

合法接触者以不正当手段获取商业秘密的刑事认定

文/周晓聪

【裁判要旨】 行为人任职期间具有接触商业秘密的权限，但其违反明确约定的保密要求，通过绕开权利人监管手段和技术限制措施，采取非法拍摄、私自转存等权利人不知情的隐蔽手段将商业秘密置于个人完全控制之下，该行为已超出授权接触范围，应当认定为以不正当手段获取权利人的商业秘密。不正当手段获取型侵犯商业秘密犯罪不以实际披露、使用或者造成重大损失为必要，只要行为人通过不正当手段实际取得了商业秘密，使其脱离权利人的管控范围，即构成犯罪既遂。未实际产生商业秘密许可费用的，可通过评估涉案商业秘密虚拟许可使用费予以认定损害后果。

□案号 一审：(2025)粤0304刑初375号

【案情】

公诉机关：广东省深圳市福田区人民检察院。

被告人：谢某。

2022年9月，被告人谢某与被害单位深圳某技术公司签订员工聘用协议书，任技术经理岗位。在签订聘用协议书之外，被告人谢某签署了信息安全承诺书，承诺书内容包括“不私自将打印的公司保密信息纸件带出公司、不私自拍摄、录音、录像公司保密信息、不通过U口/网线/WIFI等各种方式拷贝公司保密信息到任何私人介质、不私自以任何方式将公司保密信息保存到私人设备或向外部传递”。

该公司还采取了禁止员工上班期间携带私人U盘及有拍照功能的电子设备进入办公区域、同时对公司配发的办公笔记本电脑设置限制网络、复制、拷贝、传输功能等保密措施。自2023年上半年起，被告人谢某在其正常工作时间段内，利用公司办公局域网，将其具有查阅权限的公司技术信息等文件从公司保密系统下载到该办公笔记本电脑，并通过新建文档等方式去除母版文件的水印、避开文件涉密字样、公司logo等予以保存。其后将该办公笔记本电脑携带回家，在家中多次使用其私人手机对电脑中存储的上述文件进行拍照，随后将拍摄的上述文件照片通过连接私人笔记本电脑分类传输至其私人U盘中予以存储。后

经公司检查发现该U盘内存储了包含公司相关培训资料、技术信息介绍等文件照片数千张，其中包括了记载该公司涉案两项技术信息的多张照片。

经广东某司法鉴定所鉴定，深圳某技术公司主张的涉案两项技术信息属于不为公众所知悉的技术信息。从被告人谢某私人U盘内提取固定的涉案信息照片与深圳某技术公司所主张的两项技术信息具有同一性。经评估，两项涉案技术信息商业秘密的虚拟许可使用费评估值共计1300万元。

2024年8月16日，被告人谢某经公司电话通知在会议室等候民警出警归案。2025年4月，被告人谢某与被害单位深圳市某技术公司签订了谅解协议并取得深圳市某技术公司出具的

谅解书。

【审判】

深圳市福田区人民法院经审理认为：商业秘密是指不为公众所知悉，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。关于秘密性即非公知性，涉案两项技术信息是深圳某技术公司在经营过程中开发形成、实验研究的成果，并未对外披露。广东某知识产权司法鉴定所出具的鉴定意见书认定，该两项技术信息是不为公众所知悉的技术信息。关于保密性，在案证据证实，深圳某技术公司制定了规章制度，明确规定未经批准，员工不得私自拍摄、录音、录像公司保密信息，不得私自以任何方式将公司保密信息保存到私人设备或向外部传输等。该公司给员工配备的办公笔记本电脑，设置了限制复制、拷贝、传输文件等功能，同时只能在办公区域网络环境中下载公司系统内文件。公司还采取了限制员工携带U盘、可拍摄电子设备等进入办公区域等措施。上述事实、证据足以证实深圳市某技术公司对包含本案技术信息在内的公司涉密文件采取了必要保密措施。关于价值性，本案中，深圳市某评估公司接受公安机关委托后，成立评估小组对被评估单位实施了现场调查，根据被评估单位提供的研发材料费、研发人员工资薪酬等成本明细，对涉案两个技术密点的许可使用费进行评估，作出本案两项技术密点的许可使用费评估值为1300万元的资产评估报告，评估主体资质有效，评估程序科学合法。

综上，涉案两项技术信息属于商业秘密保护的客体，具有商业价值，不为所属领域的相关人员普遍知悉也不容易获得，且经权利人采取了相应的保密措施，符合商业秘密的构成要件，理应受到法律的保护。

