

侵犯商业秘密的证明：推定规则、时间维度证据与电子数据

张佳英

商业秘密侵权的证明困难，并不集中于“接触”这一环。雇佣关系中的商业秘密侵权，被诉侵权人往往自始即在权利人内部任职或工作，对涉密信息具有现实的接触条件，接触事实在多数情形下并不难证明。更多的困难集中在权利人难以证明被诉侵权人所使用的信息与商业秘密实质相同，以及难以证明被诉侵权人获取手段的不正当性。

2025年6月27日修订、10月15日施行的《反不正当竞争法》将商业秘密侵权条款由第九条调整为第十条，将举证责任条款由第三十二条调整为第三十九条。第三十九条第二款确立的举证责任转移规则，正是针对上述困难作出的制度回应：权利人完成初步举证并提供法定证据之一的，涉嫌侵权人转而证明其行为不构成侵犯商业秘密。

本文讨论侵权行为的证明路径，依循“推定如何启动、时间维度证据如何补足、自主研发抗辩如何审查、数据如何固定”三个递进层次展开。所引案例的裁判时点均在本次修订之前，文中统一使用现行法条号，涉及旧法的另作标注。

一、推定侵权三要件：接触、实质相同、合法来源不成立

第三十九条第二款第一项为推定设置了入口：有证据表明涉嫌侵权人有渠道或者机会获取商业秘密，且其使用的信息与该商业秘密实质上相同。实务中形成的完整判断结构通常还要叠加第三环——被诉侵权人对信息来源未作合理说明，即“接触、实质相同、合法来源不成立”。

上述规则中的“接触”并非指权限有无，而是指向一个更精细的追问：主体虽有访问权限，其取得信息的过程是否正当。（2023）最高法知民终539号案件对此提供了明确答案。该案中，被诉侵权人曹某某系权利人北京某科技公司甲的技术人员，有权接触涉案游戏软件源代码。在提出离职申请前的一个多月内，其未经公司许可，分阶段将源代码带离公司经营场所，并存放至一台非

公司为其配备的苹果电脑，该电脑购置资金来自王某某的微信转账，发票显示购买方为北京某科技公司乙。

一审法院认为，曹某某虽有权接触、获得涉案技术秘密，但无证据显示其获取手段属于盗窃、贿赂、欺诈、胁迫或电子侵入，其行为虽将技术秘密转移至非办公电脑，但难以认定违反法律规定或公认的商业道德，据此驳回权利人诉请。二审改判，认为不能仅孤立地考察被诉侵权人此前有无接触权限、以及其获取方式是否对应法律明文列举的手段类型，而应综合审查获取意图及获取后实施的行为，判断该行为是否导致或者可能导致权利人失去对该商业秘密的有效控制。法院认定曹某某的获取手段明显难谓正当，其行为客观上已造成源代码脱离权利人有效控制以及被披露、被他人使用的重大商业风险，符合“以盗窃手段获取权利人的商业秘密”。

该案的规则意义在于：有权接触是获取合法性的抗辩，而非获取行为的免责事由。权利基础上的访问权限，恰恰应当与获取行为的正当性审查分开评价。

指导性案例 273 号（浙江吉某控股集团有限公司、浙江吉某汽车研究院有限公司诉威某汽车制造温州有限公司等侵害技术秘密纠纷案）将“接触、实质相同、合法来源不成立”这一结构具体化为三项可操作的事实。其一，人员流动异常。吉某集团下属成都高某公司近 40 名高级管理人员及技术人员于 2016 年前后离职，转入威某方及其关联公司。其中部分离职人员随后被威某集团、威某智慧出行公司列为发明人或共同发明人，申请了 12 件实用新型专利。其二，研发周期异常。威某温州公司成立于 2016 年 5 月，其 EX5 型号电动汽车于 2018 年 9 月即开始销售，从公司成立到产品量产销售仅两年多，短于独立研发所需的合理时间。威某方在无技术积累、亦无合法技术来源的情况下，短期内推出包括 EX5、EX6、E5 在内的 EX 系列车型。其三，技术信息实质性相同。将威某方 EX5 底盘零部件图纸及数模与吉某方案涉 12 套图纸及数模比对，存在大量完全相同的技术信息，其中包含吉某方特有的技术信息。

