

顺应信息技术发展规律 推进信息安全立法进程

——访中国社会科学院法学研究所研究员陈欣新

本刊记者 李满意



陈欣新 法学博士，中国社会科学院法学研究所研究员，传媒法与信息法研究室主任。英国牛津大学访问学者。研究重点：人权理论、香港与内地法制协调、违宪审查、政府规制、传媒与信息法制建设。主要作品有《比较宪法研究》《行政处罚法》《信息自由与信息安全》《宪政之鉴》，参与撰写《人权百科全书》等。

记者：当前，信息安全问题越来越受到各国政府和社会各界的普遍关注。加强国家信息安全保障体系建设，既需要提升信息安全技术研发能力，也需要提升法律保障能力，您如何看待当前我国的网络信息安全立法及法律实施现状？

陈欣新：随着信息技术的飞速发展和互联网的普及，信息安全问题越来越严峻，已经上升到国家安全的高度。究其原因，一方面，网络已成为国家的重要基础设施和国计民生的命脉，各

行各业对信息技术和网络系统的依赖程度越来越高。网络一旦出现漏洞，或遭受攻击无法正常运行，许多重要系统都将陷入瘫痪状态，国家安全也因此受到不同程度损害。另一方面，从社会和公众的角度来看，信息安全已经不只是单纯影响到个体或某个群体，而是完成从量变到质变的过程，直接影响社会秩序的稳定运行，进而影响到国家安全。

维护信息安全，需要法律和技术双重保障。俗语“法网恢恢，疏而不漏”，而不是说“密而

不漏”。法网的“疏”需要技术优势作为支撑，技术保障能使法网“疏”但是不“漏”。一旦技术保障跟不上，法网就被迫变“密”。但法网“密不透风”，自由度将被消减。实际上，法律的“疏”是留给了“自由”，留给了社会的自治。

信息安全立法应考虑容纳技术因素，顺应技术发展的规律，这样法律才能适应技术的发展变化。否则，信息安全法尚未颁布实施，就可能落伍，无法适应社会需要。现在一些法律、法规刚一出台，社会上就反映其无法适应实际操作需要，很大程度上就在于这些法律、法规在创制阶段就脱离现实，或是没有为行业未来发展留余地，或是没有按照客观规律立法。互联网产业是不断发展的，涉及互联网的法律规定，还需及时根据社会和技术发展水平做出适当修改，不能指望制定一部法律或一个规则就能一劳永逸地解决问题。立法是国家意志的体现，但“意志论”不是绝对的，不是想立成什么样就立成什么样。如果违背了规律，在法律的实施阶段势必将会出现各种意想不到的问题。

当前，我国信息安全相关规定主要散见于宪法、法律以及各类行政法规、部门规章中，过于零散，不能构成一个完善的保护体系，无法起到应有的作用。这些规定在实施过程中，存在两个方面的问题：一是有的条文不能适应社会发展、技术发展的规律和需要，也不能适应国家安全发展的规律和需要；二是当社会出现新的行为和新的需要规制的对象时，相关法律条款跟不上，原来的法律没有为未来的发展留有余地。此外，由于信息安全问题具有一定的技术性，很多人在这些领域中知识相对欠缺，这种状况使得信息安全的宣传普及和实施也面临严峻挑战。

记者：自2012年年底，我国相继出台了《关于加强网络信息保护的决定》《信息安全技术公共及商用服务信息系统个人信息保护指南》，请您谈谈这些法规标准的制定背景及其对个人信息保护的意义。

陈欣新：近年来，我国高度重视信息安全问题，特别是信息安全立法和依法维护信息安全问题。根据我国的立法体制，如果没有上位法依据，规定就不能够超出规章所能够制定的范畴。因此，从这个意义上说，制定一部高位阶的、能够起到整合现有的法律规范，同时又为制定新的法律规范提供上位法依据和授权依据的规范性文件，尤为重要。

2012年12月28日，第十一届全国人民代表大会常务委员会第三十次会议通过了《关于加强网络信息保护的决定》，明确了网络信息保护的相关规则。该《决定》法律位阶较高，一定程度上解决了网络信息保护没有上位依据的问题。当然，保护个人网络信息安全，仅有这一《决定》还不够，具体实施的下位法目前还处于创制和研讨的阶段。

2013年2月1日起，《信息安全技术公共及商用服务信息系统个人信息保护指南》开始实施。该《指南》从实际操作角度，对于在公共及商用服务系统中如何保护个人信息给出了具体的规则指导，把很多问题细化了。比如，《指南》将个人信息分为“个人一般信息”和“个人敏感信息”，并提出“默许同意”和“明示同意”的概念。对于个人一般信息的处理，可以建立在“默许同意”的基础上，即如果客户或者个人信息主体没有提出来不同意使用，那么就推定他同意。对于个人敏感信息，则需要建立在明示同意的基础上，在收集和利用之前，必须首先获得个人信息主体明确的授权。对不满16周岁的未成年人，要通过其监护主体获取未成年人个人信息。当然，对于《指南》的相关规则也存在一些异议，有观点认为所有信息都应做不同意推定。但是，一个有缺陷的规则和没有规则相比，还是有规则要好一些。规则制定出来，可以进一步完善它；没有规则，则直接影响行业发展及权益保护。

