

企业商业秘密保护中电子证据的管理与运用（上篇）

作者：贾媛媛 籍婷、王聪睿子

引言

近年来，随着技术创新的迅速发展和科技人才的快速流动，由此引发的商业秘密纠纷与日俱增。在以判决方式审结的商业秘密侵权案件中，原告败诉的比例相对较高，主要原因在于权利人举证不充分^[1]。在商业秘密案件中，原告要对商业秘密范围、商业秘密权属、商业秘密的秘密性、保密性、价值性以及对方侵权行为进行举证，举证责任较重。随着信息化与电子办公的发展与普及，越来越多的技术资料、研发记录、交易凭证等都以电子数据的形式存在，这使得商业秘密保护和管理的难度更大，侵权行为更具隐蔽性与复杂性，权利人的维权之路更加艰难。因此，企业需要进一步加强商业秘密保护意识，在日常经营中对相关电子数据进行妥善管理，以便在诉讼中能够完成相应的举证责任。

本文将结合商业秘密保护的实务经验，探讨企业如何在日常经营中对电子数据进行管理，以及如何在诉讼过程中准备电子证据，以期帮助企业构建商业秘密保护体系并有效维护自己的合法权益。

一、电子证据概述

在信息化时代，尤其是在商业秘密案件等侵权行为较为隐蔽的案件中，电子证据往往成为决定案件事实认定的关键证据，常见的电子证据包括以下几类：

- 网页、博客、微博等网络平台发布的信息；
- 手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；
- 用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；
- 文档、图片、音频、视频、数字证书、计算机程序等电子文件；
- 其他以数字化形式存储、处理、传输的能够证明案件事实的信息^[2]。

上述电子证据普遍具有易复制性、易篡改性和介质依赖性，其易被修改、删除或损坏，故法院对电子证据的审查提出了更为具体和严格的要求，一般会结合下列因素进行综合判断^[3]：

- 电子数据的生成、存储、传输所依赖的计算机系统的硬件、软件环境是否完整、可靠；

- 电子数据的生成、存储、传输所依赖的计算机系统的硬件、软件环境是否处于正常运行状态，或者不处于正常运行状态时对电子数据的生成、存储、传输是否有影响；
- 电子数据的生成、存储、传输所依赖的计算机系统的硬件、软件环境是否具备有效的防止出错的监测、核查手段；
- 电子数据是否被完整地保存、传输、提取，保存、传输、提取的方法是否可靠；
- 电子数据是否在正常的往来活动中形成和存储；
- 保存、传输、提取电子数据的主体是否适当；
- 影响电子数据完整性和可靠性的其他因素。

结合商业秘密诉讼实务，上述电子数据可能被用以证明商业秘密范围、权属、保密措施、侵权行为等多个要件。其中，证明商业秘密范围、权属、保密措施的证据通常是在企业日常经营过程中产生的，例如流程图、设计图、立项报告、研发记录、测试报告、项目验收报告、计算机软件程序等（以下称“**内部证据**”），企业在其内部对上述材料进行收集和整理具有正当性，较容易满足“合法性”要求。因此，对于内部证据的管理和收集，主要关注如何满足“真实性”的要求。另外，证明侵权行为或获利等要件时，权利人需要证明侵权人非法获取、披露、使用或允许他人使用等侵权行为，例如在侵权人的办公场所或者其他公共场所，对侵权人进行拍照或录音（以下称“**外部证据**”），这些证据通常是在权利人企业之外产生的且主要涉及侵权人的信息，应避免侵害他人隐私或其他合法权益，既要考虑“真实性”要求，也要考虑“合法性”要求。

