年版，第 296 页。

〔22〕 参见曾胜珍：《美国有关经济间谍相关立法与沿革之介绍（上）》，载《台湾法令月刊》2005 年第 12 期。

〔23〕 See 18 U. S. Code § 2511.

〔24〕 See 18 U. S. Code § 1341& § 1343.

〔25〕 See Gerald J. Mossinghoff et. al.，The Economic Espionage Act：A New Federal Regime of Trade Secret Protection，79 *J. Pat. & Trademark Off. Soc'y*，191，194（1997）.

〔26〕 参见徐洁：《论美国〈反经济间谍法〉对商业秘密的保护》，载顾肖荣主编：《经济刑法 10》，上海社会科学院出版社 2010 年版，第 436 页。

〔27〕 如加利福尼亚州立法机构进一步扩大商业秘密范围，认为凡表现出一定经济价值的，即使是宗教文稿也属于商业秘密。（参见经贸委赴美专题考察组：《美国各州采用统一商业秘密法的情况》，载《经济研究参考》1996 年第 85 期。）

序规定之麻烦。〔28〕因此，美国商业秘密保护的法律依据仍主要是各州的普通法。不过，各州普通法规范体系不一，客观上造成商业秘密保护司法实践混乱不堪，使启动州法对侵犯商业秘密的行为进行刑事追诉缺乏强有力的司法资源保障。跨州商业秘密侵害行为的受害人维护自身利益存在极大困难，受害人需在多州分别提起诉讼并可能面临不同的审判结果；〔29〕对于跨国侵害行为，各州更是陷入无司法管辖权的困境。此外，适用各州法律规制商业间谍行为意味着无法借助中央政府的行政权力、力量与资源进行处置。按照彼时美国的司法制度，美国联邦与州法院两大审判系统对于各自管辖的社会事务分别根据联邦法律以及本州法律进行管理，且借助的司法资源力量亦有不同，前者主要借助中央政府行政管理机构及其所属部门的力量，后者则只能诉诸本州政府行政管理机构及其下属部门。〔30〕相较而言，为管理联邦犯罪所配置的司法权力和司法资源及其先进的侦查手段和强大的国家机器都是一般普通刑事侦查难以企及的，因此加强侵犯商业秘密的联邦立法，有助于整合执法司法力量和资源，化解各州及州与联邦在规制商业间谍违法犯罪上的冲突和紧张，提升惩治商业间谍犯罪的效率和效能。

（三）美国反商业间谍活动之司法动态

《经济间谍法》规定对存在外国政府扶持教唆或行为人意图裨益外国政府的商业秘密窃取行为，以规范第1条（《美国法典》第1831条）“商业间谍罪”进行惩罚。较之规范第2条（《美国法典》第1832条）“商业秘密窃取罪”，前者将使犯罪人被科处更高的自由刑和罚金刑，期望通过更为严厉的刑事政策与刑事制裁强化美国的商业秘密保护。然而，与立法者大干一番的雄心壮志形成对照的是，《经济间谍法》施行初期的司法实践显得更为温和，甚至可以说没能达到社会与国家的预期。2011年到2012年，美国因商业间谍损失超过130亿美元。尽管美国司法部联合联邦调查局对涉嫌违反商业间谍罪之行为启动优先调查，但自1996年至2012年，美国法院仅审理了九起此类案件。〔31〕其中五宗案件的被告人承认被控犯罪；一宗案件被告人在被捕之前逃往日本，但因日本拒绝引渡而尚未结案；只有其余United States v. Chung、United States v. Lee、United States v. Jin三宗案件进入法院审判程序。〔32〕

商业间谍案件审理过程中的常见抗辩与法官对其所持态度往往反映出国家在相关问题上的一贯立场与刑事政策导向。笔者在Westlaw International法律数据库进行检索，统计到自该法施行之日至2021年4月7日，美国联邦法院受理的商业间谍刑事案件约计378例。现有案件文本显示，在涉及商业秘密犯罪案件的司法审理实务中，目前普遍的抗辩事由包括以下几点：

（1）“争议信息不属于商业秘密”的抗辩。后文将述，《经济间谍法》明确商业秘密的构成要件包括秘密性、独立经济价值性以及所有人已采取合理保密措施，因此在具体案件中，被告人往往以商业秘密构成要件作为突破口进行抗辩。如否认“商业秘密所有人采取合理保密措施”，典

〔28〕 参见王伟霖：《2016年美国联邦保护营业秘密法（DTSA）于台湾营业秘密法制之借镜》，载《台湾万国法律》2016年第209期。

〔29〕 参见郑淑凤：《美国商业秘密保护最新立法阐释及其对中国的启示》，载《电子知识产权》2016年第10期。

〔30〕 参见侯仰坤：《美国〈1996经济间谍法〉及配套法律中英文解析》，知识产权出版社2019年版，第15页。

〔31〕 See Robin L. Kuntz, How Not to Catch A Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets, 28 *Berkeley Tech. L. J.*, 901, 901 (2013).