本案中，被告人谢某作为深圳某技术公司的技术经理，虽然在任职期间内因其工作职权，可在一定范围和程度内知悉、接触涉案商业秘密。但是在其入职时明确约定了保密义务，要求不得泄露公司商业秘密，不得私自拍摄、录音、录像公司保密信息，不私自以任何方式将公司保密信息保存到私人设备或向外部传递等。被告人谢某亦签署了信息安全承诺书，明知上述保密规定。在此情况下，被告人谢某仍然违反公司的保密要求和保密管理规定，在公司不知情的情况下避开公司的各种监管手段，将含有涉案技术秘密的文件，通过偷拍并去除相关保密标识的方式转存储至私人U盘。被告人采取的绕开安全监控的偷拍行为，证明其不愿意被权利人知悉其获取涉案文件的事实，符合盗窃行为中秘密隐蔽手段的特征，破坏了商业秘密未经许可不得被持有的状态、侵犯了权利人对于商业秘密的处分权利。且被告人多次、大批量的偷拍转存行为，明显超出了正常、合理使用涉案技术秘密的界限，在客观上也致使涉案技术秘密脱离了权利人的原有管控范围，在权利人不知情的情况下将涉案商业秘密信息置于自己完全管理控制之下，具有不法占有的目的，使涉案技术秘密存在可能被披露和使用的风险。该行为符合最高人民法院、最高人民检察院《关于办理侵

犯知识产权刑事案件适用法律若干问题的解释》（以下简称《知识产权刑事案件解释》）第16条规定“采取非法复制等方式，获取商业秘密的，应认定为刑法第二百一十九条第一款第（一）项规定的盗窃”的行为，故被告人谢某的行为构成侵犯商业秘密罪。鉴于被告人谢某构成自首，且取得被害单位的谅解，依法应减轻处罚。福田区法院于2025年9月25日作出判决：一、被告人谢某犯侵犯商业秘密罪，判处有期徒刑1年2个月，并处罚金5万元；二、扣押在案的涉案U盘、手机、笔记本电脑等依法予以没收，交由公安机关销毁，扣押的1部平板电脑、手机由公安机关予以退还。

一审宣判后，没有上诉、抗诉，判决已发生法律效力。

【评析】

在知识经济时代，商业秘密作为企业核心竞争力的重要载体，凝结着企业宝贵的知识产权和创新成果，保护企业商业秘密就是保护创新火种，对维护产业链安全、发展新质生产力具有重要作用。实践中企业员工基于工作职责合法接触商业秘密后违反保密规定，通过规避监管措施私自复制、偷拍等手段获取商业秘密的行为日益增多。但在目前司法审判实务中，对于已经知悉或有权接触商业秘密的内部人员，其实施的获取商业秘密行为在何种条件下可以认定为刑法规定的“不正当手段获取”，从而认定构成侵犯商业秘密罪仍存在一定的争议。本案围绕这一核心与难点问

案例

题,探讨从行为性质、主观要素等标准进行综合判断,认为有权接触案涉商业秘密的主体,并不代表其获取商业秘密的方式必然具有正当性。应综合考察其获取商业秘密的行为方式是否违背了权利人的真实意志和保密安排、其主观是否具有不法占有等非法目的、以及是否导致权利人失去对该商业秘密的有效控制等因素审慎确定。

一、不正当获取行为的核心内涵在于商业秘密控制状态的非法变更

不正当获取型侵犯商业秘密罪中,需要厘清“不正当获取”的行为概念,从而明确其规制的行为内涵。虽然刑法及相关法律并未将“获取”直接表述“取得”,但从条文列举“贿赂、欺诈、电子侵入”以及兜底项“其他不正当手段”可知,均是指行为人出于不当目的实施了不正当手段将权利人商业秘密置于自己控制之下,改变了商业秘密的占有状态。因此,刑法所规定的“获取”不应狭义地理解为从“未知”到“已知”的信息接收过程,对于内部人员而言,其核心在于非法改变商业秘密的控制状态,其“获取”行为更体现为对商业秘密控制状态的非法改变。当行为人通过隐蔽手段,使商业秘密脱离权利人的既定管控环境(如受监控的公司设备、内部网络),并将其置于个人可随时支配、使用或泄露的私人领域时,就完成了一次刑法意义上“获取”行为。如本案中被告人的辩护意见核心逻辑就在于“授权接触即阻却行为违法”,即认为谢某某作为技术经理,其职务行为已使其合法接触并知悉相关商业秘密,后续的翻