下文将结合商业秘密纠纷的审理要点，分别探讨企业在收集内部证据和外部证据时的相关事宜。

二、商业秘密权利人需要收集的**内部证据**

本部分将结合商业秘密侵权案件审理的司法实践中对于商业秘密范围、权属、保密措施等要件的要求，对较为常见的电子文档、电子邮件两种证据进行讨论并给出实操指引。

(一) 商业秘密的范围

根据法律规定，商业秘密主要包括：技术信息、经营信息以及其他商业信息，其具体范围包括：

- 技术信息：包括与技术有关的结构、原料、组分、配方、材料、样品、样式、植物新品种繁殖材料、工艺、方法或其步骤、算法、数据、计算机程序及其有关文档等信息。

- 经营信息：主要包括与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息[4]。

由于商业秘密的秘密属性，公众无法得知其全部内容，也没有经国家机关确认的、具有公示效力的文本对其范围和权利人身份予以明确。因此，在商业秘密侵权案件中，一个重要的环节就是明确商业秘密范围。权利人首先应当收集记载有商业秘密的载体，并对载体的信息进行概括和提炼以明确秘点。商业秘密案件中常见的载体主要包括：项目设计需求类文档；系统架构等软件设计类电子文档；数据库文档；用户文档；硬件、设备结构、布局等电子图纸；软件与硬件相结合、协调的电子文档；侵权人离职之前已完成的软件版本；软件源代码等。

(二) 商业秘密的权利基础

在明确商业秘密的范围后，原告还应当证明其对所主张的商业秘密享有权利。根据实践中常见的权利来源方式，原告可以是商业秘密的权利人或利害关系人。权利人可以是技术秘密和经营秘密的开发者，或者受让人、权利义务的承继者等。利害关系人一般为商业秘密的被许可人。

原告为商业秘密的原始权利人，即商业秘密的开发者，其可通过提交与其主张的商业秘密相关的项目立项报告、研发记录、测试报告、项目验收报告、项目审批流程等电子数据记录，对其主张的商业秘密的生成时间、具体内容、相关主体等进行证明。如果商业秘密还涉及计算机软件，则数字版权证书、软件著作权登记时提交的软件程序和文档亦可作为权利基础的辅助证明。若原告为上文中原始权利人之外的具有诉权的其他主体，则除了提供原始权利人应当提供的材料外，还应当提供其作为受让方、继承方或被许可方的证明材料。

(三) 商业秘密满足“三性”的要求

在原告明确商业秘密范围和权利基础的前提下，人民法院会进一步审查原告主张的信息是否满足商业秘密的“三性”，即秘密性、价值性及保密性。

- **秘密性**是指涉案信息在被告侵权行为发生时应当“不为公众所知悉”，即公众通过公开资料或公开渠道无法得知。
- **价值性**是指涉案信息具有现实或潜在的商业价值。
- **保密性**是指被告侵权行为发生以前应当采取必要的“保密措施”。

对于上述“三性”的判断，秘密性与价值性可以在产生纠纷后通过专业机构出具相关报告进行证明。而“保密性”则需要企业证明其对商业秘密采取了贯穿始终且合理保密措施，包括：

- 签订保密协议或者在合同中约定保密义务的；

- 通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；
- 对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的；
- 以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；
- 对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的；
- 要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的[5]。

(四) 内部证据管理和收集的实操指引

基于前述商业秘密纠纷中需要原告进行举证的法律要件，结合笔者在处理类似案件的实践经验，笔者在此梳理和列举商业秘密权利人在管理和收集内部证据时需要注意的常见问题，并进行如下实操指引：

1. 电子文档

电子文档包括WORD文档、WPS文档、EXCEL文档、PDF文档等易于修改编辑的文字处理器，或者用专业软件绘制的技术图纸、流程图或效果图等。因其易于修改、编辑、保存、复制、分发的特性，电子文档可以被用于企业日常经营的各个环节，承载了与商业秘密范围、权属、保密措施相关的重要信息，对商业秘密待证事实的证明起到了至关重要的作用。

例如，在笔者近期处理的一起商业秘密案件中，企业在研发阶段以PDF文档和SLDPRT、SLDASM文档（SOLIDWORKS绘制的三维图）的形式来记录其关于原料、配方、工艺、参数、设备、产品的研发过程，并在相关文档上标注“严格保密”等字样，则可以在商业秘密案件中作为证明商业秘密范围的载体或用于证明商业秘密的权属；在每次技术讨论会后生成WORD文档形式的会议纪要，包括参会人员、参会时间等信息，可以用于证明相关人员曾接触过商业秘密以及具体接触时间和范围；企业还可以向员工发送PDF文档形式的员工手册等保密规范或者含有保密条款的合同等，可以用于证明企业采取了相应的保密措施。

