私募证券基金合规运营(量化管理人篇)

商业秘密视角下的量化私募基金合规：从被动防御到主动治理

作者：陶燕 | 陈雅秋 | 孙博宇

量化私募基金已成为资本市场的重要力量，交易策略是其核心竞争力，直接关系到机构能否持续盈利。然而，交易策略作为智力成果，天然具有流动性和可复制性。随着研发人员频繁流动，策略不可避免地面临着泄露风险，由此引发的争端也屡见不鲜。

2024 年，全球最大做市商之一 Jane Street 与知名对冲基金 Millennium，曾因商业秘密争议对簿公堂。Jane Street 主张，其前员工离职时带走了一项公司认为据称为其带来约 10 亿美元利润的期权交易策略，并在加入 Millennium 后使用该策略，该案历经八个月后以双方和解结案。[1]无独有偶，中国量化私募圈同样上演类似剧情: 2023 年，上海锐天投资以侵害技术秘密为由，起诉杨某、宁波幻方量化及其关联科技公司等主体，引发市场广泛关注。[2]尽管该案商业秘密侵权的实体审理尚无细节披露，但据同事件引发的竞业限制争议判决来看，该事件同样反映出量化机构在人员流动过程中面临的策略保护风险。[3]

从 Jane Street 到锐天投资，上述案例表明: 单靠诉讼的被动“事后维权”模式，难以从根本上守护量化私募的核心资产，商业秘密侵权案件普遍面临举证难度大、审理周期长、损失认定复杂以及维权成本高昂等困境。正因如此，量化私募的商业秘密保护，正在经历从被动应对向主动“事先筑墙”的治理转型。这种转型既是行业发展的内在需求，也与当前立法层面对商业秘密保护体系的系统性建构形成呼应。

随着行业规模持续扩张、人才竞争日趋白热化，可以预见，此类商业秘密争议将逐步增加。本文将从商业秘密对量化私募的战略价值切入，结合《商业秘密保护规定》的最新制度设计，梳理保密措施的实操要点，并辅以司法实践案例，以期为量化行业合规提供一条从被动防御走向主动治理的路径参考。

[1] 参考: https://news.bloomberglaw.com/ip-law/jane-street-millennium-settle-india-options-trade-secrets-case
[2] 参考: https://m.thepaper.cn/newsDetail_forward_22107964
[3] 参见: 上海市第一中级人民法院: (2022)沪 01 民终 9691 号。

一. 量化私募基金“核心资产”的保护路径选择

量化交易的核心竞争力，根植于数学模型、统计算法与底层源代码的深度融合。与传统主观资管不同，量化领域的策略呈现出鲜明的“轻资产而高价值”的特征。一方面，竞争对手一旦获取相应策略代码，便可以较低成本快速复现，复制门槛极低；另一方面，泄密的损害后果远不止于市场份额的挤占或盈利减损，更致命的风险在于策略趋同将导致交易行为同质化，进而加速策略失效，甚至导致其彻底失效，由此产生的损失可能难以估量。

然而，梳理当前法律体系下量化策略所能寻求的各类保护路径，不难发现每种方式皆有其固定局限：

保护方式	规制困境
专利权	单纯的"智力活动的规则和方法"不属于《专利法》的授权客体。即使涉及"技术实现方案"可申请专利，专利制度"以公开换垄断"的逻辑，也与量化策略需保密的特点存在根本冲突。
著作权	《计算机软件保护条例》明确，软件著作权保护计算机程序(代码指令)及其文档，但不延及开发所用“思想、处理过程、操作方法”。而量化策略的核心商业价值恰在于其算法思想与因子配置的方法论，而非代码本身。
商业秘密	客体：数据、算法、计算机程序、代码等信息被明确纳入保护范畴； 特性：无需公开、无保护期限限制、《反不正当竞争法》保护力度较强;在现有知识产权保护体系下，“商业秘密”通常是量化机构保护未开工策略信息的重要路径。

依据《反不正当竞争法》第九条，量化策略欲获得商业秘密保护，须同时满足三项法定要件：一是“不为公众所知悉”(秘密性)，二是“具有商业价值”(价值性)，三是“权利人采取相应保密措施”(保密性)。

