·法律园地

社会分层视野下网络安全立法体系的构建

黎 慈[1,2]

（1.华中师范大学，湖北 武汉 430070；2.江苏警官学院，江苏 南京 210012）

摘要：《网络安全法》为网络安全治理提供了原则性规范指引，其配套法律法规调控网络社会的效度取决于调整对象的科学划分。网络社会分层结构的客观存在，为网络安全法律规范的调整对象类型化提供了衡量标准。从网络社会分层的视角来看，网络所有者和运营者、网络服务提供者、网络使用者在网络生态环境中分别位居基础层、中间层以及信息流通层，理应承担不同的网络安全维护义务与责任。因此，基于总体国家安全与法治的要求，我国互联网安全立法应当重视网络社会各分层主体的法律地位，构建起涵盖保护关键信息基础设施安全、调整网络服务提供者行为、约束网络信息流通层活动主体行为的法律规范体系。

关键词：社会分层；网络安全立法；法治

中图分类号：D262.13；D920.0 文献标识码：A 文章编号：1003-8477（2019）05-0125-07

DOI:10.13660/j.cnki.42-1112/c.015088

《网络安全法》的颁布和实施，标志着网络空间安全管理法治化时代的到来，成为化解网络公共领域风险的一柄法律利器。然而，网络安全法作为一部基础性法律，其功能在于为网络安全管理提供原则性指导，而具体问题的解决还依赖相关法律法规的配套运行。因此，要推进网络空间法治化发展进程，增强网络安全法律规范的可操作性，应当尽快出台相关配套规定，落实《网络安全法》顶层设计的立法目的和立法宗旨。那么，应当出台哪些相关配套规定？配套规定如何与作为基本法的《网络安全法》实现有效衔接？配套规定之间如何防范立法交叉与重复？上述问题解决的根本途径在于，以《网络安全法》为统领，构建规范边界明晰的互联网安全立法体系。与一国宏观法律体系的科学构建类似，互联网安全立法体系的架构首先必须合理划分法律规范的调整对象，以保障各类法律规范既能全面覆盖又能和谐相处。为此，本文拟借助社会分层理论，观察并厘定网络安全法律规范的主要调整对

作者简介：黎慈（1975—），女，华中师范大学政治与国际关系学院博士研究生，江苏警官学院法律系教授。

基金项目：江苏高校哲学社会科学重点项目“大学生网络安全法治意识的养成教育研究”（2017ZDIXM041）；江苏省研究生教育教学改革课题“警务硕士课堂教学场景模拟实训研究——以《警察公共关系学》课程为例”（JGLX19_101）；江苏高校哲学社会科学重点建设基地“总体国家安全与法治研究中心”项目（2018ZDJD-B007）；江苏省“333”高层次人才工程资助项目；“十三五”江苏省重点建设学科建设工程资助项目；江苏高校品牌专业建设工程资助项目（TAPP）；江苏高校优势学科建设工程资助项目（PAPD）。

象类型，探寻互联网安全立法体系的科学构建。

一、网络社会分层：传统社会分层的延续与变革

（一）传统社会分层依赖于成员的经济与政治地位。

社会分层（social stratification）作为社会学范畴的一个重要理论，经历了古典社会分层理论、现代社会分层理论、当代社会分层理论三个历史阶段。[1](p12)各阶段社会分层理论基于提出者所处的时代背景、立场不同，采用的划分标准有别，学界对其名称的界定自然也各不相同，如马克思的阶级划分理论、韦伯的三位一体分层理论、帕累托的精英循环理论等，但从这些理论的划分标准来看，主要涉及社会成员的经济地位和政治地位。

一是以社会成员的经济地位作为社会分层的根本标准。根据马克思的阶级理论，“阶级的划分归根到底是由生产力发展水平决定的”，“生产资料占有关系是阶级划分的首要标准”。资产阶级与无产阶级形成的原因在于劳动和分工的存在，“其中一个阶级占有全部生产工具和生活资料，另一个阶级只有出卖自己的劳动才能生存。”[2](p221)韦伯的三位一体分层理论的首要标准也是经济标准，即以社会成员拥有的财富多少为标准，他认为：“有产和无产，便是所有阶级处境的基本范畴。”[3](p138)帕累托的精英循环理论同样认为，处于社会上层的精英，其应有的“高度”要义之一，便是以其拥有的财富作为判断成功与否的客观标准。