然而，电子文档的易于修改、编辑的特性固然可以带来诸多便利，但其也易于被篡改、伪造、破坏且难于管理，因此在商业秘密纠纷中，如何证明电子文档的真实性，也极具挑战性。在实务中经常遇到的问题包括：设计图纸、流程图等技术资料上未显示权利人的企业名称或显示了错误的企业名称，导致无法确定权利归属；企业内部往往保存了同一份技术资料的多份中间版本，无法确定侵权行为发生之时实际使用的或者涉嫌侵权的员工实际接触的是哪个版本；企业仅保存了WORD版本的劳动合同模板，而员工签署后的劳动合同或保密协议原件或扫描件丢失，无法证明员工是否实际已知悉并签署相关协议。因此，建议企业在

前期（如存储阶段、传输和提取阶段）注意电子文档的保存和管理，以便在后期诉讼中与其他可资对照的副本、映像文件或其他资料相互佐证，形成完整证据链，以便证明电子文档的真实性。

在存储电子文档时，需考虑存储的软硬件环境的可靠性、运行状态以及是否具备有效的防止出错的监测和核查手段。在实践中，往往认为个人电脑中存储的文件真实性<公司服务器<第三方服务器。这是由于第三方服务器的数据，包括电子文档的上传、保存、修改时间、修改频率等重要信息，通常仅在第三方的控制和掌握中，而作为使用方的企业来说，一般没有能力对已经上传或保存在第三方服务器中的数据进行篡改。对此，建议企业采用中立的第三方服务器用于存储电子文档，并定期进行存档和上传。

在传输和提取电子文档时，应当考虑传输的软硬件环境的可靠性、运行状态以及是否具备有效的防止出错的监测和核查手段等因素。尤其，在导出电子文档时，应当保证传输及存储介质的清洁性，尽量保留导出文档的原始数据，不对其进行编辑、删除、合并等操作，同时对传输和提取的过程进行记录。在实践中，企业可以通过公证、第三方电子证据机构取证等方式来确保其所提取、保存、传输的电子文档的真实性。例如，可使用存证云^[6]客户端对重要的电子文档快速进行哈希值计算，保全后存储在云端，防止后期篡改。

此外，每个证据都不是一个孤岛，无论是在前期调查阶段、还是取证阶段，都需要注意形成证据链条。例如，除了对电子文档本身进行存储和管理，企业也可以保留相关电子文档的发送和接收记录，以及邮件串，例如企业通过电子邮件、工作群等方式向相关人员发送相关电子文档并要求确收回执的记录，以便作为证明电子文档真实性的辅助证据。

2. 电子邮件

电子邮件是企业间交流沟通、业务往来的重要途径，同样可能贯穿着企业商业秘密的开发和使用的全过程，包含与商业秘密范围、权属、可能接触到商业秘密的人员、时间等相关的重要信息。例如，邮箱名称往往由员工的名字与公司邮箱后缀组成，每个电子邮箱对应的用户是特定且唯一的，可以通过邮箱地址追溯到特定的人员以确认相关当事人与公司主体；邮件时间可以用于证明商业秘密生成、或相关人员接触到商业秘密的时间；电子邮件的签名可以用于证明发件人的公司名称、个人名称、工作岗位、所述部门等信息。正文内容有助于判断和证明待证事实、案件当事人之间的关系以及与案件的关联性。此外，电子邮件中包含的附件，如合同、文档、技术资料等，也是用来证明所涉及的商业秘密范围、权属、时间、人员等信息的重要来源。

在笔者近期处理的一起商业秘密案件中，权利人与其合作方约定由权利人提供技术，由合作方对相关工艺和设备进行微调并制造相关产品，且期间所产生的全部知识产权归权利人所有。在近十年的合作过程中，双方主要通过电子邮件及附件沟通技术细节，因此电子邮件中承载了大量的商业秘密。在产生纠纷后，我们梳理了近十年的往来邮件，通过电子邮件正文、附件中的图纸、会议记录、技术文档等来确定商业秘密范围；通过发件人、收件人的邮箱后缀和签名、发送或接收时间等来确定技术信息的提供主体、接收主体和接触时间；并结合双方关于知识产权权属和保密义务的约定，证明了商业秘密的范围、权属和采取的保