该案裁判要点确立的规则是：被诉侵权人招揽其他企业人才，形成获取该企业技术秘密的渠道或者机会，并在明显短于独立研发所需合理时间内即生产出与该企业技术秘密相关的产品的，可以推定其实施了侵害技术秘密的行为，但被诉侵权人提供相反证据足以反驳的除外。

两点尤须注意。其一，实质性相同采分层比对，不要求逐项完全一致。威某方基于产品定位、成本控制及自身车型特殊性对部分技术作了修改、改进，法院认为这不影响整体实质性相同的判断。其二，推定效力可及于全部案涉技术秘密，而不仅限于已完成比对的部分。在案证据既已证明被告使用了部分完全相同且含权利人特有技术信息的信息，又叠加人员流动与研发周期的双重异常，法院据此减轻权利人的证明负担，不再要求其就全部技术秘密被侵害进一步举证，而结合

汽车制造领域的研发规律与生产经验，直接推定被告实际获取、使用了全部案涉技术秘密。欲否定这一推定，须提出足以反驳的相反证据。

二、时间维度证据：形成时间与研发周期

当涉案技术难以进行逐项比对时——算法、模型、数据库类纠纷尤属典型——证明重心转向“谁先形成”的时间轴。

上海翎腾公司诉纸上绝知公司等侵害技术秘密纠纷案（（2023）最高法知民终 1503 号，最高人民法院知识产权法庭审理）说明了这一点。权利人通过 Gitlab 系统存储及管理代码、通过付费购买的商业空间存储训练图库，其上传文件日志显示训练图片自 2018 年 7 月 16 日起持续上传，至 2020 年 8 月存储量已达 4.34TB。法院据此认定涉案秘点在被诉侵权行为发生前已经形成。

该案的另一组事实是研发周期：涉案公司成立于 2019 年 5 月，至同年 7 月，其技术已使商业合作伙伴的产品具备手指定位及识别功能，历时未超过两个月。法院认为，在如此短的周期内从无到有推出一款具有人工智能视觉识别和定位功能的产品，有违日常经验法则。

被告抗辩称技术来源主要为各开源渠道收集的开源代码。法院未予采纳，理由是：将不同渠道的开源代码整合为初始模型并通过大量训练形成性能完善的模型，既是研发的关键环节，也是核心难点；在缺乏足够投喂数据支撑模型大量训练的情况下，仅凭开源代码即可在短期内使合作伙伴产品具备该功能，显然不合常理。法院同时注意到，被告提交的代码中未见涵盖 2019 年 4 月至同年 7 月的时间段。

由此形成一项实用规则：研发周期异常的作用并不在于免除权利人对“接触”与“实质性相同”的举证，而在于作为否定被诉侵权人合法来源抗辩的补强事实。权利人仍须完成“接触”与“实质性相同”的初步举证；在此基础上，被诉侵权人若主张自主研发，研发周期明显异常将使其关于研发过程的说明难以与客观进度相符，从而承担举证不利的后果。其逻辑基础是日常经验法则——一项技术的复杂度与所需研发投入之间存在可客观预估的对应关系，进度异常即构成对“独立研发”主张的实质怀疑。

三、自主研发抗辩的审查基准：穿透式而非文件罗列

举证责任转移后，被诉侵权人最常见的抗辩是主张技术信息具有合法来源，其中以自主研发最为常见。此类抗辩的审查重心，落在所提交证据能否体现研发过程的连续性与完整性。

建某公司诉康某公司、冉某、罗某某、张某等侵害技术秘密纠纷案（（2023）最高法知民终

1669号)完整呈现了这一审查思路。建某公司主张旋叶式汽车空调压缩机中转子、叶片等核心部件的设计参数构成技术秘密。经拆解比对,康某公司生产的A型压缩机从外观设计到内在布局与建某公司产品一致,相关零配件的公差系数与建某公司图纸设计亦完全吻合。冉某、罗某某、张某三人从建某公司离职后相继入职康某公司,其中冉某、罗某某在原单位任职时能够接触生产部图纸并向公安机关作了相应陈述。