就秘密性要件而言，量化机构通常对核心策略实施严格的物理隔离与管控。价值性方面，策略代码直接关系到机构的套利效率与收益能力，其商业价值不言自明。三项要件中，保密性的判断最为关键，也最具操作难度——其核心在于权利人需要采取与信息性质、价值相匹配的合理措施。这不仅是法定的形式门槛，更是量化机构构建合规体系的内在起点。下文将围绕如何将保密义务在事前主动嵌入研发、运维及人员管理的全周期展开分析。

二. 《商业秘密保护规定》新规解读：主动治理的制度锚点

2026 年 2 月 24 日，国家市场监督管理总局发布第 126 号令《商业秘密保护规定》(以下简称“《保护规定》”)，自 2026 年 6 月 1 日起施行。该部门规章的出台，标志着我国商业秘密行政保护进入专门化、系统化的新阶段。

在此之前，除最高人民法院《关于审理侵犯商业秘密民事案件适用法律若干问题的规定》(以下简称“《商业秘密司法解释》”)为司法裁判提供规则指引外，商业秘密的行政保护长期依赖 1995 年原国家工商行政管理局公布、经 1998 年修改的《关于禁止侵犯商业秘密行为的若干规定》(以下简称“旧规”)。

然而，旧规全文仅 12 条，制度框架相对粗放且实施性亦显不足，已难以回应当下数字经济时代中商业秘密保护面临的新形势与挑战。尤其就量化私募等行业场景而言，算法、代码、策略等新型商业秘密形态不断涌现，旧规在秘密性认定标准、保密措施要求以及侵权行为的认定规则等方面均存在规则模糊与制度缺位，致使权利人在寻求行政救济时面临诸多现实障碍。

鉴于此，《保护规定》在吸收《商业秘密司法解释》相关内容的基础上，对商业秘密的界定、保密措施要求、侵权场景认定、行政保护手段及法律责任等进行了体系化重构。立足于量化私募行业的实践场景，《保护规定》在下述三个方面的调整为商业秘密保护提供了更为清晰的规范指引：

(一) 商业秘密客体界定精细化

《保护规定》以清单列举的方式，对可纳入商业秘密保护的客体类型进行了更加全面系统的数字化扩充。其第五条第二款明确规定："与技术有关的结构、原料、配方、材料、样品、样式、工艺、方法、数据、算法、计算机程序、代码等信息，属于第一款所称的技术信息。" 相较《商业秘密司法解释》第一条所列举的技术信息类型，《保护规定》进一步将"代码"与数据、算法、计算机程序并列列入技术信息范围，强化了对数字化技术成果的保护。

这一范围扩张有效地回应了实践中长期存在的争议，尤其对量化机构等此类从事算法开发的科技企业具有现实意义。具体而言，例如：**以源代码形式呈现的核心交易策略、以数据或数据库形式存储的 Alpha 因子库、各类算法模型及参数配置等，均可以在上述列举范围内找到对应的"商业秘密"依据**。对于此类核心数字资产，在难以满足专利授权要求或不宜对外公开披露的情况下，商业秘密路径往往是现实中最为可行的法律保护方式。

此外，《保护规定》第五条第三款将"与经营活动有关的创意、管理、销售、财务、计划、样本、客户信息、数据等信息"纳入经营信息的保护范畴，这同样为量化机构的另一大重要资产——例如**投资者名单等**——提供了规范依据。上述规定使得商业秘密的客体认定标准更加精细，也为行政执法与司法裁判提供了可操作的统一标尺。

(二) 商业秘密保护措施现代化

《保护规定》延续《商业秘密司法解释》以列举方式界定合理保密措施的规制思路，并进一步体现出标准与时俱进的特征。其第九条第一款明确了权利人采取保密措施的基本标准，即"权利人为防止商业秘密泄露，采取与商业秘密及其载体的性质、商业秘密的商业价值等因素相适应的合理保密措施。"该定义实质上对量化机构等科技企业的商业秘密管理实践提出了更为严格的规范化要求：即保密措施的强度须与受保护客体的内在属性和经济价值相匹配。否则在争议审理中，可能因保密措施"不适应"而被认定不满足商业秘密的法定构成要件，进而直接导致丧失获得商业秘密保护的基础。