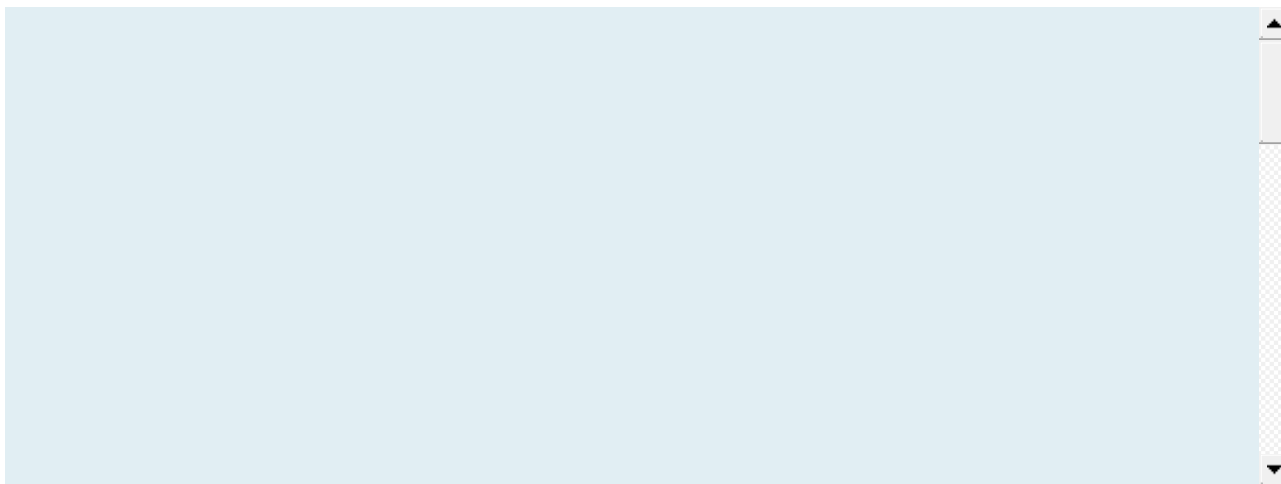
密措施等。

在实践中，除了可以通过电子邮件发送上述技术资料，企业也可以通过电子邮件向员工送达企业内部关于商业秘密管理的规范性文件，以证明采取了相应的保密措施。例如，通过群发邮件的方式，向员工发送员工手册等保密规范并且设置回执提醒，以作为证明员工收到并知晓该邮件及员工手册的初步证据，避免员工因主张其并未收到类似邮件而否定自己的保密义务。

对于电子邮件的管理，随着企业员工的入职离职、邮箱账号迁移、邮箱账号注销等情况发生，相关电子邮件可能被损坏或灭失，从而导致重要证据的遗失。针对上述情形，建议企业在核心员工离职后，尽量对邮箱内容进行备份，避免立即注销邮箱账号，并且建议企业要求员工在发送电子邮件时，尽可能避免仅发给唯一的收件人，以保证在该收件人离职、邮箱账号异常或注销时，其他被抄送人员的账号中仍保存有相关原始邮件。此外，类似于上述电子文档的保存，与企业自己运行的邮箱服务器相比，由中立第三方提供的企业邮箱导致数据被篡改的可能性更低。

对于电子邮件作为证据的提交方式，应当尽量提交原始邮件，并体现电子邮件的收件人和发件人信息、收发时间、邮件正文及附件等必要信息；相反，如果电子邮件经过转发或引用，因在转发或引用过程中可以进一步编辑邮件内容或附件，可能导致难以证明真实性。另外，可以通过当庭展示或证据保全的方式来证明电子邮件的真实性。在当庭展示时，建议提前将需要演示的邮件放入单独的文件夹中，以便节省时间、提高庭审效率；对于需要特殊网络设置才能打开的邮件，建议提前由技术人员测试相关环境，确保当庭演示中，可以正常打开和浏览相关邮件。这种方式可以尽可能地节省时间和成本，但也存在因网络或设备故障无法打开邮箱，以及误删或遗失相关电子邮件的风险。因此，在时间和预算允许的情况下，提前由公证处或第三方电子存证机构进行证据保全是更为稳妥的方式。为了提高保全效率并节约成本，目前我国法院已逐渐接受由第三方电子证据机构进行存证的方式，根据近日的统计数据，采用可信时间戳TSA的案例有8万余件，覆盖全国900多家法院[7]。除了可信时间戳TSA外，企业还可以采用：网易公正邮[8]、IP360取证[9]、腾讯推出的至信链[10]、阿里云可信存证服务[11]等。

以上为有关企业商业秘密保护中电子证据的管理与运用中“商业秘密权利人需要收集的内部证据”的相关内容，下一篇文章我们将继续探讨“商业秘密权利人需要收集的外部证据”。



*本文首发于知产前沿

2023-09-21