经济参考报/2013 年/4 月/23 日/第 008 版
思想 · 法眼

保护个人信息不是限制信息流动

中国社科院法学所研究员　陈欣新

保护个人信息不是为了限制个人信息的流动，而是要保证个人信息能够在合理、合法的状态下流动，保证符合信息主体同意的目的，保持信息的正确、有效和安全。

必须正确处理保护个人信息与表达自由这两个重要法律价值之间的平衡。

如果在保护个人信息的过程中，过度管制传媒表达，就会妨碍传媒业界社会责任的充分实现。

在实施互联网监管时，如何处理国家利益、公共利益与个人正当合法权益的平衡是一个重要的问题。

目前，通过法治途径保护网络信息已经成为社会共识。保护个人信息，关键在于必须正确处理保护个人信息与表达自由这两个重要法律价值之间的平衡，要在网络信息保护与传媒自由之间取得一种动态平衡。在互联网监管方式的使用方面，也应该按照不同性质的监管对象采用不同的监管机制。

保护个人信息旨在合理合法流动

网络信息保护的法律的直接目的之一是保护个人信息，经济合作与发展组织(O EC D)提出的个人信息保护八项原则，体现了保护网络个人信息的基本思路：

收集限制原则，个人信息的收集必须采取合理合法的手段，必须征得信息主体的同意；

数据质量原则，个人信息必须在利用目的范围内保持正确、完整及最新状态；

目的明确原则，个人信息收集目的要明确化，不能超范围利用；

使用限制原则，对个人信息资料的使用不得超出收集目的，不得随意提供给第三者；

安全保障原则，对个人信息的丢失、不当接触、破坏、利用、修改、公开等风险必须采取合理的安全保护措施；

公开原则，必须以方便的方法和人们容易理解的语言向社会公开有关个人信息保护的政策；

权利人参与原则，信息主体有权知道自身信息的所在位置，有权对自身信息提出质疑，有权对自身信息进行修改、完善、补充和删除；

责任原则，个人信息的管理者对个人信息的保管负全责。

这些个人信息的保护原则体现了对人的尊重和对个人信息的规范管理，在保护个人信息的同时，让个人信息能真正实现自身价值和更好地为公众服务。可见，个人信息的保护不是为了限制个人信息的流动，而是要对个人信息的流动进行正规的管理和规范，以保证能符合信息主体同意的目的，保持信息的正确、有效和安全。保证个人信息能够在合理、合法的状态下流动。

“ 保护个人信息 ” 不能危害表达自由

但是，如果保护个人信息的立法中伴随着某种程度上过度管制传媒表达活动的色彩，就会给传媒自由带来某种危险，就会妨碍传媒业界社会责任的充分实现。

日本的《个人信息保护法》就曾因具有间接管制传媒的作用，而招致强烈的批评。该法要求新闻机构在公开报道前应把个人信息加以 “ 适当处理 ”。具体来讲，即要求新闻机构应从当事人那里直接取得信息，或者在信息发布之前将其内容公开给该当事人，使其能有更正的机会等等。如果把这样的原则机械性地用于新闻媒体，就会导致新闻媒体不能揭发那些政治人物和公职人员的贪污腐败和丑闻。因为政治人物和公职人员不可能主动向新闻机构提供有关自己贪污腐败或丑闻的准确信息，甚至不可能同意媒体公开报道相关的信息。

我国当前国情条件下，媒体监督特别是网络监督在遏制公权力滥用和反腐败方面具有不寻常

但却必不可少的作用，因此，不宜对媒体监督公职人员的报道施加过于严格的个人信息保护义务，因为公职人员尤其是领导干部不论基于党纪还是国法，都有接受人民较高水平的监督的义务。

问题实际上并不在于“保护个人信息的基本原则”本身，而在于在适用过程中必须正确处理保护个人信息与表达自由这两个重要法律价值之间的平衡。从保障表达自由的观点来看，新闻媒体在监督公职人员尤其是政治人物时，应被免除从事个人信息处理业务的企事业单位所承担的一般性法定义务。应引入“恶意判断”的责任原则，即除非媒体在披露有关公职人员尤其是政治人物的个人信息时具有恶意，否则，不承担法律责任。并且应实行举证责任倒置原则，由相关公职人员尤其是政治人物承担证明媒体“存在恶意”的举证责任，而不是由媒体承担证明自己“不存在恶意”的举证责任。

对不同的监管对象可采用分类监管机制

从目前的情况看，加强网络信息保护的关键之处是完善依法监管。在互联网监管方式的使用方面，可以考虑按照不同性质的监管对象采用不同的监管机制。

我国目前许多大型 ISP、IA P 和 ICP 是国有单位，对于这些单位可以考虑在行政监管之外，充分利用其上级主管部门或主办机构的基于所有权人地位的监督作用。某些上级主管部门或主办机构较之行政监管机关，在信息内容监管方面具有更多优势。

对基于商业运作目的，以传播、利用个人信息或可能发布有害信息获取商业利益的商业网站，可以通过法律规范、操作规范、行业自律准则、行政许可的方式来进行监管和预防。同时辅以事后追惩的制度，使不当发布和传播个人信息或有害信息的商业网站在经济上受到严厉惩治，提高其运营成本，从而使经营性网站基于经济利益的考虑，自觉遵守监管措施，主动抵制个人信息或有害信息的非法传播和不当利用。