在具体实施层面，第九条第二款沿袭现有的保密措施类型(例如签订保密协议、限定接触范围、对涉密场所采取物理隔离等)外，还新增设了契合数字时代运营特性的规定：明确要求"针对远

程办公、跨境协作等场景，采取权限分级、数据脱敏、操作日志留痕等技术保密措施”。上述补充内容对量化私募行业尤为具有现实意义。一方面，**该类量化机构的研发活动可能确实涉及多地协同作业、跨境数据传输以及远程代码迭代等工作场景，以物理隔离和纸质协议为核心的防护手段已难以有效覆盖潜在的泄露风险**。另一方面，《保护规定》既为量化机构提供了可参照落地的操作指引，也意味着监管部门在未来审查保密措施时将更加趋向实质化——不仅要有相关制度和协议等约束文件，更需要在技术层面落实执行，方能在纠纷发生时充分举证机构自身已尽到合理保密义务。

同时，该条规定的“对能够接触、获取商业秘密的计算机设备、网络设备、存储设备等，采取禁止或者限制使用、访问、存储、复制等措施”，同样强化了数字化环境下对涉密信息载体的管控要求。此款规定在《商业秘密司法解释》中可以找到相同的规制要求，旨在打通行政保护与司法救济之间的衔接通道。这种部门规章的“重申”，同样在强调保护着力点从事后维权逐步前移至事前预防，最终促使市场形成以企业自主防护为基础的商业秘密保护格局。

(三) 商业秘密侵权行为场景化

《保护规定》对《反不正当竞争法》所规制的“不正当手段”获取商业秘密作出了迄今最为具体的界定，其中对网络环境下新型侵权场景的考虑尤为突出。

首先，第十条第二款第(三)项中明确将“未经授权或者超出授权范围，擅自进入权利人的数字化办公系统、服务器、邮箱、云盘、应用账户等，或者通过设置恶意程序、漏洞攻击等技术手段获取商业秘密”列为不正当手段之一。**这一规定之所以关键，在于它精准回应了多数量化机构及科技企业面临的现实困境，即相较于传统物理意义上的“盗窃、贿赂、欺诈、胁迫”，电子侵入才是这类企业商业秘密更常遭遇的实质威胁，也有助于明确数字环境下获取行为的认定边界，为权利人举证提供更加明确的依据**。同时，该条款的覆盖范围兼具外部性与内部性：既包括了外部黑客攻击等技术入侵，也涵盖内部员工虽有授权但实施越权访问的情形，从而为数字环境下的商业秘密保护提供了更周延的规范基础。

其次，第十条第二款第(四)项同样值得关注。“未经授权、超出授权范围或者授权期限届满后，擅自将商业秘密下载或传输至不受权利人控制的电子邮箱、云盘等网络存储空间或者电子设备”，亦构成不正当手段获取。从该认定逻辑来看，侵权行为成立的判断基准在于保密信息是否已脱离权利人的有效管控的范围，即单纯的转移行为已足以构成侵权，无须进一步证明该信息后续是否被实际使用或对外披露等。**对量化机构来说，这一条款直指实践中最为高发的风险场景：员工往往在离职前将工作系统中的文件批量下载至个人设备。依此规定，该行为可能构成以不正当手段获取商业秘密的风险行为，而无需等待后续披露或使用行为发生。**

此外，第十三条对教唆、引诱、帮助他人侵权的行为作出专门规定。具体包括以明示或暗示方式怂恿、指使他人实施侵权，通过物质奖励或职位许诺等非物质奖励诱导他人侵权，以及明知或应知他人侵权仍提供资金、技术、设备等便利条件。上述规定有助于明确竞争主体通过第三方、

员工等间接获取商业秘密时的责任边界。这一规定一方面有助于遏制同业竞争中通过迂回手段获取对手核心策略信息的行为；另一方面对量化机构在人才引入环节也提出了更高要求：在招聘人员时，即使未直接参与或授意侵权，若该员工携带前雇主的保密信息入职并加以使用，量化机构仍可能因“明知或应知”的认定标准而面临连带追责风险。