二是以社会成员的政治地位作为社会分层的重要标准。马克思认为，阶级作为一个社会集团，不仅反映了社会成员的经济地位差别，也反映出由经济差别决定的政治地位和社会地位的差异。此外，他在分析法国分散的小农不能形成一个阶级的原因时指出，小农尽管具有形成一个阶级的经济条件，但“由于他们的利益的同一性并不使他们彼此间……形成任何一种政治组织，所以他们就没有形成一个阶级。”[4](p693)在韦伯的三位一体分层理论中，政治标准即指权力，他认为权力就是“处于社会关系之中的行动者即使在遇到反对的情况下也能实现自己的意志的可能性。”[5](p158)帕累托将精英阶层分为统治精英阶层和非统治精英阶层，他曾就此打了一个比方：“一位著名棋手肯定属于精英阶级；但无疑他作为棋手的功绩并未为其开拓通向政界之路；因此，他不属于执政的精英阶级”，[6](p77)并认为非统治精英阶层没有能力掌握政治权力用以统治整个社会，因此在政治上依附于统治精英。

（二）网络社会分层是对传统社会分层的延续与变革。

互联网使人类社会在经济、政治、文化、社会生活等方面发生了巨大的变化，对于这种信息技术带来的新型社会形态，曼纽尔·卡斯特将其界定为“网络社会”。与传统社会的人们处于不同层级一样，网络空间的网民基于占有的网络资源不同，所享有网络话语权存在差异，由此产生了网络社会的分层问题。对此，国内一些学者给予了关注，但大多认为基于信息技术为基础的网络社会发生了翻天覆地的变化，传统社会以财富标准为象征的经济标准和以权力为象征的政治标准在网络社会已失去其作为社会分层标准的根本前提。[7](p44)与此同时，他们认为网民是网络社会分层的对象，并根据不同标准划分了网络社会的不同层次，如有学者通过分析网民占有的信息资源多寡、技术能力高低、表达能力强弱等方面得出，网络社会是不平等的，并由此将网络社会大致分为决策层与平民层：决策层是信息的主要创造者、发布者，如软件设计师、硬件制造商以及影响巨大的黑客；平民层则指一般网民。[8](p78)对此，我们认为网络空间的社会分层的确发生了明显变革，但它在一定程度上仍然存有对传统社会分层的延续。

一方面，网络社会分层是传统社会分层的延续。传统社会分层的经济因素和政治因素在网络社会分层中依然发挥着重要作用。其一，经济因素影响网民对网络资源的占有。社会成员从事网络活动首先必须拥有手机、电脑等上网设备，同时必须拥有时间。第41次中国互联网发展状况统计报告显示，月收入在中高等水平（2001—5000元/月）的网民群体占比最高，达到39%，而广大的农民、农民工以及城市失业人员，或每天忙于生计，或不具备上网条件，他们在网络社会分层中处于底层。其二，政治因素对网络活动具有重大影响。这是因为，政治权力能够借助法律法规或是网络政策等，引导网络活动的走向，如我国近几年通过立法治理网络谣言及其取得的成效便是很好的例证。

