

Enterprise Software Compliance: Risks and Strategic Countermeasures (I) — Pirated Software Infringement Issues

Author: Yolanda JIA

近年来，随着我国知识产权保护体系的日益完善和执法力度的持续加强，软件权利人的维权意识显著提升。在这一背景下，企业软件合规使用问题日益凸显。实践中，许多企业由于缺乏专业的知识产权管理机制，往往在不知情的情况下陷入软件侵权纠纷——或是突然收到法院传票，面临高额索赔；或是频繁遭遇权利人的律师函警告，却因缺乏专业应对策略而陷入被动。这种法律风险不仅可能给企业带来重大经济损失，更可能对商誉造成难以弥补的损害。

帮助企业防范法律风险、制定合规策略，我们推出“企业计算机软件合规风险及应对”系列文章，从不同场景解析软件侵权的法律后果及应对方案。本文为开篇，**聚焦盗版软件侵权问题**，分析企业可能面临的法律责任，并提供实务建议，助力企业构建合规管理体系，降低侵权风险。

一、使用盗版软件的具体情形

在实践中，每个企业对于不同软件的需求各不相同，每款软件的下载渠道、许可方式也存在较大差异，故软件使用情况较为复杂和多样。如果企业没有完备的合规体系或审核制度，那么企业员工在通过不同渠道下载软件并进行安装、使用的时候，就有可能给企业带来侵权风险。常见的使用盗版软件的行为主要体现为以下几种情形：

- 擅自使用软件权利人官方网站提供的免费版或试用版软件从事商业活动；
- 通过非官方渠道获取软件，包括但不限于第三方镜像站点、网盘分享等非正规下载途径；
- 直接下载和使用经过技术破解的软件版本，或使用非法激活工具规避正版验证机制；
- 冒用教育机构工作者等主体资格获取专用免费版本，如面向老师及学生的免费教育版本；
- 在软件许可到期后未及时续约仍继续使用，或擅自使用已被权利人明确撤销的授权密钥进行软件激活等。

以上行为均属于未取得软件权利人授权或超出软件权利人授权范围的侵权行为。如软件权利人对企业上述获取及使用软件的行为进行取证并向企业主张权利，企业将面临承担相应侵权责任的风险。

二、权利人常见取证渠道

软件权利人可以通过多种渠道获取软件使用信息，并根据所获信息的证据证明力强度及取证手段合法性，在谈判、诉讼等阶段进行有选择地使用。常见取证渠道如下：

（一）通过公开渠道取证

企业对外发布的公开信息是权利人获取初步线索的重要渠道之一。例如企业公开招聘信息中要求应聘者须熟练使用权利人软件，企业官网宣传资料的水印包含权利人软件水印，或企业宣称的其产品的功能或效果仅权利人软件可以实现等，均可以作为权利人进一步对企业进行侵权调查的线索。

同时，该等信息也会在诉讼阶段作为辅助证据证明侵权行为。例如在(2022)最高法知民终1910号案中[1]，原告提交的公证书及其附件载明，被告的公开招聘信息中，对于部分工程技术人员岗位要求包括熟练使用、操作原告软件等设计软件。一审法院湖北省武汉市中级人民法院对此认为，“武汉某汽车技术有限公司（被告）的互联网招聘信息也印证了其将权利软件作为经营工具使用的事实”。二审法院最高人民法院未对此进行进一步论述。

（二）通过技术手段取证

1. 后台数据

部分软件在运行过程中可能会出于功能实现、安全维护等需要，自动连接至软件权利人的服务器。在该机制下，如果企业安装了盗版软件，软件权利人可能会获取部分使用信息，从而作为侵权证据使用。不过，在我国对数据保护愈加重视的背景下，此类信息是否满足证据的“合法性”的要求尚存在争议。此外，这种后台数据通常是在权利人的服务器上生成并在权利人的控制之下，权利人如果将其作为证据使用，如何能证明其真实性、未经篡改，也有一定难度。

2. Telnet远程取证

Telnet远程取证是通过计算机命令与目标服务器端口建立TCP连接，探测并获取目标服务器反馈的正在运行的软件信息，从而帮助判断目标服务器是否正在运行权利人软件。目前，部分法院认为提交Telnet远程取证数据可以视为原告完成初步举证，从而将举证责任转移至被告，如被告未能举证，则法院将认定权利人主张的侵权事实成立[2]。