三. 量化私募基金的保密措施实践：主动治理的具体落实

基于《保护规定》对商业秘密保护措施提出的新要求，我们建议量化机构宜从“人员管理”和“技术管理”两个维度同步将保护体系落到实处，具体可以从以下几方面把握：

(一) 日常运营层：涉密人员约束与制度建设

以(2022)沪 73 知民初 997 号为例，J 公司在与员工 L 某侵害技术秘密纠纷案中提交了主张保护其商业秘密的系列文件，主要包括：(1)约定有保密义务及知识产权归属条款的《劳动合同》及《补充协议》；(2)L 某签署的《入职承诺书》，其中承诺不将第三方商业秘密带入公司且在职期间及离职后均不使用相关保密信息；(3)《员工保密及竞业禁止协议》，对保密信息的范围、归还义务及违反后果作出了明确约定；(4)J 公司的《信息安全管理制度》及《配置管理过程》，对涉密信息范围、源代码管理及离职交接要求作出了制度性规定；(5)L 某签字的《规章制度签收确认书》，确认其已阅读并知悉上述规章制度并自愿遵守。法院最终认定 J 公司在劳动合同和公司政策中已经体现要求员工保守商业秘密的意愿，并采取一定防范措施，应判定已采取合理的保密措施。

可见，人员管理始终是商业秘密保护的“第一道防线”。实践中，量化机构大多数策略泄露事件并非源于外部电子入侵，而多发于内部员工在离职前夕带走代码，或是在职人员越权窃取核心信息。因此，尽管人员管理和相关制度建设不属于技术层面的实质性防护手段，但这类事前以书面形式固定下来的书面保密约定，同样是量化机构在商业秘密纠纷中主张自身已采取合理保密措施的有力佐证之一。以下三项措施是人员管理中最基础也最为必要的制度安排：

1. 签署保密协议

量化机构应与直接从事策略代码开发、负责算法模型运营的涉密员工，以及虽不直接参与但基于岗位职责能够获取或接触上述内容的相关员工签订单独的保密协议，或选择在劳动合同中约定相应保密义务。在此类约定中，应详述保密内容范围、保密期限、接触权限，并在协议中确认泄密损失计算方法及违约责任等。

2. 保密培训与制度建设

《劳动法》及《劳动合同法》均赋予企业依法建立和完善劳动规章制度的权利，员工亦负有依据规章制度履行保密义务的相应责任。员工在职期间，量化机构可通过定期组织商业秘密培训、制定并落实相关规章制度等方式，向员工明确提出不时更新的保密要求。

3. 签署竞业限制协议

实践中，量化机构通常在员工入职时即要求签署包括保密协议和竞业限制协议在内的一系列文件，但两者在性质和适用上存在一定差异：竞业限制只限于高级管理人员、高级技术人员和其他负有保密义务的人员，且最长不得超过两年。而保密义务的约束范围相较宽泛，期限也可为无限期。应当理解，竞业限制本质上是通过支付经济补偿平衡核心员工在一定期限内的择业自由与企业商业秘密保护需求，以此防范掌握核心商业秘密的员工离职后短期内加入竞争对手。事实上，竞业限制不能代替保密义务的一般性约束，机构在约定竞业限制时也需注意诸多法定要求。

(二) 技术管理层：核心代码与数据的隔离及保护

结合前述《保护规定》对“相应保密措施”的扩充列举，应当理解与商业秘密及其载体的性质、商业秘密的价值等相适应的合理措施不应止于人员管理层面，还需要采取必要的技术手段予以保护，最高院在过往的裁判案例中亦表明此观点：

(2012)民监字第 253 号中，最高人民法院认为“合同的附随义务与商业秘密的权利人对具有秘密性的信息采取保密措施是两个不同的概念，不能以 G 公司负有合同法上的保密附随义务来判定 H 公司对其主张的信息采取了保密措施…作为商业秘密保护的信息，权利人必须有将该信息作为秘密进行保护的主观意识，而且还应当实施了客观的保密措施。”此外，最高人民法院在(2016)最高法民申 2161 号中再次重申：“J 公司除在与员工所签劳动合同中规定有保密条款外，并未就其所主张技术信息和经营信息采取了其他保密措施提供证据。由于涉案劳动合同中的保密条款仅为原则性规定，不足以构成对特定技术信息或经营信息进行保密的合理措施。从这个角度讲，其关于前述信息构成商业秘密的主张，亦不能成立。”因此，量化机构可以考虑采取以下技术手段对商业秘密予以保护：

