检察日报/2013 年/1 月/24 日/第 003 版
学术

对信息内容可分级法律规制

中国社会科学院法学研究所研究员　陈欣新

根据公共信息内容与法律规制的关系以及信息源属性，对信息内容进行分类，并按照信息内容与国家安全、公共安全、社会道德和普遍的社会价值以及个人(法人)正当权益保护的关联程度，对信息内容进行分级监管，应是当前确定网络信息内容法律规制方式和手段的基本思路。

对国家安全、公共安全具有明显而即时威胁的有害信息的监管

对于那些对国家安全、公共安全构成即时性或明显而现实的危险的信息内容，应采取事先积极预防、事中及时处置为主、事后追惩为辅的思路来管理。主要监管手段有两个，其一是网络信息过滤措施，其二是即时监控措施。由于网络技术本身的特性，预防的效果不可能达到完全阻断传播的目的，一旦在网络上发现有此类信息传播就应立即采取措施进行有针对性的阻断或删除措施，尽量缩小有害信息传播的范围，消除其不良影响。在这种情况下，事后的惩治虽然重要，但并不是监管所面临的最突出矛盾。此时，最突出的矛盾是如何在短时间内采取应对措施，而不是如何处置当事人。因而，此种情况下，监管的原则是，事先的监管和即时的监管应优先于事后监管和事后的惩治。即时应对的机制应体现在具体的法律规定之中，使相关机构的作为有法可依。最佳的监管方式是能够平衡公民权利与国家安全之间的关系，即便是在国家出现危机或处于紧急状态的情况下，这种平衡也不会被打破。

从多数国家的法律规定看，基于防范对国家安全、公共安全构成即时性或明显而严重威胁的行为，法律都授权政府可以采取限制信息自由的措施，如美国联邦最高法院根据霍姆斯大法官提出的“ 明显而即时的危险 ”原则，允许政府采取网络监控、信息下载储存、屏蔽网页、过滤特定信息的措施。“ 9 · 11 ”以后，基于对国际恐怖主义的防范需要，美国国会以压倒性优势通过了相应的法案，授权美国联邦政府对美国境内的数字通信活动进行监视。美国联邦调查局启用了互联网监控系统，对互联网用户的隐私权造成了一定威胁。此外，根据美国国会制定的新法律，ISP(互联网服务提供商)必须允许政府机构获取通过其网络传送的数据信息。

欧洲人权法院根据欧洲人权公约第 10 条第 2 款的规定(行使表达自由伴随一定的义务和责任，故应当受制于一定的形式、条件、限制或刑罚。此类制约应该为法律所规定，为民主社会所必需，并且有利于国家安全、领土完整或公共安全，服务于防止秩序混乱或犯罪、维护健康或道德、保障其他人的名誉或权利、防止披露保密获得的消息、或者维护司法的权威和公正无偏)，不否认各成员国有权通过立法赋予政府对互联网所传播的有害信息进行监控和屏蔽。

值得注意的是，在对国家安全和公共安全的安全程度要求方面，中国与美国具有相似性。如果比较我国和美国的情况，由于美国政府在技术上具有优势，技术上的优势可以在一定程度上弥补行政监管的不足，才能做到“ 疏而不漏 ”，法律上“ 疏 ”的基础是由技术优势构成的，技术上的“ 漏 ”是由法律来弥补的。信息安全的立法，只有容纳进了技术因素，法律才能适应技术的变化，具有一定的预见性和前瞻性，而不是拘泥于形势，“ 头痛医头，脚痛医脚 ”。过去在信息安全立法方面，我们的教训是法律与技术的结合点，总是拘泥于技术的具体形式。实践证明，需要技术解决的问题未必能通过法律来解决，需要通过法律来解决的问题，也未必能通过技术来解决。加拿大、澳大利亚等国家在技术上的水平与我国差不多，但这些国家在国家安全方面(政治领域)的压力要小，因而在互联网监管领域对国家安全事项的规制不是特别严格，我们未必能借鉴其监管经验。而在不涉及国家安全、政治事务而只涉及公共利益和私权利保障的领域，他们所面临的情况与我们相似，我们可以借鉴其成功经验。

对普遍的社会价值、文化价值有害的信息的监管

对于那些在互联网上传播的攻击社会制度、贬损我国民众普遍的社会价值、文化价值的信息、对青少年健康成长不利的信息、煽动种族歧视和种族仇恨、宗教歧视的信息等有害信息内容，除对国家安全、社会安全构成明显而现实的危险的信息内容外，基本上是在较长的期间内才能形成一定影响，其作用才能凸显。对于此类信息内容的监管应首先区分信息发布者的目的，针对不同的情况采取不同的监管措施。