〔32〕 参见前引〔31〕，Robin L. Kuntz文，第907页。

型案件如 U. S. v. Hanjuan Jin 案以及 U. S. v. Robert O'Rourke 案。〔33〕美国司法实务界坚持，公诉机关无需证明商业秘密所有人穷尽所有可能想到的保密措施，仅需证明所有人采取的保密措施“合理”即可。U. S. v. Hanjuan Jin 案查明的事实显示，案涉商业秘密所有人摩托罗拉公司采取了包括物理安保措施（如安保摄像头和警报器）、网络与计算机安保措施（如访问密码与防火墙、限制网络访问等设置）、与员工签署保密协议、组织员工参加保密培训等在内的商业秘密安全保障措施。审理法院明确提出：“纵使摩托罗拉公司未能穷尽所有预防措施，但这并不意味着其所采取的措施不满足‘合理’的要求。”〔34〕而正如 Rockwell Graphic Systems，Incorporated v. DEV Industries，Incorporated 案所揭示的，对商业秘密定义中“合理性”要素的判断应根据具体案件中商业秘密所有人所采取措施的成本与收益具体分析。一般而言，所有人为防止商业秘密泄露所投入的成本越高，就越能表明该商业秘密具有真实价值并值得法律保护，也就越能证明所有人因商业秘密侵害行为所受损害的严重程度。〔35〕

U. S. v. Hsu 案被告人抗辩称，争议商业秘密申请专利获准授权后便已进入公共领域成为通用知识，因而欠缺商业秘密的秘密性。目前司法实务认为，信息成为专利申请的对象并不意味着该信息丧失了商业秘密的法律保护。美国专利法并未规定，发明人在专利申请获准之后必须公开其申请材料并完全披露其因发明所获取的所有技术与金融信息。〔36〕对于争议商业秘密已在公司日常经营活动中向顾客公开而丧失秘密性的抗辩，司法实务往往不予认可。前述 U. S. v. Hanjuan Jin 案裁判要旨即已明确：即使部分商业秘密曾公之于众，但对于公司文件中未向公众披露的这部分技术信息，不认定其丧失秘密性。

（2）“商业秘密规范描述的违宪性”与“欠缺不法意识”之抗辩。如 U. S. v. Chung 案的被告人答辩称，《经济间谍法》未能准确定义“商业秘密”术语的含义，主张《经济间谍法》违宪因而不能作为认定犯罪之依据。但目前司法实践对该抗辩几乎不予支持。审理法院强调，规定犯罪与刑罚的规范必须充分界定犯罪行为构成要件，使得一般社会公众能够理解规范具体禁止何种行为，质言之，只要求以一般人的理解与常识能够明白规范语言所传达出的禁令内容即可。关于被告人以商业秘密的定义界定模糊为由主张合宪性抗辩，审理法院指出，在“a. 被告人明知其提供给外国政府的信息系属公司专有机密信息，且只有项目内部人员才有权限接触；b. 波音公司要求被告人签署数份保密协议；c. 被告人明知波音公司为保护其专有信息所采取的系列保密措施以及外国政府为获取该信息所付出的种种‘艰辛’”等情形之下，凡智力正常的人都能够意识到争议信息是商业秘密，被告人亦不例外，因此驳回其无罪抗辩。再者，《经济间谍法》立法之初便存在如下担忧：严格的商业秘密立法保护将导致刑法过度介入社会生活而限制国民行动自由，这可能影响员工自由选择工作之权利，不利于美国经济与科技的长远发展。但是，《经济间谍法》的立法目的并不在于禁止离职员工利用自身具备的一般知识或专业知识，或正当使用个人在任职

〔33〕 United States v. O'Rourke，417 F. Supp. 3d 996（N. D. Ill. 2019），appeal dismissed，No. 19 - 3179，2019 WL 8631809（7th Cir. Nov. 14，2019）.

〔34〕 United States v. Hanjuan Jin，833 F. Supp. 2d 977（N. D. Ill. 2012），affd，733 F. 3d 718（7th Cir. 2013）.

〔35〕 See Rockwell Graphic Sys.，Inc. v. DEV Indus.，Inc.，925 F. 2d 174（7th Cir. 1991）.

〔36〕 See United States v. Hsu，185 F. R. D. 192（E. D. Pa. 1999）.

期间习得知识的行为。〔37〕

（3）“行为人商业秘密的窃取行为没有裨益外国政府”的抗辩，具体分为两个切入点：一是行为裨益对象是否为“外国政府、外国机构或外国代理人”。如 U. S. v. Xiaoquing Zheng and Zhaoxi Zhang 案件显示，被告人 Zheng 在担任 GE 公司工程师期间，利用职务便利窃取含有该公司燃气和蒸汽涡轮机的组件与测试系统的专有技术，并将所窃取专有技术加密传输给在中国的合作伙伴 Zhang 以裨益两家中国企业。经查明这两家受益公司是由中国政府所有、实际控制、资助、指导、管理的。因此，两被告人面临着明知窃密行为将有利于外国政府及其所实际控制机构仍共谋实施商业间谍行为的指控。〔38〕二是行为是否“裨益”外国政府。实务立场坚持，“裨益”不限于有形利益。如 U. S. v. Lan Lee and Yuefei Ge 案，被告人被控犯有共谋与实质性商业间谍罪以及商业秘密窃取罪。在商业间谍罪的认定上，本案的争议与存疑之处在于被告人是否意图使其商业秘密窃取行为或明知其窃取行为将“裨益外国政府、外国机构或外国代理人”。公诉机关试图通过证明被告人意图向中国政府主导的 863 项目（国家高技术研究发展计划）申请 350 万美元的发展资金，使陪审团相信被告人窃取商业秘密行为系“裨益”外国政府。二被告人辩称，即使美国政府能够证明这一点，也不能因此认定系意图“裨益”外国政府，因为这里的“利益”应限于有形利益。〔39〕