一审法院认为,被诉侵权产品所包含的与建某公司主张密点相同或实质相同的技术信息,来源于侵权行为发生之前康某公司自主研发的技术信息,据此驳回诉请。二审法院认定自主研发抗辩不能成立,其理由指向三处:其一,无法证明技术来源的基础。康某公司未能证明被诉侵权产品系在相关高校与另一企业合作研发的既有型号基础上形成,且自始至终无法提供涉案图纸的纸质原件或电子文档。其二,时间逻辑与常理相悖。设计图纸是制作作业指导书的基础资料,图纸内容理应较作业指导书更为丰富、形成时间理应更早。但康某公司提交的图纸,形成时间晚于作业指导书,所体现的密点内容反而少于作业指导书,且仅有纸质复制件。这一情形不符合日常生活经验,真实性存疑。其三,证据之间无法相互印证。康某公司提交的发票中,21张开于2013年、型号仅记为"DDX-03",与其自述"应标注为完整型号"的说法不能自洽,不足以证明侵权产品技术在相关员工入职前已经存在。二审撤销原判,改判康某公司及三名自然人立即停止侵害、销毁相关载体、限期签署保密承诺书,连带赔偿经济损失及合理开支共100万元。

该案的启示是明确的:自主研发抗辩的证据准备,应当指向一个在时间逻辑、技术细节与其他证据印证关系上均能自洽的完整研发过程,而非若干份早于侵权事实的技术文件。零散文件的数量并不构成证明力,时间顺序上的自相矛盾反而可能成为突破口。

四、电子数据:从结果固定到过程还原

(一) 获取行为本身即构成侵权,不以披露、使用为要件

天津市第三中级人民法院(天津知识产权法庭)审理的一起侵害技术秘密纠纷案¹明确了"不正当获取"与"披露、使用"在侵权认定上的界限。被告小李于2022年8月入职原告公司担任机械设计工程师,签署保密协议,对在职期间获取的各类商业秘密(含设计、程序、技术文档等)负有保密义务。2024年7月某日凌晨,公司发现其办公电脑未关机且正被远程控制下载其无权限浏览的技术文件,随即报警。经调查,小李在即将离职之际为留存公司技术资料,陆续下载了100

¹ 2025年审结。

余份技术资料。

法院认定，小李虽未披露、使用或允许他人使用上述资料，未给公司造成实质性损害，但其行为属于《反不正当竞争法》规定的以电子侵入方式获取公司技术资料，构成以不正当手段获取商业秘密，应承担停止侵权、赔偿损失等民事责任。法官在释明中特别指出：作为签署保密协议的技术人员，即便已删除、未外传，仍不能免除相应责任。案件最终调解结案，小李当庭致歉并出具道歉信，承诺彻底删除所复制资料，原告正值上市之际，出于警示员工之目的放弃部分赔偿请求。

该案的价值在于揭示了“获取”与“使用”在侵权认定中的层次差异：披露、使用反映的是侵权的结果，而不正当获取本身即已构成侵权。本案中，实质性损害尚未发生，但法院仍可依据不正当获取行为认定侵权，从而及时制止侵权行为、保护权利人利益。权利人无需等待泄密结果发生即可主张权利，这直接改变了取证的时间窗口。

（二）私人终端与跨网络转发链的固定

李某健、罗某侵犯商业秘密罪案²提供了另一类样本。该案事实为：“海某项目”系某公司首款运动手表无线快充项目，李某健负责研发管理，罗某负责软件代码编写，二人先后转岗离开项目组。罗某利用系统权限漏洞，从公司内部远程登录其研发期间使用的工作电脑下载源代码，通过内部通讯软件发送给李某健；李某健为规避公司网络监管，将源代码压缩包改名为《报销.rar》发送至本人 126 网易邮箱，再转发至罗某 QQ 邮箱。罗某参考后因源代码无法移植至案外人芯片，未再披露使用。

该案裁判要旨明确：内部员工因参与特定技术项目组而在研发、测试过程中有限“掌握”商业秘密，转岗丧失获取权限后利用系统权限漏洞秘密下载的，属于“以盗窃、电子侵入等其他不正当手段”获取，系获取型犯罪而非违约型犯罪；尚未披露、使用或允许他人使用的，可根据合理许可使用费确定权利人损失数额。经鉴定，源代码包含的信息不为公众所知悉，且与罗某邮箱、笔记本电脑、U 盘中固定的《报销.rar》文件所含信息实质相同。据此，两名被告人均被以侵犯商业秘密罪判处有期徒刑并处罚金。