1. 信息分级与分类管理

量化机构应考虑对核心算法、交易策略、模型参数及相关数据实施分级分类管理，建议可划分为“核心级、重要级、一般级”等不同等级，并针对各“密级”分别制定相应的存储方式、访问权限及使用规范。

2. 全流程日志留痕与访问核查

量化机构可考虑建立完善的访问日志与核查机制，对代码及数据的读取、修改、导出等操作实行全量记录，确保每项操作行为可追溯、可复核。日志应具备防篡改功能并接受定期核查，以便及时识别异常访问与潜在泄密风险。

3. 最小权限与动态授权机制

建议落实最小权限原则，根据岗位职责和业务需要精准划定访问权限，实现机构内部“按需授权”。同时，建议引入动态授权或临时授权机制(如限时访问、审批后授权等)，避免高权限账户被长期持有，降低核心数据暴露风险。

4. 其他技术防护措施

参考《保护规定》对保密措施的相关要求，量化机构可结合自身系统架构与业务特性，构建多层次技术防护体系。可采取的技术手段有以下供参考:

网络隔离	将核心代码与敏感数据等部署于内网环境，与互联网实施物理隔离或通过严格的边界控制进行访问隔离。
主机安全控制	服务器可以拆除无线通信模块，禁用 USB 接口及未经授权的外设接入，消除物理层面的非授权数据导出通道。
数据加密机制	对核心代码、模型文件及数据实施自动加密存储，并建议采用集中式密钥管理系统进行统一的密钥管理。
身份认证与访问控制	采用令牌、密码等多因素身份认证机制，并结合堡垒机或跳板机实现统一入口管控及操作行为审计。
代码版本控制	对策略代码实施版本管理，权限分离控制提交与合并，所有改动留痕可追溯，防止未经授权的代码修改或导出。
数据流转管控	建立严格的数据导入导出流程，通过专用中转设备进行病毒查杀、内容检测、格式校验和审批控制，并使用受控介质进行传输。
外网访问管理	严格控制外网对内网的访问权限，如确因业务需要接入内网，须经由 VPN 或跳板机等实现受控访问。
数据脱敏机制	在测试、开发或对外合作等场景中，应使用脱敏数据或模拟数据，避免直接暴露真实策略细节。
数据水印与溯源	对关键数据和文档嵌入隐形水印，便于泄露事件发生后实现溯源定责。
权限定期复核	定期对员工权限进行复核，及时清理冗余权限或回收离职人员权限。
灾备与备份加密	在保障数据安全的同时，应建立数据加密备份与灾难恢复机制，防止因系统故障或意外事件导致数据丢失。

结语

模型、算法、交易策略与底层源代码等，不仅是量化机构核心技术壁垒的载体，更是其生存与发展的根本。这些数字资产具有一经泄露即难以挽回的特性，若单纯寄望于事后诉讼救济，往往面临难以发觉、举证困

难、赔偿有限等问题，无法弥补竞争优势丧失所造成的损失。《商业秘密保护规定》的发布与正式实施，释放了明确的监管信号：商业秘密保护的重心正在从外部合规约束转向企业内部驱动，从被动的事后追责转向主动的事前防控。新规不仅为行政执法细化了更具操作性的标准，更重要的是，它倒逼企业将保密义务嵌入研发、人员管理及日常运营的各个环节，合规成为管理层必须落实的前置要求。

对量化私募行业而言，主动治理绝非为满足监管要求的合规成本，而是构筑核心竞争力的战略抉择。如果对商业秘密保密措施流于形式、心存侥幸，无异于将多年积累的研究成果置于险地。规则的完善提供了外部准绳，但真正的屏障，始终在于量化机构能否将商业秘密视为与投研能力同等重要的战略资源。

如您希望就相关问题进一步交流，请联系：

陶 燕
+86 21 3135 8755
yan.tao@llinkslaw.com

陈雅秋
+86 21 3135 8744
jane.chen@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野