诚然，“裨益”或“有利于”是十分广泛的概念，取决于“利益”的内涵与外延范围。但该构成要件是对行为人行为犯罪化与否以及裁量刑罚时最主要的根据，也是具体案件被告人与公诉机关的争议焦点。就其形态而言，利益可分为有形利益与无形利益，前者如金钱等，后者譬如求职升学、升迁机会、名誉荣誉等。“利益”范围的解读在 U. S. v. Lan Lee 案中至关重要。裁判理由强调，公诉人虽然没有任何证据证明被告人意图与中国政府或其机构建立风险投资关系，但确有证据证明被告人意图向中国 863 项目申请资助：政府对外资助他人发展表面上是不能获得实质性利益回报的“赔本买卖”，而实质上却不能排除政府通过对外提供资金的“赔本买卖”来赚取名誉荣誉上的“吆喝”。法院提出，这种名誉荣誉上的回报亦在“利益”涵摄范围之内，即“裨益”不限于“经济上”之利益，更包括“名誉、荣誉、策略、战略”等无形利益。

三、美国《经济间谍法》的内核机制及其评介

《经济间谍法》在美国乃至世界历史上都具有开创性意义，其是美国首部专门针对商业秘密保护的联邦级别刑事法律，根据行为人主观目的之不同明确区分商业间谍罪与商业秘密窃取罪，并对前者设置更严格的法定刑以严惩有外国政府因素介入的商业间谍行为。

（一）商业间谍定义的理论分歧与规范界定

究竟何谓“商业间谍”？有学者将商业间谍形象地界定为“高风险的斗篷与匕首间谍游戏”

〔37〕 See United States v. Chung，622 F. Supp. 2d 971（C. D. Cal. 2009），order amended and superseded，No. SACR08 - 00024 - CJC，2009 WL 10680757（C. D. Cal. Apr. 21，2009）.

〔38〕 See United States v. Xiaoquing Zheng，No. 1：19 - CR - 156，2020 WL 6287481（N. D. N. Y. Oct. 27，2020）.

〔39〕 See United States v. Lan Lee，No. CR 06 - 0424 JW，2010 WL 8696087（N. D. Cal. May 21，2010）.

(high-stakes cloak-and-dagger spy game)，持论者认为，商业间谍活动是外国公司与外国政府为主体实施的窃取美国科学技术与商业秘密的行为。〔40〕另有学者认为商业间谍是当今世界经济战的前线，并指出区别于传统政治军事间谍，商业间谍是外国情报机构为争取竞争优势或非法利用外国科学技术以巩固本国军事实力而对另一国企业工业实施的间谍活动。〔41〕也有学者主张，商业间谍是外国政府资助、协调或协助情报机构实施的非法或秘密地锁定或获取别国国内政府、企业、机构或个人的商业秘密及敏感的金融、贸易或经济政策信息的行为。〔42〕根据该定义，商业间谍的侵害对象包括外国国内政府机构在内，例如 A 国情报机构对美国政府机构 B 开展间谍活动同样构成商业间谍。但此类间谍活动传统上隶属于政治军事间谍范畴，这无疑会导致商业间谍的外延过于宽泛。加拿大安全情报局对商业间谍的界定更为明确，即“由外国政府参与或促成的非法、秘密、胁迫或欺骗活动，旨在为经济利益获得未经授权的经济情报，如专有信息或技术”〔43〕。

不同于将商业间谍行为对象界定为包括“敏感金融、贸易或经济政策信息”在内的观点，《经济间谍法》明确立法意图旨在保护企业的商业秘密。在《经济间谍法》中，商业秘密的范围非常广泛，包括任何类型的金融、商业、科学、技术、经济或工程信息，包括但不限于模式、计划、编译、程序设备、公式、设计、原型、方法、技术、过程、程序、项目或代码等信息，包括有形的或无形的信息，存储、编辑或记忆方式涵盖物理的、电子的、图形的、摄影的、书面的等。《经济间谍法》明确，判断争议信息是否为商业秘密有三个构成要件：其一，具备秘密性；其二，具备独立经济价值性；其三，所有人已采取合理保密措施。〔44〕有论者评道：“从这个定义来看，商业秘密的范围包括想法和意念。因此就很难找到不是商业秘密的例子。”〔45〕其中，商业秘密的秘密性强调不为一般民众所知悉，且公众通过合法手段也难以确定、取得或开发该信息。〔46〕质言之，即使涉及该类信息之人知悉此信息，但若一般人不知悉，该信息仍符合秘密性构成要件。商业秘密的经济价值性系指由其秘密性所衍生出来的具有实际或潜在的、独立的经济价值。关于第三个构成要件，前已述及，所有人已采取保密措施是“合理的”即可，而非穷尽所有可能想到的措施，而保密措施是否合理的司法实务判断应根据具体案件实际地衡量措施的成本与收益。

（二）《经济间谍法》之核心内容：商业间谍罪与商业秘密窃取罪

作为《经济间谍法》的核心内容，商业间谍罪与商业秘密窃取罪的罪刑规范详细规定行为该当犯罪的构成要件，对国内国外商业秘密窃取行为实施者科处刑责，有利于威吓与遏制由企业竞

〔40〕 See Jonathan Eric Lewis, The Economic Espionage Act and the Threat of Chinese Espionage in the United States, 8 *Chi.-Kent J. Intell. Prop.*, 189, 194-195 (2009).

〔41〕 See Karen Sepura, Economic Espionage: The Front Line of a New World Economic War, 26 *Syracuse J. Int'l L. & Com.*, 127, 128-129 (1998).

〔42〕 See Darren S. Tucker, The Federal Government's War on Economic Espionage, 18 *U. Pa. J. Int'l Econ. L.*, 1109, 1112 (1997).

〔43〕 前引〔41〕，Karen Sepura 文，第 128 页。

〔44〕 See 18 U. S. Code § 1839 (3).