这一路径的证明价值在于：转发链的存在进一步确定了二人的共同犯罪事实。李某健、罗某分别任职于同一集团的下属公司与母公司，李某健为帮助他人解决技术问题，与罗某共谋，由罗

² 深圳市中级人民法院 2025 年度知识产权典型案例，2026 年 4 月 25 日发布；另入选广东省检察机关服务保障发展新质生产力典型案例，《广东省人民检察院公告》2025 年第 12 号。

某利用系统权限漏洞下载源代码，李某健接收后为规避公司网络监管，改名并外发至个人邮箱。法院据此认定二人系在均已丧失下载权限的情况下，共谋将源代码从公司内网外发用于帮助第三方研发，属于采取非法复制、未经授权或者超越授权使用计算机信息系统等方式窃取商业秘密，构成以盗窃等不正当手段获取权利人商业秘密的共同犯罪，而非各自的违约行为。本案提示：判断获取型犯罪与违约行为的界限，在于行为实施时行为人是否仍合法掌握商业秘密；已丧失权限仍实施获取的，即脱离违约而进入侵权乃至犯罪的规制范围。这一路径的证明价值在于：转发链的存在进一步确定了第二名被告的责任基础。罗某未经许可利用系统权限漏洞下载源代码，本身已构成以不正当手段获取商业秘密；李某健系权利人员工，与罗某构成共同侵权，落入第十条第一款第一项、第三项（以不正当手段获取、违反保密义务披露使用）规制范围。

（三）多源互证与专业工具辅助

夏某铭、李某等四人侵犯商业秘密案³展示了电子数据审查的工程化方向。检察机关在审查起诉阶段运用电子证据智能审查应用软件，快速筛查涉案电脑、手机、U 盘等设备中的电子数据；庭审中再次运用该软件，通过展示聊天记录、管理系统登录操作记录及 U 盘数据等方式，还原李某获取、披露涉案技术信息的过程。案件还从浙江省人民检察院与省市场监督管理局等多部门共建的知识产权技术调查官库中选取相关领域专家，从专利数据、学术文献、技术标准、互联网公开信息等多方面检索，就涉案技术信息的非公知性形成技术调查意见书。法院于 2025 年 12 月 29 日判处四人有期徒刑三年至二年不等，均适用缓刑，并处罚金，判决已生效。

该案中，技术调查官库的作用尤为关键：非公知性的判断专业性极强，检察机关自行检索难以支撑，引入跨部门专家资源并出具调查意见书，才使这一要件的证明达到可采信程度。

（四）毁证行为的证明效果需审慎评价

在张某等十四人侵犯商业秘密罪案⁴中，张某原系海某公司射频芯片开发部门负责人，离职后设立尊某公司并拉拢海某公司人员共同研发同类型芯片。在获悉海某公司准备提起侵权之诉后，张某指示他人删除服务器内涉嫌侵权数据、替换销毁服务器硬盘、安排员工签署所谓“承诺函”，

³ 嘉兴市秀洲区人民法院，2025 年 12 月 29 日判决；最高人民检察院知识产权检察办案技术支持典型案例，2026 年 9 月 2 日发布

⁴ 上海市第三中级人民法院（2024）沪 03 刑初 67 号，2025 年 7 月 28 日判决；最高人民法院 2025 年人民法院知识产权典型案例，2026 年 4 月 20 日发布。

以掩盖技术来源的非法性。法院认定，张某等人明知海某公司对商业秘密有严格的保密措施，作为外部人员无权接触，仍以明示或者暗示方式通过高额薪资待遇诱使海某公司内部员工以浏览、下载、摘抄、截屏等方式非法提供商业秘密，属于结伙通过不正当手段获取权利人商业秘密，情节特别严重，构成侵犯商业秘密罪。侦查机关委托资产评估公司评估涉案技术信息的合理许可使用费折现值为 3.17 亿余元，具有合理性，可以据此确定损失数额。法院判处张某有期徒刑六年，并处罚金；其余十三人判处有期徒刑六年至一年，并处罚金人民币三百万元至二十万元不等。判决已生效。该案入选最高人民法院 2025 年人民法院知识产权典型案例。

