

优秀论文：互联网技术措施的合法性问题探讨 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/484/2021_2022__E4_BC_98_E7_A7_80_E8_AE_BA_E6_c122_484568.htm

互联网的产生和应用，依赖于先进的、强大的技术支撑。互联网的全球连接和彼此交互特性，又使得基于互联网的技术措施具有越来越普遍、广泛的影响力。互联网的基本技术是计算机软件技术，而软件技术的快速发展、迅速应用，以及软件产品在法律意义上的技术标准的滞后、缺乏，又使得这些技术措施的研发和应用缺乏必要的规范性。对于越先进的技术，用户就越只能专注于使用，无法了解功能背后的技术门道，互联网技术也同样使得大部分用户对其所使用的功能背后的深奥技术背景几乎一无所知，完全任由技术开发商们的摆布。所有这些已影响互联网商业秩序和用户的应用。一般提到技术措施，人们一般容易联想到我国著作权法中所禁止的“故意避开或者破坏权利人为其作品、录音录像制品等采取的保护著作权或者与著作权有关的权利的技术措施”。著作权法所称的该技术措施，是指著作权人为保护其权利所采取的控制他人访问和使用作品的技术手段，常用于互联网环境，但不限于互联网环境。著作权法所禁止的一般就是故意避开或破坏这些技术措施的技术措施。本文所讨论的主要是基于互联网应用的软件技术措施，而不讨论单独的软件技术。此处讨论的技术措施广义上包括所有互联网技术，而限于该技术措施的特定用途。比如“蜘蛛程序”，可以称为是一种技术措施，最后成为具有巨大影响力的互联网搜索行业的技术基础。另如，拦截弹出页面的技术，既可用于用户拦截弹出广告，也

可用于拦截其他公司的软件安装弹出框。可见，这些技术措施的应用形式是发展的，开始可能是小打小闹、属于雕虫小技，最后也可能发展为一个独立行业，有的可以用于合法用途，同时也可用于非法用途。本文试图探讨基于互联网的技术措施的合法性和规范问题，以浅薄之见以图抛砖引玉之效。

一、互联网技术措施的分类 从不同的角度，互联网技术措施有不同的分类，比如：

- 1、按照技术措施的重要性，可分为基本功能性技术措施和附属功能性技术措施。前者是指实现该技术的主要基本功能而采取的技术措施，后者只为了基本功能更好地实现而采取的辅助技术措施。如电子邮件系统软件，收发邮件及邮件管理等技术措施属于基本功能，防垃圾邮件、过滤等技术措施属于附属功能。
- 2、按照技术措施的对外特性，可分为消极防御性技术措施、积极防御性技术措施、攻击型技术措施。消极防御性技术措施，是指针对外来的破坏，能够通过该措施进行某种程度的阻碍，但无论阻碍是否成功，一般都对该外来的技术措施并无影响，比如普通加密措施。积极防御性技术措施，是指针对可能或必然产生的外来破坏，通过判断和识别，先行制止该破坏行为的发生，其中有可能对该外来的技术措施进行“先发制人”的破坏，比如杀毒软件的查毒和杀毒。攻击型技术措施，是指以破坏对方为目的、对其自身正当功能毫无必要(或者其自身并无破坏对方之外的其他功能)的技术措施，典型的如病毒程序。
- 3、按照技术措施在相应软件中的作用，可分为必要技术措施和非必要技术措施。必要技术措施是指实现软件基本功能所必不可少的技术措施，而非必要技术措施，是指对该软件的正常功能而言，该技术措施并非必不可少。
- 4、按照技

术措施的生效方式，可以分为客户端控制技术措施和系统性控制技术措施。客户端控制技术措施，往往是由用户安装客户端软件并能够有效选择和卸载来实现的技术措施，而系统性控制技术措施，是指在用户不知情的情况下自动生效、被迫安装或安装后无法选择、卸载的技术措施。比如，广告拦截常是前者，设置链接常是后者。还有一些系统控制性技术措施，比如捆绑安装，如果某用户安装了某公司的一种产品，则被迫安装该公司的另一个产品，否则原来的产品就无法再使用。这就有可能涉及到侵犯消费者权益和垄断问题。

5、按照技术措施的功能和目的，可分为善意技术措施和恶意技术措施。如果技术措施是为了满足社会正常的需求或为了满足法律的规定而采取的，一般是善意的技术措施。否则，如果是出于非法目的而采取的，就是恶意的。如关键词过滤技术，如果是公众BBS系统正常使用，就可能是善意的，而如果是用于控制公众对竞争对手的网站的访问，或者是在搜索中控制公众对信息的正常获取，就可能是恶意的。应该说明的是，如果善意的技术措施被他人不可控地用于非法目的，则不能随意确定为恶意技术措施，如用户用即时通讯技术传输淫秽资料。但如果某软件专门用于供公众搜索淫秽资料，就可能是恶意的。