〔45〕 刘妙香、白恒晶：《美国〈经济间谍法〉对商业秘密的超强度保护》，载《法学杂志》2002 年第 4 期。

〔46〕 参见时英：《从美国〈经济间谍法案〉看商业秘密的保护》，载《国际贸易问题》1998 年第 9 期。

争对手实施的商业秘密窃取行为以及在外国政府介入下的商业间谍犯罪行为，从而维护国家经济安全与国家利益。

商业间谍罪罪刑规范专门规制行为人未经授权非法窃取商业秘密，且明知其商业秘密窃取行为“将裨益任何外国政府、外国机构或外国代理人”仍实施之。〔47〕商业秘密窃取罪罪刑规范系针对行为人未经授权非法窃取商业秘密，并意图将所窃取商业秘密转化为“所有人之外”的第三人之“经济利益”，且主观上明知或应当知道其犯罪行为将损害商业秘密所有人。〔48〕不同于商业间谍罪，商业秘密窃取罪要求行为人必须意图将商业秘密转化为所有人之外的任何人的“经济利益”。即使无法查明行为人窃取商业秘密行为是为何人之经济利益，只要行为人不是为“所有人”经济利益而实施犯罪，都可进行刑事追究。

商业间谍罪的受益方或潜在受益方具有特定的指向。其中，外国机构系指实质上为外国政府所有、控制、资助、命令、管理或支配的任何机关、局、部门、协会，或任何法律组织、商务组织或商业组织、公司或实体等。外国代理人系指任何外国政府之官员、雇员、受托人、公务员、与会人员以及代表。〔49〕不论外国机构抑或外国代理人，皆系在政治上或经济上与外国政府有这样或那样的联系，具有深刻的政治化属性。正是因为商业间谍犯罪中存在外国政府这一政治因素的介入，该外国政府有从中获益之可能，才有必要将该行为从广义的商业秘密犯罪行为中剥离出来单独规制并加重处罚。较之商业秘密窃取罪，商业间谍犯罪的法益侵害不仅在于商业秘密所有人的财产权，更包括国家安全与社会公共利益。对于并非由外国政府扶持教唆，或行为人主观上并无意图裨益外国政府的商业秘密窃取行为，则以商业秘密窃取罪追诉之。如前述之U. S. v. Hanjuan Jin 案，因现有证据不足以证明被告人系为中国政府的利益而实施商业秘密窃取行为，故承审法院否决了对被告人犯“商业间谍罪”的指控。

除受益方与潜在受益方的不同，这两类犯罪具有以下相同的构成要件：其一，犯罪对象要件，即争议信息须是符合法定构成要件的商业秘密；其二，侵害行为要件，即行为人的行为须是不法的；其三，主观意图要件，即商业间谍罪中意图裨益外国政府等，商业秘密窃取罪中意图转化为所有人之外的第三人之经济利益；其四，主观故意要件，即商业间谍罪中明知其行为将裨益外国政府等，商业秘密窃取罪中明知其犯罪行为将损害商业秘密所有人。此外，这两类罪刑规范都对共同犯罪、犯罪的未完成形态、自然人犯罪与单位犯罪及其量刑等作出规定。例如，禁止二人以上共谋对商业秘密实施规范所列举的任何一种犯罪行为。〔50〕意图实施商业秘密窃取行为同样是不被允许的。〔51〕根据该法对被告人提起公诉，并不以其成功实施罪刑规范所禁止的行为为必要，本罪的未完成形态同样受到惩罚。自然人犯罪的，对自然人判处自由刑或单处罚金，或并罚；单位同样具有犯罪主体之资格，单位构成犯罪的，处罚金。〔52〕但不论是自然人犯罪抑或单位犯罪，商业间谍罪规定的自由刑或罚金刑上限皆明显高于商业秘密窃取罪，这反映出国家对存

〔47〕 See 18 U. S. Code § 1831.
〔48〕 See 18 U. S. Code § 1832.
〔49〕 See 18 U. S. Code § 1839 (1) & (2).
〔50〕 See 18 U. S. Code § 1831 § 1832 (a) (5).
〔51〕 See 18 U. S. Code § 1831 § 1832 (a) (4).
〔52〕 See 18 U. S. Code § 1831 (a) (individuals) & (b) (organizations); § 1832 (a) & (b) (same).

在外国政府扶植唆使，或行为人主观上意图裨益外国政府等情形下的商业秘密窃取行为更低的容忍度。除此之外，公诉机关还可以要求被告人归还其非法占有之商业秘密，〔53〕并因普通法上侵权损害赔偿的主要目的在于弥补商业秘密所有人过去所受的损失，为避免被告人将来可能继续对权利人造成损害，公诉机关可以诉请法院适用禁令救济制度，以防止未来损失的继续和扩大〔54〕。

在追诉对象范围上，《经济间谍法》明确，自然人犯罪的，只要是美国公民或永久居民，单位实施犯罪的，只要其是根据美国法律、各州法律及其政治分支机构法律而成立的组织，无论其犯罪行为发生在境内抑或境外，联邦政府均可对其进行刑事追诉。此外，即使犯罪实行行为发生在美国境外，只要促成实行行为的其他行为如帮助、教唆行为发生在美国境内，都系属本罪罪刑规范追诉的对象。〔55〕据此，犯罪行为即使发生于美国领域外，但只要犯罪行为“人”是美国公民或美国永久居民，或系依据美国法律成立的组织，联邦政府仍能根据属“人”管辖原则行使管辖权；或者只要犯罪行为发生在美国领域内的，不论是实行行为还是促成行为，也不论行为“人”之国别，仍能根据属地管辖原则对案件进行管辖。显然，《经济间谍法》的域外效力规定赋予美国联邦政府追诉域外商业秘密窃取行为的力量与权力，对本国经济利益进行更为全面的保护。