（三）申请行政机关或法院进行证据保全

由于计算机软件侵权行为往往发生在被告的经营场所内，极具隐蔽性，软件权利人难以直接获取关键侵权证据。此时，软件权利人可以申请行政机关或法院进行证据保全，从而获得侵权证据。该等证据通常作为法院认定侵权成立以及计算赔偿数额的重要依据。

例如，(2018)沪民终511号案中[3]，文化执法总队经原告申请对被告经营场所内的计算机进行了现场检查，发现了未经原告授权许可的软件3套。一审法院上海知识产权法院据此明确了侵权软件数量，并据此判决被告赔偿原告经济损失849,000元，二审法院上海市高级人民法院维持一审判决；(2017)京73民初396号案中[4]，经原告申请，一审法院北京知识产权法院至被告办公场所进行证据保全，对被告办公场所的电脑进行随机抽样检查，并根据抽查电脑中安装涉案软件或有删除涉案软件痕迹的软件占抽查软件总数的比例，推定被告所有电脑中安装/曾安装涉案软件的数量，据此确认被告实施侵权行为对应的软件数量，并判决被告赔偿原告经济损失2000万元。

三、使用盗版软件的法律风险

《著作权法》第五十三条规定，未经著作权人许可复制作品的，侵权人应当承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任。除《著作权法》规定的使用盗版软件的法律风险外，侵权人还可能面临惩罚性赔偿，甚至罚款等责任。

（一）卸载盗版软件

根据《著作权法》的规定，停止侵权是侵权人应当承担的责任。毫无疑问，使用盗版软件的法律风险包括立即停止使用盗版软件，并卸载相关侵权软件。

（二）赔偿损失

除停止使用盗版软件外，赔偿损失也是常见的法律风险。通常而言，赔偿损失的金额可以根据权利使用费进行计算，即赔偿金额=涉外软件对外销售或许可时的价格乘以侵权软件数量。例如(2021)京73民初345号案中[4]，法院以被告使用103套盗版CATIA软件（单价33万元）总价3399万元为基础，最终支持原告2000万元诉请。此外，合理维权费用（如公证费、律师费）亦由侵权方承担，在该案中，法院判决被告赔偿合理支出80,500元。然而，还有一种情况是被告拒绝提供使用盗版软件的数量，导致法院难以查明事实。此时法院会综合考虑涉案计算机软件的名度、销售价格、被告公司侵权行为的性质、主观状态、侵权情节及持续时间等酌情确定赔偿金额。例如，在(2020)最高法知民终404号案中[5]，被告戴鑫公司不能提供涉案服务器和软件的销售数据，且原告微软公司于不同时间从被告戴鑫公司处购买的3台服务器中均安装有未经许可的涉案软件，因此法院最终酌定被告戴鑫公司赔偿经济损失500,000元及合理费用100,000元。

（三）惩罚性赔偿

《著作权法》第五十四条规定了惩罚性赔偿制度，对于主观恶意明显、侵权情节严重的著作权侵权行为，法院可以在计算确定赔偿数额的基础上，判处一至五倍的惩罚性赔偿。

例如，在（2023）最高法知民终1778号案中[7]，当法官在被告公司进行证据保全时，发现公司员工正在电脑上紧急删除软件，在法官重申相关规定的情况下，公司员工的删除行为依然持续发生。法官当场开展调查后发现，公司为避免被发现使用盗版软件，在多个微信群中通知员工删除软件。法院认为，该公司曾经采购过涉案正版软件，明知使用涉案软件应取得权利人许可，在权利人多次发送律师函的情况下仍持续侵权，在人民法院证据保全过程中拒不配合，侵权故意明显、侵权情节严重，参考软件销售价格酌定权利许可使用费金额，基于侵权软件数量，确定惩罚性赔偿数额的计算基数，同时适用一倍惩罚性赔偿，判决该公司等停止侵权、并赔偿原告损失600万元。[8]

（四）罚款

除民事责任外，侵权者可能面临其他制裁，例如妨碍诉讼的罚款。在前述（2023）最高法知民终1778号案中，由于被告存在规模性的删除侵权软件、毁灭侵权证据的行为，最高人民法院依据《民事诉讼法》第一百一十四条，对被告顶格罚款100万元。[9]