6、按照相关技术的发展状况，可分为无法克服的技术措施和可以克服的技术措施。前者是指由于受到当前硬件、软件技术的限制，有些技术问题无法解决，或者说需要经过发现后才能解决。典型的如一些软件的Bug，是设计和编写软件时无法克服的，有可能因此而导致一些技术问题，但无法一开始就予以克服。后者是指该技术措施是可以取消的、可以替换的，或者比照同等替换的第三方技术而

言，是可以克服的。二、判断技术措施合法性的标准 对技术措施进行初步分类，有利于对纷繁复杂的互联网技术措施进行合法性判断。此处所指的合法性，应综合考虑技术措施的目的和动机、效果和影响、法律的明确强制性规定等因素。由于互联网技术发展和应用极快，而立法、司法相对滞后，因此判断互联网技术措施的合法性应比一般技术措施倍加谨慎。这是双刃剑，既可能促进互联网的健康发展，也可能因不慎而阻碍甚至扼杀某个领域的技术措施所带来的良好社会效果。特别是在互联网的条件下，人们的预见能力大为降低，今天的预计和判断与明天的现实可能完全相反。尤其是考虑到互联网的生命力就在于其开放性的环境，以及由此焕发出来的商业和技术创造力，并且考虑到中国在互联网技术领域与世界水平相对差距较小，因此，笔者认为，在目前我国判断技术措施的合法性，应更多地考虑其是否具有现实或潜在的强大公众需求和商业应用前景，是否损害公众利益，是否影响网络安全，而不应该更多地考虑竞争是否充分、是否存在垄断等相对利益的问题，多关注国家、社会、行业和公众利益，少关注局部或个体利益，在合法性的判断上采取较宽松的标准，先扶植、发展和商业性应用起来再说。笔者反对在该领域采取技术和秩序上的保守主义，害怕秩序被打破，担心技术滥用和引起不公平。因为互联网的发展就是在不断地打破秩序的过程中建立秩序，在短暂和表面的不公平中寻找实质性公平。不这么做就可能窒息互联网的生命力。技术措施的违法性与其后果密切相关，目前来看，常可适用反不正当竞争法、消费者权益保护法、民法（尤其物权）、合同法等法律，同时可能适用著作权法等具有明确规定的法律。

根据上述分类，基本功能性技术措施常不具有违法性，只要该技术措施能满足正常的社会公众需求，具有商业应用前景，不具有不可逆的破坏性，就应该认定为合法的技术措施。典型的如广告框拦截技术。对这一类技术措施尤其不容易识别，在大规模的商业化应用甚至成为一种行业之前，其价值很难让人充分意识到。比如搜索、链接，在其产生的早期也许并不是都能意识到其日后的风光，也有可能被作为“异端”而认定为非法。因此，判断此类技术措施时，尤其有必要看大方向、大趋势。如果这种技术措施不是攻击型的、恶意的，尤其是如果属于客户端控制的，那么常应认定为合法。消极防御型的技术措施（如登陆密码之类）常不会是非法的，而攻击型的常是非法的（除非是杀毒这一类的“以毒攻毒”），著作权法中的关于破坏权利技术措施的行为就属此类（其中的合理使用属于法律明确规定的攻击型技术措施的例外）。攻击型技术措施的合法性应由法律明确规定。积极防御型技术措施的合法性就存在很大的模糊空间，存在合法性和善意恶意不确定的状况。如果防御的对象是假象的、不存在的，或者是被夸大的，那么这就成了攻击型的技术措施。如果防御行为超出必要限度，就成了非必要技术措施，其违法可能性就增大。非必要技术措施一般只能是消极防御型的，否则违法的可能性就大增。无法克服的技术措施，即使对他人或用户具有一定的不良影响，但只要其益处是主要的，那么就应该允许其存在，就是合法的。还有一些其它标准可用于判断技术措施合法性，比如同等替换的第三方软件情况，该技术措施对用户是否必要，用户是否足以享有知情权和选择权。

三、非法技术措施的法律后果

技术措施一旦被认定

非法，最直接后果就是停止该行为（其它民事法律责任，或行政责任、刑事责任在此不赘述）。而要准确要求其停止该行为，就首先要认准这在技术上到底属于什么样的行为。这在实践中很不容易做到。实践中常只能先捕捉现象，有时候甚至对现象的取证都很难，而对现象进行技术分析就更难，没有软件的源代码常难以做到，而非法技术措施的提供者又不可能主动提供。在此情况下需要一些强制措施以了解技术措施的真相。因此，对于认定为非法的技术措施，先要准确判断和描述该技术措施行为的具体情况，包括其技术手段、功能或效果特征，在此基础上可采取不同的措施，比如责令取消特定技术措施，责令修改特定技术措施等。由于技术手段花样翻新，对于非法技术措施，不应只制裁所取证到的具体表现形式的技术措施，而应该包括禁止采取相同或类似功能、效果的技术措施，即使其技术实现方式不一样。

100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com