《经济间谍法》同时还规定了商业秘密保密命令制度。在涉及商业秘密案件的审理过程中，现代国家往往通过不公开审理、不公开质证、不公开文书等变通相关诉讼程序的措施来防止商业秘密在诉讼程序中遭到泄露。但是，变通现有诉讼程序制度虽能有效防止诉讼参与人之外的主体泄露或滥用案涉商业秘密，却难以完全禁止诉讼参与人对在诉讼中知悉的商业秘密的不当利用或泄露。对此，《经济间谍法》明确，在适用本章规定所实施的司法程序中，法院可对符合法定条件的案件颁布保密命令并采取必要且合理措施防止商业秘密遭到泄露。〔56〕此外，除非所有人明确表示弃权，否则所有人依法定程序将其商业秘密提供给政府或者法院或者对其进行披露之行为并不当然构成对商业秘密保护的弃权。〔57〕商业秘密案件的审理难免要在一定范围内披露商业秘密，这加大了所有人利益风险。保密命令制度的创设与运行有力地缓和了商业秘密保护与正当审判程序之间的紧张状态，为现代国家和地区所普遍采用。例如我国台湾地区的“智慧财产案件审理法”第 18 条第 6 项规定，为防止申请人利用诉前证据保全程序实施窥探他人营业秘密，可以适用本法秘密保持命令。〔58〕

四、美国商业间谍立法对我国的借鉴价值

美国商业间谍立法及其实践客观上引领着国际商业秘密立法之趋势，我国对商业秘密的立法保护、司法实践以及理论研究应积极镜鉴美国法中具有时代价值的内容机制。

---

〔53〕 See 18 U. S. Code § 1834 (2012).

〔54〕 See 18 U. S. Code § 1836 (a) (2012).

〔55〕 See 18 U. S. Code § 1837.

〔56〕 See 18 U. S. Code § 1835 (a).

〔57〕 See 18 U. S. Code § 1835 (b).

〔58〕 参见沈冠伶：《智慧财产民事诉讼之新变革》，载《台湾月旦民商法杂志》2008 年第 21 期。

（一）促进商业秘密法律保护体系的完善及国家科技进步

《经济间谍法》以联邦刑事规范将商业秘密侵害行为区分为普通的商业秘密窃取行为以及存在外国政府扶植或唆使，或行为人意图裨益外国政府情形下的商业间谍行为，将商业秘密保护上升为全国性的运动，并对相关犯罪行为实施最严厉、对行为人施加最痛苦的否定性评价。这一举措有力地弥补了美国联邦法律体系中有关商业秘密刑事规范保护的漏洞，有利于维护商业关系中的伦理道德规范，为保护国内企业商业秘密提供良好的法治环境，也有助于增强企业创新创造的激情与信心，从而有助于国家经济发展。正如美国联邦最高法院首席法官沃伦·伯格所言，商业秘密立法背后的既定政策在于维护商业伦理道德与鼓励发明与创新。〔59〕美国商业秘密法律保护体系是对这一政策的现实写照与诠释。

（二）充实并发展商业秘密法律保护的法理基础

商业秘密法律保护理论基础学说主要包括“契约义务违反说”“信任关系违背说”以及“侵权行为理论说”等。〔60〕但现有学说主张无不是坚持商业秘密为私权或民事权利的法律定位。如在“契约义务违反说”中，法院依据当事人之间的合意来保护商业秘密；“信任关系违背说”根据契约之外的特殊关系推定当事人具有保密义务，系“契约义务违反说”的进一步发展；“侵权行为理论说”将商业秘密视为一种具有价值并能给权利人带来竞争优势的无形财产，任何以不正当手段获得或利用商业秘密的行为都构成侵权。〔61〕商业间谍罪的设置是以代表公权的刑事处罚介入商业秘密保护，使得商业秘密保护的法理基础不仅局限于民事权利的侵犯或是特定主体之间民事关系的违背，而是上升到维护良好市场竞争秩序的社会利益以及国家安全利益保护的高度，并在一定程度上突破商业秘密的私权属性。对此，外国学者曾言明，在现代交通与网络科技发达的时代，企业商业秘密已然突破原有的纯粹私有权利属性，演变为一种国家与企业所有人共同拥有所有权的混合型财产权。国内企业商业秘密的失窃与泄露不仅会导致企业丧失竞争优势，还会危及国家在经济上、战略上的利益，或因维持商业秘密的秘密性所能获得的其他利益。〔62〕

（三）创新并拓宽商业秘密法律保护的路径选择

根据援引规范的不同，商业秘密法律保护路径具体区分为合同法保护路径、侵权行为法保护路径以及反不正当竞争法保护路径等，但上述路径主要诉诸私法救济，不属于打击与遏阻商业间谍的合理路径选择。首先，原告须承担相当程度的举证责任。在当事人之间力量与资源悬殊的情形下，受害方可能囿于经济实力的不足或缺乏足够的调查资源而不得不放弃寻求公力救济。由此产生某种法律上的偏差：肇事者是否要承担侵权责任，并非基于处于危险中的商业秘密，也并非基于法律规定的侵权行为构成要件实现与否，而似乎取决于当事人之间资源实力的对抗。其次，即使原告圆满履行举证义务，侵权损害赔偿亦难以有效弥补其因商业秘密的失窃与泄露而遭受到的经济损失。毕竟侵权损害赔偿的目的往往在于填补受损害方因侵权行为遭到的损失，使其权利

〔59〕 参见王彦怀：《美国商业秘密立法及司法实践浅析》，载《北方论丛》2001年第5期。

〔60〕 参见孙山：《反思中前进：商业秘密保护理论基础的剖解与展望》，载《知识产权》2011年第8期。

〔61〕 参见黄勤南主编：《知识产权法学》，中国政法大学出版社2003年版，第369页。

〔62〕 See Susan W. Brenner，Anthony C. Crescenzi，State-Sponsored Crime：The Futility of the Economic Espionage Act，28 *Hous. J. Int'l L.*，389，461（2006）.