另一方面，网络社会分层在传统社会分层基础上发生了重大变革。基于互联网技术，网民在互联网空间的活动能力及其影响程度不再完全受控于

经济实力和政治地位，拥有网络话语权的网民即人们所称的博主、大V、意见领袖等形成互联网空间的精英阶层，并且表现出强大的感召力和组织力。同时，我们还要意识到，网民只是维系网络空间的部分力量，网络的所有者、运营者和网络服务的提供者同样是互联网存在与发展的重要力量，并且三者之间相互联系，形成一定的层级关系。具体而言，网络的所有者和运营者是基础层，他们掌握着底层的关键信息基础设施，为防止关键信息基础设施遭到攻击导致国家核心利益以及公共利益受损，应当承担起维护网络安全的法律责任；网络服务的提供者是中间层，他们作为信息发布的平台与通道，在网络所有者和运营者与网络用户之间、网络用户与网络用户之间发挥着桥梁作用，促进了网络信息的流动，需要对网络信息安全尽到注意义务，即在合理限度内保护他人免遭因第三人不正当使用网络平台带来的侵害；网络使用者是网络信息流通层的主要活动者，主要以网民形式出现，他们既可以是信息的发布者，也可以是信息的接受者，其在网络空间发布的信息直接关系网络安全。

二、网络社会分层对网络安全立法体系构建的指引

网络安全法是调整社会关系的规范，它通过规范网络组织和个体的行为实现对社会关系的调整。可见，网络安全法的调整对象仍然是特定的社会关系，但基于网络社会活动主体的复杂多变性，这种“特定的社会关系”必然是众多组织和个人间结成的复杂关系网络。对此，《网络安全法》第2条根据不同主体在互联网空间发挥的作用及其行为方式，整体上规定了本法的调整对象，即“在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。”由此可见，网络安全法律规范的调整对象至少包括两个层面：一是从事网络建设、网络运营、网络维护、网络使用的组织和个人与网络安全监督管理者之间的关系；二是从事网络建设、网络运营、网络维护、网络使用的组织与个人之间的关系。同时，《网络安全法》第8条规定的网络安全监督管理者涉及国家网信部门、国务院电信主管部门、公安部门以及其他有关机关，这些监督管理部门之间的职责范围及其相互协调关系，也应当成为网络安全法调整对象的重要组成部分。网络安全法调整对象的复杂性，决定着网络安全法律规范体系的构建必须遵循分层设计的原则。如果不实行分层设计或者分层不合理，不仅会因为相关立法机构相互意见的不统一造成配套立法的难产，而且会导致相关配套法律法规因为相互交叉重复甚至相互冲突而降低实施效果。究其原因，主要是忽视了法律调整对象的属性差异对相应法律原则、管理对象以及调控方式的不同要求。

（一）调整对象差异决定配套法规侧重不同的法律原则。

法律原则是法律规范产生的基础，对法律规范的产生和法律概念的界定具有指导意义。每个法律部门的所有同类法律规范都需要遵循共同的法律原则，但该法律部门中每一部法律法规因调整对象存在差异，在遵循法律原则方面的侧重点也会有所不同。《网络安全法》已明确的法律原则主要包括网络空间主权原则、责权利相统一原则、网络安全与发展并重原则以及共同治理原则，但因为相关配套法律法规各自不同的调整对象，各网络活动主体享有的法律权利和需要承担的法律责任差异，在具体法律规则的创制方面必然需要不同的法律原则予以指导。否则，法律规则在适用过程中容易引发社会争议。例如，《消费者权益保护法》第44条规定：“网络交易平台提供者明知或者应知销售者或者服务者利用其平台侵害消费者合法权益，未采取必要措施的，依法与该销售者或者服务者承担连带责任”；《食品安全法》也规定，消费者合法权益因通过网络平台购买食品受到损害时，网络食品交易第三方平台“应当与食品经营者承担连带责任”；《广告法》第64条则规定互联网信息服务提供者“明知或者应知广告活动违法不予制止的”，由工商行政管理部门没收违法所得，并处以罚款，甚至可以由有关部门责令其停止相关业务。上述规定在实施中引发了业界的广泛批评，原因在于对网络服务提供商予以规制的这些法律规则没有遵循避风港原则，[9](p31)让互联网企业承担了本应由政府承担的责任，这势必会影响网络的正常发展，不符合网络安全法应当遵循的网络安全与发展并重原则。

（二）调整对象差异决定配套法规调整不同的管理对象。

网络安全法的调整对象是在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理等方面产生的社会关系，相应地，其管理