而对于仅以发布有害信息为目的并不以取得现实的经济利益为目的的网站，由于这类网站根本不可能向行政机关申请许可，因此行政许可及其它行政审批手段根本不会对此类网站形成实质影响。

考虑到对有害信息内容实施即时监管的成本过高，而且监管的效果也不免挂一漏万，从成本效益分析的角度来看，对于此类信息内容亦不能仅以监管 IC P 为既定目标，监管的对象应以 ISP 或 IA P(互联网接入服务提供商)为重点。要求其消除影响、提交记录，便于监管机关、有关部门和被侵权人对信息发布者进行事后的追惩。

目前监管信息内容的方法主要有：事先监管的许可、审批、备案；事中监管的技术控制；事后制裁的追究法律责任。

事先监管的许可、审批、备案是传统的信息内容监管方式，主要是通过许可证、资质认证认可、重要信息报备等措施，将不符合法律规定的主体排斥在合法运营范围之外，达到维护信息内容安全的目的。事中监管的技术控制是最为体现互联网时代特点的监管方法。各国使用的互联网信息内容监管的技术手段主要有网络实时监控、信息过滤、网页屏蔽、信息拦截、网络临时管制等。事后制裁主要是通过依法追究不法行为人的法律责任，达到惩治已有违法、警示和预防未来违法的效果。

由于互联网具有极大的影响力和极快的信息蔓延速度，就使事中监管的价值变得极为重要。而高技术手段的使用和快速反应能力就成为各国在互联网监管中最为重视的因素。在“9·11”恐怖袭击发生后的几小时内，美国网站上所有与“政府”这一关键词相关的信息都被屏蔽了。在其后的很多天，甚至几个星期内所有层次的行政机构都不对外提供信息，并对政府机密进行了重新定义。

对互联网的监管要受法律限制

我们处理互联网监管问题时，如何处理国家利益、公共利益与个人正当合法权益的平衡的关系是一个重要的问题。

一些人士认为，“9·11”已经永远改变了美国政府信息透明的作法。在“9·11”事件发生后，

几个提供敏感信息的网站从网络上消失了，其中包括美国运输部的全国管网地图系统、环保署的风险管理计划网站及核能管理委员会的网站在内。

对于网络传播的与国家安全无关的其它有害信息内容，如对儿童有不良影响的网上色情信息等，美国也通过立法予以规制。美国曾通过“ C D A 法案 ”来限制色情内容在网络上的传播，但该法案受到了美国民权组织的挑战，他们在总统签署该法案的几个月内就向法院提起了一项违宪审查诉讼，并得到了联邦巡回上诉法院的支持。

与此同时，美国还存在着另一种现象，法律明确规定政府有义务向公众提供相关信息的情况下，政府会利用手中的自由裁量权，以相关文件仅供内部使用为由拒绝向申请人提供。实际上，美国的《信息自由法》(英文简写为“ FO IA ”)明文规定，除了法律明确规定不能向公众提供的信息外，相关政府部门应向申请人提供相关信息。此外，根据《电子政务法》的规定，除了《信息自由法》所规定的向公众提供相关信息的文本阅览外，各政府机关应开设专门的电子阅览室，向公众提供电子文本的信息或在线提供相关信息。

上述因素综合作用的结果就形成了政府事实上一般不直接对网络传播的内容进行管制，而是更多地依靠网络参与者的自律，以政府的管制作为补充和保障的信息内容规制体系。

在法治条件下，任何权利或权力都不是绝对的，管理者不具有不受限制的权力来监管网络中的用户。一些法律、内部规则和用户协议会使无视这些规定的网络管理者陷入民事纠纷或犯罪的困境。

在美国，如果网络管理者的网络监控行为是在政府的指导下运作的，则需要考虑美国联邦宪法《第四条修正案》。《第四条修正案》限制没有经过法官“ 第一类安全搜索 ”授权的政府代理机构搜索证据的活动，违反《第四条修正案》而获得的证据不能用于指控遭受非法搜索的人。个人参与者配置网络监控和监督用户时不需要担心违反《第四条修正案》，除非个人参与者是政府的代理。当然，只监督攻击者的活动的网络监控系统不会违反《第四条修正案》，但如果监督的范围超出了入侵者，对《第四条修正案》就不能掉以轻心。美国的上述经验对于我们处理互联网监管问题时考虑国家利益、公共利益与个人正当合法权益的平衡机制具有重要的借鉴价值。

在社会常态的一般情况下，对信息安全的监管必须使用常规的方法，一些带有极端性和严重限制私权利的互联网特别管制措施是禁止使用的。在紧急状态条件下，考虑到国家和社会根本利益正在或即将受到极其严重危害，监管效果要求较高，需要采取一些特别的互联网管制措施，并且特别管制措施实施的时间可能需要持续一段时间，直到紧急状态解除或导致实施特别措施的情况消失。在这一点上可以参考道路交通临时管制和紧急状态下交通管制的不同做法。