四、收到侵权警告函后的合规建议与应对

软件权利人为全面维护自身权益，往往会批量向涉嫌侵权的企业发送侵权警告函。然而，收到警告函本身并不等同于企业确实存在侵权行为，这仅是权利人维权的初步动作。面对此类警告函，企业应当保持冷静，采取专业、审慎的应对态度。以下是针对此类情况的专业合规建议与系统性应对策略：

（一）核实发函公司的身份和合法授权资质

在采取任何实质性行动前，企业应全面审核发函公司的真实性以及权限，例如：审核发函公司的软件权属证明材料是否完整齐全、发函公司是否具有软件权利人的合法授权等。

在笔者处理的多起软件维权案件中，即存在某些公司并无软件权利人的维权授权却发送警告函的情形。此时，发函公司及其代理人是否有权代表软件权利人进行维权存在较大不确定性，企业应谨慎对待与该代理人的后续沟通。

（二）开展企业内部自查

在收到侵权警告函后，企业应同时开展内部自查。自查内容包括被指控软件是否存在实际使用、使用数量、使用方式、使用范围、使用人员；软件的来源、版本、下载渠道；是否有购买记录或许可协议等。

需要注意的是，企业还应重点核查员工是否私自下载安装盗版软件。部分员工可能存在法律意识薄弱的情况，下载安装了盗版软件，此时企业并不知情。但鉴于企业对员工的工作行为负有监督义务，如员工因工作原因使用了盗版软件，员工的行为与企业经营利益一致，那么企业可能需要对该员工的行为承担责任。

考虑到软件使用合规的复杂性，建议企业尽可能在早期引入律师团队，以获取专业的建议和指导，从而避免企业在交涉中由于法律意识薄弱或经验不足作出了一些不利陈述使得企业陷入被动局面。

（三）自查后的应对措施

如企业自查后，未发现使用盗版软件的行为或盗版软件存在合法来源。那么建议企业注意收集、保存、固定相关证据，例如邮件、合同、票据等。另外，企业也可以告知发函公司其并不存在侵权行为。

如企业自查后，发现存在使用盗版软件的行为，应立即要求相关人员停止使用并卸载相关软件。并根据企业目前的

生产经营情况、未来需求以及过去的使用情况，确定需要购买或增购的软件数量，与权利人开展商业谈判，以达成一揽子解决方案。同时，在一揽子许可协议中明确约定，权利人是否放弃对企业的历史使用行为主张权利，包括放弃诉讼、仲裁、举报等。

若购买或增购正版软件的费用过高，企业也可以考虑使用免费替代软件，或购买价格低的其他正版替代软件。

（四）增强员工培训，避免员工个人下载盗版软件为办公使用

实践中，许多使用盗版软件行为是员工个人行为，因此建议企业加强内部培训。例如：将软件合规纳入新员工入职培训，定期举办软件合规专题讲座，制作《正版软件使用指南》宣传材料等。

（五）其他

除了前述建议外，企业还可以通过以下途径做好风险防控：

1. 制度及流程管理，如建立规范的软件管理制度和使用规范，要求员工按照制度规范下载、安装或使用软件，以更好地监督员工的软件使用行为，同时也可以用于证明企业履行了一定的管理义务；
2. 合同约定，例如企业在与供应商、合作方进行合作时，在协议中明确约定供应商、合作方应使用正版软件，若存在侵权行为，则由供应商、合作方承担侵权赔偿责任等；
3. 规范招聘广告和对外提供的其他信息，如在发布广告或其他对外信息前进行审核，以避免可能的侵权风险等。

五、结语

在信息时代，计算机软件在企业中的作用愈发重要，因计算机软件引起的纠纷也越来越多。本文先对目前较为常见的权利人发送有关使用盗版软件的侵权警告函的情形，进行分析并提出合规及应对建议，以期为企业提供实操指引与合规思路。后续我们将介绍其他常见的软件侵权情形并提供应对建议，敬请期待。

注释：

[1] (2022)最高法知民终1910号民事判决书

[2] (2017)粤民再463号民事判决书

[3] (2018)沪民终511号民事判决书

[4] (2017)京73民初396号民事判决书

[5] (2021)京73民初345号民事判决书

[6] (2020)最高法知民终404号民事判决书

[7] (2023)最高法知民终1778号民事判决书

[8] <https://www.hshfy.sh.cn/shfy/web/xxnr.jsp?pa=aaWQ9MTAyMDQxMTkwNCZ4aD0xJmxtZG09bG01MTkPdcssz>

[9] 同上