《决定》和《指南》的意义在于，《决定》从高位阶给予个人信息保护较高法律依据，同

时,通过《指南》的方式,提供规范指引,相关行业可按规范指引开展业务工作。实际上,越到具体操作阶段,相关规则的指引性,可能会强过强制性。不仅是信息安全立法,包括其他行业立法,在技术尚未发展成熟的时候,如果过多地使用强制标准,效果未必好。信息安全的维护,如能采用强制性规范和指引性规范相结合,先提供指引性规范,不断完善,待其成熟后再作为强制性标准推行,这样做会更符合实际发展规律。

记者:虽然《宪法》《刑法》《国家安全法》《电子签名法》等法律法规从刑事、民事及行政责任角度对信息安全保护进行了规范,但我国仍缺乏一部高位阶的信息安全法,您认为信息安全法难以出台的主要原因是什么?党的十八大报告提出“健全信息安全保障体系”,您认为这对该项立法有何指导意义?您对该法的立法内容有哪些建议?

陈欣新:信息安全立法及实施,和其他领域立法的不同之处主要在于,其涉及的立法领域和法律责任种类较多。近年来,信息安全立法呼声越来越高,但一直未能出台,个人认为,主要有以下三方面原因。

一是与互联网发展速度有关。主要发达国家在互联网时代之前,电子化程度已经很高,积累了很多经验,信息安全立法有一个自然发展的过程。而我国互联网的使用起步晚,从20世纪90年代中期,才逐渐开始走向普及化,虽然在短时间实现了技术的迅猛发展,但也造成立法步伐很难在很短的时间内适应技术快速发展。信息技术发展越快,对于法律如何适应技术发展要求的顾虑就越大。

二是与信息安全领域囊括的问题范围广泛有关。信息安全既包括信息技术安全问题,也包括信息内容安全问题。信息从产生、发出、传播、接收,再到反馈,是一个闭合回路,每一环节都存在安全问题。从保密工作角度,要着力解决有效控制信息源。而在信息宣传领域,诸如危害青少年、危害国家安全的消息,当不能完全控制信

息源时,就要考虑传播和接收环节的信息安全问题。此外,政府信息公开与保密也是相对应的。这些都属于信息安全概念的范畴,信息安全立法规范方向多,规范和规制手段又不一样,而且有时看法也存在很大分歧,导致综合性的信息安全立法难以出台。

三是和社会发展程度有关。当前,我国多种所有制并存,多元化利益主体并存。在整个信息安全领域中,也存在基于不同利益出发点的主体和集团,因而在同一个法律规范上主张不可能完全一致,甚至会出现完全对立的主张,主要矛盾难以调和。例如对于个人信息,从商务角度来讲,提供商务服务的主体,希望尽可能多采用同意推定;而对个人主体则更倾向于不同意推定,双方的利益出发点不一样。

上述问题集中起来,造成信息安全法较难创制和出台。对于这种情况,虽然可以理解,但仍需着力解决。中央一直高度关注信息安全立法,党的十八大明确提出健全信息安全保障体系,不断完善法律体系是构建信息安全保障体系的重要组成部分。个人认为,信息安全保障体系是目标主导型的,最终要达到的目标是信息安全有保障,从立法到执法,到守法,再到法律监督都应提供保障。健全信息安全保障体系应强调人人有责,每一利益主体维护自身信息安全的同时还应维护其他利益主体的信息安全,限制其他利益主体权利的同时也要限制自己的自由。

信息安全立法涉及信息产生、发送、传递、接收、反馈各个领域的内容,我认为应坚持原则与具体规则相协调,强制性规范与选择性规范、指引性规范相结合,技术标准与法律规则相结合。不同层级的立法工作要适应本层级的规范,高位阶的法律不能太局限于具体技术性规范问题,具体的法律规范不能写得太原则竟至无法操作。

此外,个人建议可将信息内容安全和技术安全分离,分别立法。信息内容安全是控制信息源、传播、接收,与从技术角度保护个人信息没

有关系,分别立法将有利于技术领域的综合立法先行出台。例如,新的保密法已于2010年5月颁布实施,虽然保密法实施办法还未出台,但对于控制泄露国家秘密已经有了法律保障。对于信息传播的管制,涉密信息部分已通过保密法规范了,其余的有害信息在别的法律规定中亦一样可以规制,与信息传递的媒质没有关系。技术角度主要解决网络电子化条件下如何实施信息保护的问题,和传播媒质方式高度相关,分别处理技术和内容的法律规制,有利于矛盾分解。应该摒弃“搭车立法”的思路,把遵循不同规律的问题按不同方式进行法律创制工作。信息内容安全立法和技术安全立法差异较大,信息安全法难以出台的主要矛盾都是在内容安全部分,在技术领域就是服务提供者和享受者,与具体的意识形态没有关系,如能分开立法,可集中力量研究信息安全保障立法,再辅以技术标准和相关指引性规范配合即可。