恢复到侵权行为发生之前的状态，但不会对商业秘密泄露产生的损失进行赔偿。换言之，主要以民事上的填补损害赔偿原则或发布禁令的方式来救济业已遭到侵害的商业秘密，无法有效吓阻与遏制相关侵权行为，也无法真正弥补商业秘密所有人的损失。再者，诉诸民事救济难以保证侵权人履行义务。在以民事救济为主的法律规范框架下，往往会发生一些阻碍民事判决正常执行的情形，致使许多企业不得不放弃民事追诉。〔63〕例如侵权人以隐藏、转移财产等方式导致无足够财产可供履行义务，于是补偿判决就成了无法兑现之“空头支票”。更有甚者，施害者视民事赔偿判决如无物，不配合执行的情况时有发生。

此外，《经济间谍法》特别强调将国家安全与经济安全划等号，这也为我国商业秘密保护提供了刑事规制的路径借鉴。不同于民事损害填补原理，刑事制裁通过对规范违反者施以刑罚的方式来惩罚行为人并预防未来刑事越轨行为的发生。鉴于商业间谍对国家整体经济与政治安全的影响与威胁，国家法律理应通过给予肇事者刑事惩罚，为商业秘密提供清晰明确的保护路径，有力规范商业秘密的不当使用。

（四）商业秘密保护应紧跟国际潮流、应对国际挑战

《经济间谍法》发布之初，将商业秘密保护纳入联邦刑事法律规制范围所引起的质疑之声甚至发展到国际层面，这一举动引起国际社会的广泛关注。不过，实践强有力地证实美国以刑事路径规制商业秘密窃取行为的前瞻性与正确性，加强商业秘密刑事保护业已成为知识经济时代世界各国的普遍选择。〔64〕我国此次对知识产权犯罪的修正更是被视为“回应人民关切”的看点之一。〔65〕除对传统知识产权犯罪增加行为类型以拓展犯罪圈，并大幅提升法定刑进一步加强保护外，《刑法修正案（十一）》还专门增设为境外窃取、刺探、收买、非法提供商业秘密罪，强化商业秘密的刑法保护，严防境外非法获取、利用境内商业秘密。“徒法不足以自行”，国家以立法犯罪化形式将商业间谍行为纳入刑法规制后，应当重视对该罪罪刑条款的规范化阐释，这对后续具体案件的司法处置以及推动未来科学立法都有重要意义。就目前本罪的规定来说，牵涉的关键问题有三。

其一，本罪的犯罪对象系商业秘密。《刑法修正案（十一）》删除原第 219 条“侵犯商业秘密罪”第 3 款关于商业秘密的概念，似乎放弃了商业秘密司法认定的明确标准，难免产生商业秘密犯罪打击面无限扩张与司法适用泛化的法治担忧。不过在我们看来，这种担忧实无必要。此次刑法修正删除商业秘密定义的真意在于维护法秩序的统一：修正前《刑法》对商业秘密的界定是对 1993 年《反不正当竞争法》第 10 条的原文照搬。但问题在于，《反不正当竞争法》的规定已经多次修改，而照搬原文的《刑法》第 219 条第 3 款却迟迟不见更新。不仅如此，涉及该罪名的刑事司法解释、有关知识产权刑事案件立案追诉标准的规定以及各地检法的会议纪要等亦未见修订。〔66〕《刑法修正案（十一）》将商业秘密定义删除既可使《反不正当竞争法》作为前置法的功

〔63〕 See Mark Halligan, The Theft of Trade Secrets is Now a Federal Crime, 8 *Competitive Intelligence Review*, 7, 10 (1997).

〔64〕 参见杨燮蛟：《知识产权刑法学的建构及其应用》，浙江大学出版社 2018 年版，第 9 页。

〔65〕 参见张宝山：《刑法修正案（十一）草案：回应人民关切》，载《中国人大》2020 年第 13 期。

〔66〕 参见谢焱：《商业秘密刑事条款与新〈反不正当竞争法〉的衔接》，载《交大法学》2020 年第 4 期。

能作用不至落空，也可避免因《反不正当竞争法》频繁修改而导致商业秘密定义在国家规范体系中的偏差与矛盾，是立法理念以及立法技术的重大进步。

其二，商业秘密的具体认定标准应作出相应调整。修正后对商业秘密构成要件的把握应与《反不正当竞争法》（2019年修订）第9条第4款对商业秘密的重大修改保持一致，如表1所示：

表1　　修订前后商业秘密构成要件的对比

	修订前商业秘密的构成要件	修订后商业秘密的构成要件
规范表述	不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息。	不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。
构成要件	非公知性、价值性、实用性、保密性	非公知性、价值性、保密性
内涵外延	技术信息和经营信息	技术信息、经营信息等商业信息

相较于修正前商业秘密构成要件，修正后商业秘密的特征有三处明显差异：一是删去原来的“实用性”特征。《刑法》修正之前，不乏“实用性”特征并无存在之必要的理论主张，有论者认为“实用性”特征使得消极性信息（如失败的商业经验）被排除在商业秘密之外，但这类信息同样需要法律的保护，否则无异于鼓励竞争对手不择手段获取这类信息，极易对公平有序的市场竞争秩序造成冲击与破坏。〔67〕二是将“经权利人采取保密措施”修改为“经权利人采取相应保密措施”，增加“相应”二字实质放宽对权利人采取保密措施的要求，这与并不苛求商业秘密权利人穷尽所有而仅需采取“合理”保密措施即可的《经济间谍法》具有类似旨趣。三是将商业秘密的具体范围进一步扩充为“技术信息、经营信息等商业信息”。据此，诸如既不属技术信息也非经营信息的数据信息等商业信息，在今后司法实践中有可能被认定为商业秘密并得到刑法的有力保护，这也回应了此前学者关于对非法获取并使用非公开性衍生数据的行为以侵犯商业秘密罪规制的主张。〔68〕