关于毁证行为的证明效果，需要作出准确的区分。该案的公开文本中，删除数据、替换硬盘、补签“承诺函”三项事实出现在基本案情部分，裁判结果部分并未就其作出独立的法律评价，法院未以举证妨碍为由作出不利推定。因此，实务中更为稳妥的做法是将此类行为的价值定位为间接证明，即毁证行为的事后性与针对性可以强化对被诉侵权人“自主研发”或“合法授权”主张真实性的怀疑，但不能独立替代举证妨碍的法定后果，也不能据此直接推定侵权成立。

五、制度衔接：证据互认的实践进展

2025 年，厦门市海沧区市场监督管理局与厦门市海沧区人民法院签署《海沧区商业秘密执法司法证据互认备忘录》，以“证据互认”为核心构建行政执法与民事司法的全链条衔接机制，明确了互认的标准、范围与程序，填补了福建省商业秘密执法司法证据互认的制度空白。技术层面，该机制借助第三方技术力量拓展现有商业秘密保护登记平台功能，融合电子数据存证、数字签名验证、时间戳及哈希算法等技术构建存证系统，企业将商业秘密源文件的 Hash 值存储至系统后，由平台实时自动生成存证证明；备忘录签署部门可依当事人申请委托司法鉴定机构对证据出具鉴定意见。

该备忘录属制度性文件而非个案裁判，但其指向的趋势具有现实意义：商业秘密案件的取证重心正在前移。既然获取行为本身即可能构成不正当手段、不以披露使用为要件，企业就应当在日常经营中即完成证据固定——权限日志、下载记录、远程控制痕迹、私人设备数据、版本迭代记录，均属平时无关紧要、涉诉时无从补造的材料。

结语

侵犯商业秘密的证明可归纳为三个层次。推定层面，形成“接触、实质性相同、合法来源不成

立"的判断结构，指导性案例 273 号将其展开为"人员流动异常、研发周期异常、技术信息实质性相同"三项叠加事实，并明确在部分信息已被证明相同且人员流动与研发周期双重异常时，可推定被告获取、使用了全部涉案技术秘密；其中"接触"指向获取行为是否导致权利人丧失对载体的有效控制，而非权限本身。时间层面，当技术信息难以直接比对时，第三方系统日志可证明权利人持续研发过程与信息形成时间，研发周期异常并不免除权利人对"接触"与"实质性相同"的初步举证，其作用在于作为否定合法来源抗辩的补强事实。数据层面，电子数据的审查重心是来源链条的可验证性；系统日志、远程控制痕迹、第三方上传记录与私人终端数据的证明力高于单次公证；毁证行为具备间接证明价值，但其法律效果有赖举证妨碍规则的配套，不宜径行作为侵权成立的依据。

结合本文所归纳的规则，权利人在取证与举证中可注意以下四点。其一，尽早固定接触与流转痕迹。离职前的权限交接、离职后的账号回收、工作终端与私人设备的清理，均可能造成证据灭失，权利人宜在员工离职环节即完成日志留存。其二，把“实质性相同”的比对前置到可比对阶段。技术信息一旦定型，比对成本与难度显著上升；对算法、模型类对象，应在争议萌芽时即完成版本固定。其三，注意区分接触与获取的正当性。拥有访问权限不能成为取得行为的免责事由，维权主张应指向手段与获取过程，而非仅指向权限状态。其四，对毁证行为及时固定痕迹。删除、替换、补签等行为既可能构成举证妨碍，其事后性与针对性本身亦可作为补强证据，宜第一时间完成公证或证据保全。

对权利人而言，需要区分两个问题：一是侵权行为发生时权利人往往并不知情，取证时点无从谈起；二是在发现侵权线索之后如何尽可能固定证据。后者仍宜尽早——尽管多数案件可以循系统日志、第三方平台记录等线索回溯，但回溯取证通常更困难，相应事实的证明力也更低。

说明：本文所引案例的裁判结果部分，仅摘取与侵权行为认定主题相关的内容。指导性案例 273 号裁判要点中关于停止侵害具体化与迟延履行金的两项，与侵权事实认定无直接关联，未予引用。文中法条编号统一采用 2025 年修订后条文，涉及旧法的案例已在文中标注。