信息安全立法还应与国情相结合,我国的技术水平、法制水平和主要发达国家还有差距,应在充分借鉴其他国家经验的基础上,与自己的国情结合,制定信息安全法律法规。

记者:网络窃密、制造和传播病毒等形式的网络犯罪属于全球性问题,且具有明显的跨国性。我国有关部门一直致力于与各国执法机构加强合作,联合打击跨国网络犯罪,请问主要有哪些国际法规对跨国合作打击网络犯罪提供法律支撑?

陈欣新:互联网在某种程度上已经超越了传统主权国家的边界限制,具有明显的跨国特性,网络违法行为并非我国独有,其在发达国家和互联网产业发展较快的国家势头也很迅猛。我国互联网主管部门、互联网犯罪侦查部门一直致力于国际合作,但问题是,目前在国际公约和国际条约中,还没有专门针对网络犯罪或联合打击网络犯罪的公约,虽然我们与一些国家签有司法协助

协议,但其本身更侧重程序性规定,没有对实体规范加以规定,这在一定程度上影响了打击跨国网络犯罪的工作效率。对于与意识形态无关的、国际公认的网络犯罪,可能将来国际社会会有一些共识,是可以期待制定公约的。

对于打击网络犯罪,个人认为,一方面我们要重视国际合作;但另外一方面又不能过于依赖国际合作,只能在主权范围内做好这方面工作。一些国际社会公认的属于网络犯罪的行为,我们和其他国家合作开展打击工作较为顺利推进。但在一些与国情和意识形态有关的领域,国际合作打击网络犯罪则存在一定难度。例如,制造传播病毒,是公认的网络犯罪,但如果将制造传播病毒作为窃密手段,在某些特殊情况下,问题会很复杂。所以说,打铁还需自身硬,当务之急,还是要加强我国自身的信息安全保障能力建设。

记者:构建健康、规范、有序的网络生态环境,也有赖于公民法制观念和防护意识的提升,您对网络信息安全法规的宣传普及工作有哪些建议?

陈欣新:在法治条件下,构建健康有序的网络环境,有赖于整体国民法治观念和信息安全防护意识的增强,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。

当前,我国整体法治水平还不够高,信息安全领域法治观念和防护意识水平从根本上受制于法治发展整体水平。在这种情况下,可以分步有重点地做好信息安全法规宣传普及工作。建议在面向社会进行信息安全法规宣教工作时,首先做好网络使用频率相对较高的单位及公民的信息安全法律法规普及工作。这些单位和人员使用网络频率高,在专业领域的知识较多,他们的法治观念提升了,更有利于提升国民整体防护意识。带动作用不容忽视,会起到事半功倍的效果。**END**

顺应信息技术发展规律 推进信息安全立法进程 / P 6

随着互联网的发展，信息安全问题日益凸显，并上升到国家安全高度。维护网络信息安全，离不开法律和技术的双重保障。围绕当前我国网络信息安全立法及法律实施现状、信息安全法难以出台的主要原因、信息安全法的立法内容、信息安全法规的宣传普及等问题，本刊记者采访了中国社会科学院法学所研究员陈欣新。

特别策划：“棱镜门”事件曝光美国网络监控计划 / P 10

自2013年6月6日起，英国《卫报》和美国《华盛顿邮报》陆续披露了一系列美国国家安全局绝密级文件，涉及美国网络监控政策及项目。泄密者是美国国家安全局合同商雇员、前中央情报局技术助理爱德华·斯诺登。在这些文件中，由于“棱镜”计划涉及面最广、影响最大，故本次事件又被称为“棱镜门”事件。本期《特别策划》栏目对国外有关媒体披露的美国网络监控计划涉密文件进行了翻译整理，以期对读者了解美国网络监控系统有所帮助。

电磁屏蔽机柜在涉密信息系统中的应用研究 / P 32

随着分级保护工作的逐步深入，越来越多的涉密信息系统开始使用屏蔽机柜作为电磁泄漏发射防护手段。本文从屏蔽效能、散热性能和机柜结构等方面，分析和研究了电磁屏蔽机柜的选型问题。

关于加强涉密人员保密教育培训工作的思考 / P 60

本文以涉密人员保密教育培训为研究对象，梳理近年来涉密人员保密教育培训工作的开展情况，分析当前存在的问题，提出解决的具体方法，并对未来发展趋势做出预判，力图使下一步工作更加具有计划性和前瞻性，促进涉密人员保密教育培训工作水平进一步提高。