拍、存储行为仅是持有形式的变更,不构成新的获取行为。然而,商业秘密的合法接触本质上是企业基于经营管理需要,对员工赋予的职务范围内信息获取权,具有职务关联性和权限法定性,即该接触行为与其职责范围直接相关,且仅有权在其职务范围内了解商业秘密内容,并不等同于有权无限制保存、持有该商业秘密。所以,员工的合法接触权具有明确的前提与边界,概括而言即范围边界。接触权限应限于履行职务必需的最小范围;用途边界,合法接触的目的仅限于完成工作任务,不得用于个人私利或其他非法目的;管理边界,合法接触主体必须遵守权利人的保密制度管理,不得违反权利人关于商业秘密存储、传输、复制等限制性规定。以上边界界限由保密协议、公司规章制度等共同划定,它授予员工在特定时间、特定地点、为特定目的使用商业秘密的权限。当合法接触者突破上述边界,以非法方式获取商业秘密并脱离权利人控制的,其行为即可能由合法接触转变为不正当获取。因此,有权接触案涉商业秘密,并不代表其接触、获取商业秘密的方式以及获取后对技术秘密实施的处置行为必然具有正当性。本案中,被告人谢某将秘密信息从公司受控电脑转移至私人U盘,正是实现了对商业秘密控制权的非法转移。

二、不正当手段的实质判定在于违背权利人意志与保密安排

不正当手段的判断关键,不在于行为人是否曾有权接触,而在于其获取信息的具体方式是否违背了权利人的真实意志和保密安排。本案被告人

谢某在其入职时明确约定了保密义务,明知不得私自拍摄、录音、录像公司保密信息、不私自以任何方式将公司保密信息保存到私人设备或向外部传递等,且公司另采取了禁止员工携带U盘、可拍摄电子设备进入办公区域,限制办公电脑的下载、复制、传输功能等措施。在此情况下,被告人谢某仍然违反公司的保密要求和保密管理规定,在公司不知情的情况下避开公司的各种监管手段,将含有涉案技术秘密的文件,通过偷拍并去除相关保密标识的方式转存储至私人U盘。被告人采取绕开安全监控的偷拍行为,证明其不愿意被权利人知悉其获取涉案文件的事实。其采取的“去除水印”“避开涉密字样”“在家中私人设备拍照”等一系列行为目的明确,即规避公司为防范信息失控而设置的技术与制度屏障,将涉案商业秘密非法转移至自己控制保管之下。这种行为方式的秘密性与欺骗性,充分体现了其手段的“不正当”本质,与“盗窃”行为的秘密窃取特征相吻合。该行为符合《知识产权刑事案件解释》第16条规定“采取非法复制等方式,获取商业秘密的,应认定为刑法第二百一十九条第一款第一项规定的盗窃”的行为。

三、主观故意的推定需要结合行为方式与控制意图综合判断

侵犯商业秘密罪中,行为人的主观故意和目的至关重要。特别是对于不正当获取型商业秘密犯罪案件中,由于行为人尚未实施非法披露或非法使用商业秘密的行为,对于其主观违法意图的辩解,需要结合其行为目的、获取方式及是否(下转第107页)

(上接第041页)导致权利人失去对商业秘密的有效控制等因素判断。即对于内部人员的不正当获取行为,其主观状态的认定不能仅凭其是否已实际披露或使用判定,而应判断其是否具有非法占有的目的,使涉案商业秘密存在可能被披露和使用的风险。此处的“非法占有”并非仅指物理上的占有,而是指排他性控制与处置信息载体的意图。行为人通过非法复制、转存,意图在权利人不知情的情况下,建立自己对商业秘密的独立控制力,这种意图本身使商业秘密脱离了权利人设置的安全边界,处于随时可能被利用或扩散的危险境地。此外,从客观行为即被告人的获取方式上面

推定,谢某多次数、大批量的转存行为,以及其刻意规避监管的手段,可以推出其主观上并非为了正常工作需要,而是意图长期、独立地控制这些商业秘密。

四、不正当获取型侵犯商业秘密的行为后果可以虚拟许可使用费作为损失依据

对于不正当获取型商业秘密犯罪,行为人虽已获取商业秘密,但由于意志之外的原因尚未披露使用。如果仅以行为人未使用或者未获利而认为未造成危害后果,忽视了商业秘密的特点,不利于对权利人权益的保护,不利于遏制此类违法行为,也会导致对商业秘密的非法获取人违法行为的放

纵。在某种意义上,商业秘密被非法获取本身即导致其保密性受损,无论其后续披露、使用与否,均造成权利人的商业秘密价值减损,产生被披露、使用的现实风险,具有刑法所要求的现实危害性。《知识产权刑事案件解释》第18条规定:“以不正当手段获取权利人的商业秘密,尚未披露、使用或者允许他人使用的,损失数额可以根据该项商业秘密的合理许可使用费确定。”因此,对于非法获取型侵犯商业秘密罪中,未实际产生许可费用的,可以通过评估涉案商业秘密虚拟许可使用费予以认定其情节严重的后果。

(作者单位:广东省深圳市福田区人民法院)