对于不直接危害国家安全，却对普遍的社会价值、社会道德与文化价值有害的言论，即使是西方发达国家也不是采取听之任之的放任态度。但是，在不同国家的国内法律体制下，对此类信息内容监管的结果也并不理想。

从其他国家和地区对可能损害普遍的社会价值、文化价值或公共利益的有害信息内容的监管模式分析，主要有以下四种类型。

(1)互联网经营企业实行行业自治和自律，政府鼓励终端用户自愿使用有害信息过滤或隔离技术预防和抵制有害信息。采用这一模式的国家主要有加拿大和大部分西欧国家。在某种程度上讲，新西兰也实行这一制度，但新西兰的法律并没有明确规定，对传统媒体实行的分类、检查制度是否适用于互联网信息内容的监管。在这些国家或地区，与暴力、色情相关的内容及煽动种族仇恨和民族歧视的内容都是被禁止的。对于“ 青少年不宜的内容 ”则鼓励用户自愿使用在线技术来控制对相关信息内容的访问。

(2)对“ 少儿不宜的内容 ”等“ 严重损害普遍的社会价值、文化价值或公共利益的有害信息内容 ”的在线提供者进行刑事处罚(罚金或监禁)。美国以及澳大利亚的某些州有这样的司法倾向。但是，美国联邦和州都没有对“ 少儿不宜的内容 ”的信息提供者进行刑事制裁的相关法律规定，因此，对内容提供者进行处罚的理由是内容的违法性，而非“ 少儿不宜 ”。多数国家对种族仇视和儿童色情的内容加以限制，但都还没有严格到在互联网上限制“ 不适合儿童的资料 ”的程度。

(3)政府对损害普遍的社会价值、文化价值或公共利益的有害信息内容进行强制屏蔽、封堵、隔离。采用这一模式的国家有澳大利亚联邦、沙特阿拉伯、新加坡、阿拉伯联合酋长国和越南等。在印度，对于那些在用户上网过程中自动弹出的色情网站，有专门的软件工程师“ 对症下药 ”，设置相关屏蔽保护程序。

(4)政府禁止公众接入互联网或互联网用户必须注册或取得许可方可接入互联网，并且只能对部分经过政府事先审查的网页进行有限访问。采用这一模式的国家有朝鲜、缅甸等。

互联网传播或发布的损害个人合法权益的信息的法律规制

当互联网传播或发布的信息所损害的对象并非不特定公众，而是具体的个人(包括法人和非法人团体)时，应由受害人要求加害人或相关网络服务机构采取技术措施停止侵害、减少损失、消除影响，或提交相关记录，以便通过协商或诉讼的方式维护自身的合法权益。即使需要采取法律监管方式，也应由受害人自己选择是否提请有关部门予以救济，而不应由行政执法部门主动积极地使用国家强制力的措施进行监管。目前，在打击盗版活动等侵犯网络知识产权的不法行为方面，行政机关采取了较为主动、积极实施监管的态度，虽然对于维护市场秩序和保护知识产权权利人的合法利益起到了积极作用，但也消耗和占用了大量行政资源。从法理上讲，私人经济权利的保护应当以权利人主动积极为主，且法律规制应以司法规制而非行政规制为主。

必须强调的是，在法治条件下，信息安全的维护，需要国家、社会和个人共同参与，并非国家单方面的作为就可以实现。而行政监管也不是唯一的国家监管方式，司法介入同样也是国家监管的重要方式。鉴于政府资源和行政能力的有限性以及政府在现代社会的有限角色，政府不可能也不应当对所有涉及信息内容安全的领域都采取行政监管的措施，必须采取“ 有所为、有所不为 ”的原则。鉴于政府较之个人(或法人)，在维护国家利益和公共利益方面，具有更大的义务和更强的优势，而个人(或法人)则在维护私权益方面具有更强的意识、便利和优势，所以政府应当只对涉及国家利益和公共利益的信息内容安全事项进行行政监管，而将单纯涉及私权益(如并非政府掌

握的商业秘密和个人隐私)的信息内容安全保障事项交由商事主体和个人负责，一旦出现侵权行为，则由受害人通过司法途径或非诉讼争端解决机制予以解决，而不是通过直接的行政监管予以解决。