

执法咨询委员会

第十八届会议

2026 年 6 月 2 日至 4 日，日内瓦

打击数字盗版：通过 DNS/IP 屏蔽和 OSINT 工具进行战略执法

撰稿：立陶宛广播电视委员会监督处处长阿德里乌斯·卡蒂纳斯（Andrius Katinas）先生，立陶宛维尔纽斯*

摘 要

本文介绍了立陶宛广播电视委员会为打击在线版权侵权而采用的执法模式，该模式将 DNS（域名系统）和 IP（互联网协议）屏蔽与开源情报（OSINT）调查相结合。该委员会实施了一系列措施，如 DNS 屏蔽、镜像网站屏蔽和相关 IP 地址屏蔽、版权侵权罚款，以及冻结与盗版活动有关的银行账户。本文进一步强调了 2025 年执法的成功范例，并建议其他司法管辖区可以效仿立陶宛为保护在线版权和邻接权而采取的独特方法。

* 本文件中表达的观点为作者的观点，不一定代表产权组织秘书处或成员国的观点。

一、导言：立陶宛广播电视委员会

1. 立陶宛广播电视委员会（委员会）是国家视听服务监管机构。其职能之一是打击数字盗版。自 2019 年以来，委员会一直致力于保护在线版权。这包括实施域名系统（DNS）屏蔽，随后屏蔽盗版镜像网站和互联网协议（IP）地址，并对侵犯版权和邻接权的行为处以罚款。委员会冻结了用于为盗版活动牟利的银行账户，将 URL、域名和 IP 地址从谷歌搜索引擎中移除，删除了盗版网站上的广告（也使用了 WIPO ALERT 平台），并暂停了 Google Play 和 Apple Store 平台上的非法互联网协议电视（IPTV）服务。

2. 委员会已经屏蔽了 400 多个域名和 7,000 个 IP 地址，这些域名和 IP 地址在未经权利人同意的情况下发布了受版权保护的内容。自 2023 年以来，委员会还对 250 多起版权侵权案件处以罚款。为确保屏蔽程序的有效性，委员会开发了一个集中式自动域名屏蔽系统，以最大限度地减少人为错误的可能性。该系统会自动向互联网服务提供商（ISP）发送具有约束力的指令。当委员会发现违规行为（如先前已被屏蔽的盗版域名的“镜像”网站）时，会同时向所有提供商发出指令。当委员会决定限制访问某些域名或 IP 地址时，这些信息会被上传到一个集中式系统。在 20 分钟内，域名或 IP 地址会被自动屏蔽（或在同一时限内解除屏蔽）。

3. 2025 年是委员会在执法方面取得成功的一年：针对非法 IPTV 服务做出了若干项决定，其中包括：

(a) 委员会对托管服务提供商 UAB Melbikomas 罚款 10,000 欧元，原因是其违反了欧洲联盟（欧盟）的制裁规定，包括非法托管和通过流媒体播放 50 多个体育频道的内容。[†]这是立陶宛首例针对促成非法内容分发的托管的案件。继 2023 年发现该提供商违规之后，2025 年的调查显示，其仍在托管违反制裁规定的内容。

(b) 维尔纽斯地区法院维持委员会对 UAB Consilium Optimum 非法分发 Go3 节目处以 1,900 欧元罚款的判决。该公司被发现向其用户非法分发 Go3 Sport、Go3 Sport 2 和 Go3 Sport Open 等节目。委员会根据《立陶宛行政违法法典》第 122 条第 3 款，对非法公开分发受版权保护内容或相关权内容的行为处以罚款。2025 年 6 月，法院维持上述判决，驳回了该公司的上诉，并确认委员会的措施合法合理。

(c) 根据《行政违法法典》关于不遵守国际制裁规定的第 515 条第 1 款，委员会对违反欧盟制裁的个人处以 3,100 欧元的罚款。[‡]当事人通过网站非法分发被禁电视频道，其中包括 30 多个体育频道和其他受欧盟制裁广播公司的内容。