其三，准确把握商业间谍犯罪法益侵害实质。法益保护是刑法的重要使命，准确厘定法益是规范适用刑法的前提。前已述及，商业秘密具有双重属性，既关系到权利人的私有财产权，又关系到国家市场经济秩序安全，因此围绕商业秘密的刑法保护，“国际社会一直存在着以维护正当市场竞争秩序为依归的竞争法模式与保护权利人的私有财产权为核心的侵权法模式之争”〔69〕。《刑法修正案（十一）》将为境外窃取、刺探、收买、非法提供商业秘密罪设置在刑法分则第三章“破坏社会主义市场经济秩序罪”中，强调从市场经济竞争秩序的维度完善商业秘密的刑法保护体系。相较来看，美国《经济间谍法》径行将商业秘密与国家安全等同论之，在美国优先的外交政策影响下，该规范日渐异化为美国遏制其他国家发展的法律工具。特别是晚近以来，随着国际经贸往来与人才交流的日益频繁，美国动辄以“保护商业秘密”“维护国家经济安全”为由，对开展涉美业务的外国企业、个人抑或政府以商业间谍恫吓之，美国联邦调查局更是频频闹出

〔67〕 参见寇占奎、许振台：《Trips协议中未披露信息与我国商业秘密构成要件的比较》，载《经济论坛》2002年第21期。

〔68〕 参见刘双阳：《衍生数据刑法保护进路的多重考察——兼论财产权客体的时代变迁》，载《科技与法律》2020年第3期。

〔69〕 田宏杰：《强化知识产权保护的又一里程碑》，载《检察日报》2021年1月6日，第3版。

“司法乌龙”与“中国间谍”冤案（如郗小星教授间谍案），使得美国司法逐渐沦为政治武器。〔70〕在“中国行动计划”中，美国甚至将执法的枪杆子对准自己国内公民、机构和企业，比较有影响的案件如哈佛大学“利伯”案。〔71〕可以预见，此次《刑法修正案（十一）》对我国商业秘密刑法保护体系的重大完善必将有利于我国企业、公民以及政府有效应对包括美国在内的国际社会强化商业秘密法律保护、维护国家经济安全的时代需要以及现实挑战。

五、我国对美国商业间谍刑事立法威胁的应对之策

2020 年 1 月 15 日，中美两国签署《中华人民共和国政府和美利坚合众国政府经济贸易协议》，为两国之间长达一年多的“贸易战”画上休止符，但是两国在经济、政治、科技、法律等方面的竞争仍在持续并有加剧之势。

在知识经济和全球化经济不断深入发展的时代背景下，知识产权日益成为中美两国博弈的“进攻之矛”与“防守之盾”。早在 21 世纪初，在美国政治力量的鼓吹下，中国便被视为美国商业秘密的“头号威胁”，此等昭然若揭的敌对立场同样存在于美国的学术界。例如有学者撰文称，中国政府为促进经济发展极力倡导以非法手段窃取美国先进科学技术。〔72〕更有甚者认为，《经济间谍法》难以有效应对中国政府支持下的商业间谍活动给美国国家安全带来的威胁，主张应同时运用旨在遏阻中国商业间谍活动的政治与外交举措，进一步提高《经济间谍法》的法定刑确保打击力度。持论者进一步呼吁，应增设新罪专门规制为使外国政府获益，故意帮助、预谋帮助或实施计算机黑客行为以窃取商业秘密或破坏美国商业或政府计算机信息系统的行为。〔73〕

美国《经济间谍法》可谓是悬在中国头顶上的“达摩克利斯之剑”。该法已异化为遏制中国发展的法律工具，该规范虽能用以遏阻与惩治不正当竞争行为，维护良好的市场秩序，也存在被滥用于恶意打压甚至于扼杀中国企业的风险。如 United States v . Yang 案中，美国联邦情报局以创造性证据实施诱捕，但如此明显不公正之侦查手段依然得到美国法院确立的判例原则的认可：针对经济间谍犯罪嫌疑人，可以虚假的商业秘密实行诱捕定罪。该案指控书显示，1989 年，艾利公司员工李担任四维公司技术顾问，此后 8 年间，李通过邮件向四维公司传输艾利公司的专有商业秘密。1997 年，李获取艾利公司在亚洲的商业拓展秘密计划后，意图向四维公司董事长披露时被发现导致案发。之后李与美国合作，以艾利公司保密资料对四维公司董事长进行诱捕，后者被指控犯有窃取商业秘密罪。1998 年 4 月 28 日，俄亥俄州北区地区法院陪审团作出有罪认定。〔74〕但所谓的艾利公司的保密信息几乎被专门设计用于诱捕。令人瞠目结舌的是，这些信息完全是依据当初合作过程中四维公司提供的技术、客户信息以及市场分析资料等编制而成。〔75〕

〔70〕 参见李永成：《间谍冤案令在美华裔不安》，载《社会观察》2015 年第 10 期。
〔71〕 参见杨先德：《美执法机关办理的涉“中”案背后》，载《检察风云》2020 年第 11 期。
〔72〕 参见前引〔4〕，Michael L. Rustad 文，第 464 页。
〔73〕 参见前引〔40〕，Jonathan Eric Lewis 文，第 193 页。
〔74〕 See United States v. Yang，74 F. Supp. 2d 724（N. D. Ohio 1999）.
〔75〕 参见张玉瑞：《商业秘密的法律保护》，金城出版社 2002 年版，第 5 页。