这些执法行动是防止转播被禁内容和确保在该国遵守国际制裁的持续任务的一部分。

二、开源情报：版权侵权调查的现代方法

4. 在常规监管措施中，委员会开发了在线追踪犯罪者的开源情报（OSINT）技能。经验表明，提供托管、VPN、在线金融交易、云服务和 DNS 解析器等服务的在线中介是版权侵权调查的核心。为了跟踪数字侵权行为，委员会使用了 domaintools.com、oxylabs.io、epieos.com、Wireshark 和 SimilarWeb 等工具，帮助识别犯罪者和评估非法活动。

[†] <https://www.rtk.lt/en/news/rtcl-fines-hosting-provider-eur10-000-for-breaching-eu-sanctions>

[‡] <https://www.rtk.lt/lt/naujienos/lrtk-skyre-didziule-bauda-uz-es-sankciju-pazeidima>

5. 委员会官员还为国家和欧盟法官、信息技术专家、国家监管机构、检察官和警察举办 OSINT 培训或参加这些培训。委员会认为，分享良好做法和技术诀窍使追踪数字侵权行为的任务变得更加容易。

三、版权侵权是一种混合威胁：私人数据泄露

6. 委员会发现，立陶宛的盗版行为与泄漏的私人数据密切相关。2019 年或 2020 年的某个时候，立陶宛非法电影流媒体服务 Filmai.in 遭到数据泄露，645,000 个电子邮件地址、用户名和纯文本密码被曝光。被泄露的数据库已在暗网公开。[§]当用户在盗版网站注册时，网站管理员会收到一些数据，其中包括 IP 地址（表明用户的位置）、ISP、密码、假名（登录名）、电子邮件地址和电话号码。如果服务是付费的，用户还会留下银行卡详细信息。由于盗版网站的管理员连最起码的数据安全要求都不遵守，更不用说侵犯版权了，因此用户的个人数据最终会流入黑市，在那里被出售或免费分发。例如，此类数据对金融欺诈者非常有用，他们利用这些数据锁定受害者。因此，除了版权侵权，还存在非法使用个人数据、欺诈和身份盗窃的风险。甚至还发现政府官员使用官方电子邮件地址在 Filmai 网站上注册，造成安全问题，例如可能未经授权进入国家机构、签署文件或答复居民的询问。该网站现已被屏蔽，但密码等敏感信息却被公开了。^{**}

四、版权侵权是一种混合威胁：虚假信息

7. 委员会还对互联网上的非法电视频道分发商（IPTV）进行监控，这些分发商往往在敌对国家运营。是通过 SimilarWeb 搜索引擎优化（SEO）工具监控的，该工具可自动监控用户流量最高的非法 IPTV 服务。然后对域名、IP 地址和互联网中介（如托管服务提供商、代理服务器和 VPN）进行人工分析，以便采取适当措施。这些频道包括欧盟制裁的媒体平台，它们不仅传播宣传和虚假信息，还在未经权利人同意的情况下转播许多国家频道和体育赛事直播。委员会在以版权侵权为由屏蔽转播内容的同时，还会屏蔽对敌对信息的获取（反之亦然），这是混合战争的一种手段。

五、结论

8. 自 2020 年以来，委员会已经建立了健全的国家法律框架和信息技术能力，以保护在线版权和邻接权。鉴于该国的地缘政治形势及其在版权侵权方面的法律实践历史，委员会制定了一套应对此类侵权行为的独特方法，可为其他国家当局和权利人提供参考范例。

[稿件完]

[§] Have I Been Pwned (2026 年)。Filmai.in 数据泄露。可查阅：[//haveibeenpwned.com/Breach/FilmaiIn](https://haveibeenpwned.com/Breach/FilmaiIn)。

^{**} Jokubaitis, Marius (2021 年 2 月 20 日)。Kaip rodo nutekinti „Filmai.in“ duomenys, piratinėje svetainėje naudodami Seimo ar ministerijų el. adresus registravosi ir valdžios atstovai. LRT。可查阅：https://www.lrt.lt/naujienos/lietuvoje/2/1348778/kaip-rodo-nutekinti-filmai-in-duomenys-piratineje-svetaineje-naudodami-seimo-ar-ministeriju-el-adresus-registravosi-ir-valdzios-atstovai?srsId=AfmB0oraqvuySUNo3f3V_Ha8nWCZB3eDiryazKGCNFi-qr4e249ggD（仅立陶宛语）。