换言之，四维公司案中，赖以定罪的证据是创造性的而非证明性的。正如学者指出："在刑事诉讼中，只有嫌疑人重复相同性质的行为时，FBI 所设陷阱才能是在先犯罪的证据；如果嫌疑人以前没有相同行为，那么这种陷阱，足以使任何没有警觉的经营者，被控构成犯罪。"〔76〕

不仅如此，美国《经济间谍法》明确其条款并不排除其他商业秘密补救措施，而这更是让我国芒刺在背。United States v. Aleynikov 案被告人谢尔盖·阿列尼科夫（Sergey Aleynikov）曾系高盛集团计算机程序员，其在即将离职之际秘密窃取老东家专有计算机源代码，准备在总部位于芝加哥的特扎科技有限责任公司正式就职时使用。〔77〕2012 年 4 月 11 日，第二巡回法院认定被告人的行为不违反联邦法规《经济间谍法》并推翻对阿列尼科夫的定罪。然而，纽约上诉法院仍维持对其"非法使用秘密科学材料"的定罪。〔78〕《经济间谍法》明确经济间谍罪与商业秘密窃取罪罪刑条款不优先于任何其他商业秘密补救措施，因此被害企业仍有权依据联邦或州法律规定追究行为人的法律责任。外国人在美国境内不被豁免追诉，这就意味着涉嫌相关犯罪的当事人将面临双重甚至多重控诉。

对于开展涉美业务的中国企业、个人乃至我国政府而言，规避风险的最佳措施往往不是等到开庭受审时进行法律抗辩，而应在被卷入美国商业间谍纠纷案件之前即做好事前"防御"性规划。如为规避受到美国政府调查的法律风险，应携带"清洁"电子产品出入美国。在该语境下的"清洁"电子产品，是指具备存储功能，但储存内容不存在任何可能被美国政府刑事追诉的敏感商业信息的电子产品，包括移动手机、平板电脑、手提电脑或移动硬盘等等。这主要是考虑到，根据美国《爱国者法案》，美国联邦调查局以及美国海关有权对在他们看来可能危害美国国土安全的嫌疑人在出入美国边境时所携带的电子储存产品进行内容扫描和必要的备份。〔79〕

另一方面，随着市场经济的快速发展，人才频繁流动虽然能够充分发挥人才优势，但也存在商业秘密窃取与泄露的风险，从而使雇佣公司可能陷入法律纠纷的漩涡之中。〔80〕在美国法院审理的涉及商业秘密刑事案件中，雇员窃取老东家商业秘密而连累雇佣公司甚至是本国政府的案例占了绝大多数。这反映出企业加强合规管理的重要性，毕竟按照通常逻辑和法理，企业法人应当为其员工的行为负责，一国政府应当为其代理人的行为负责。而在美国的司法实践中，企业合规已成为联邦检察官机关对涉嫌经济犯罪的企业起诉量刑时的重要考虑要素。根据《美国量刑指南》，一个完备的合规计划甚至可以将企业的罚款参考数额降低 30%，亦即完备合规计划能够帮企业免去数百万美元乃至更多的罚金。〔81〕这无疑从外部激励了参与对美贸易的中国企业积极强化自身合规建设，尽可能消除生产经营中存在的合规风险。

---

〔76〕 参见张玉瑞：《盗窃商业秘密构成经济间谍犯罪——美国 1996 年反经济间谍法及相关案例介绍》，载《电子知识产权》2001 年第 11 期。

〔77〕 See United States v. Aleynikov，785 F. Supp. 2d 46，54（S. D. N. Y. 2011），rev'd，476 F. App'x 473（2d Cir. 2012）.

〔78〕 See Robert Damion Jurrens，Fool Me Once：U. S. v. Aleynikov and the Theft of Trade Secrets Clarification Act of 2012，28 *Berkeley Tech. L. J.*，833，833－834（2013）.

〔79〕 参见周立权：《商业秘密保护指南》，中国社会出版社 2019 年版，第 154－155 页。

〔80〕 参见赵天红：《商业秘密的刑事保护研究》，中国检察出版社 2007 年版，第 102 页。

〔81〕 参见李本灿等编译：《合规与刑法：全球视野的考察》，中国政法大学出版社 2018 年版，第 147 页。

Abstract: The Economic Espionage Act of 1996 is the first federal criminal statue to address trade secrecy misappropriation, altering the judicial custom of protecting trade secrets under states' common laws, laying the foundation for the legal system of regulating against trade secret crimes, and leading the legislative tendency of international trade secrets protection. EEA draws a clear line between economic espionage and theft of trade secrets on the basis of subjective differences, and enforces higher legal sentence on the former in an attempt to deter and punish the theft of trade secrets with foreign governments involved, taking into consideration the defense of both trade secrets and national security. The regulation is gradually becoming the legal tool used by the American government to curb China's development. The principle set forth by the American court that defendants could be convicted through fabricated evidence makes it easier for American corporate competitors to maliciously push Chinese company out of the market. The EEA expressly states that it does not preempt any other trade secret laws, which leaves companies open to pursue federal or state actions. For Chinese companies, citizens or government involved with U. S., the wisest method is taking defensive measures beforehand. Such measures include carrying clean electronic devices when entering and leaving the United States as well as corporate criminal management for Chinese companies.

Key Words: economic espionage act, trade secret, criminal regulation, defensive measures beforehand, corporate criminal management

(责任编辑：简　爱　赵建蕊)