对象主要包括关键信息基础设施所有者和经营者、网络服务提供商、网络信息发布者和传播者、从事网络安全监督管理的政府部门。上述管理对象对互联网的存在与发展所起的作用不同，在维护网络安全方面承担的法律责任明显存在差异，如果在同一部配套法律法规中同时规定关键信息基础设施的保护、网络服务提供商的规范、网络信息流通的规制，势必会产生两方面的不良后果：一方面在于，将不同管理对象规定在一部法律法规中，会因立法技术难度过大，导致配套法规的难产。例如，《信息安全条例》于2008年便被列入了国务院立法计划，然而直到现在仍没能出台。另一方面在于，即便制定了相关法律法规，基于在同一部法律中兼顾调整不同管理对象进行的妥协容让，极有可能与其他立法部门制定的相关法律法规间发生冲突，从而导致可操作性缺乏，以至影响立法的实施效果。

（三）调整对象差异决定配套法规采用不同的调控方式。

法律对社会关系的调控是通过立法给管理对象设定相应的权利和义务来实现的。管理对象类型不同，其享有的权利和应当履行的义务必定有别，也就意味着法律应当采用不同的调控方式。就网络安全法律规范体系而言，其管理的对象包括关键信息基础设施所有者、网络服务提供商、网络信息流通层活动主体等多方面，基于各自对维护网络安全的作用不同，亦应当设定不同的权利义务加以调控。其一，基于关键信息基础设施的战略性和基础性的地位，其往往成为大国间网络安全博弈的焦点，也因为其关涉国家核心利益，容易被恶意攻击，因此需要重点保护，这种保护不仅需要明确关键信息基础设施的所有者和运营者的法律责任，同时需要明确政府职能部门承担的保护责任。其二，基于网络服务提供商在互联网运营中的作用是提供通路，为互联网用户接入网络服务，助使用户与网络连线，故既应当明确其维护网络安全的法律责任，同时又要注意法律责任的设定应当适度，防止他们因为成长空间受过度挤压，从而对中国互联网发展产生负面影响。其三，对于网络信息流通层的组织和个人，网络安全法律规范在设定法律责任时，既要规制他们破坏网络安全的违法犯罪行为，又要防止压缩他们参与政治、沟通交流等活动的行动空间，维护其应当享有的网络言论自由。

三、网络社会分层视野下网络安全立法体系的构建

由于网络关键信息基础设施的所有者和运营者、网络服务提供者、网络使用者在网络生态环境中分别位居基础层、中间层以及信息流通层，理应承担不同的网络安全维护义务与责任。因此，我们需要区分这些不同类型的调整对象，有针对性地设置不同的法律原则、管理对象以及调控方式，促成配套法律法规的科学设计，最终实现网络安全立法体系的有效构建。

（一）构建关键信息基础设施安全保护的规范体系。

随着网络空间不安全因素的增多，关键信息基础设施受到的威胁持续强化。对此，《网络安全法》对关键信息基础设施的安全保护给予了高度重视，以专节形式明确了“关键信息基础设施的运行安全”，并授权国务院制定其具体范围和安全保护办法。随后，国家互联网信息办公室会同相关部门起草了《关键信息基础设施安全保护条例（征求意见稿）》，并于2017年7月向社会公开征求意见。从社会各界的反映来看，争议颇多，主要涉及法律定位和保护理念、保护范围、保护机制、保护责任等诸多方面。[10](p19)借鉴美国、日本、俄罗斯等网络发达国家的立法经验，基于关键信息基础设施安全保护的实际需要，我们认为，关键信息基础设施安全保护规范体系的内容至少应当包括：

一是明确关键信息基础设施的具体范围。一方面，确定关键信息基础设施的具体范围应当遵循两个基本原则：其一，坚持国际准则和国内实际相结合的原则，其原因在于互联网具有国际性，但同时我国关键信息基础设施涉及的领域又有自身的特点；其二，坚持忠于现状与注重发展的原则，因为新领域的出现或一些非关键领域向关键领域的转变会导致关键信息基础设施具体范围的变化。另一方面，确定关键信息基础设施的认定标准及其程序。认定标准可以通过识别指南的方式予以明确，但要注意作为设定者认识能力上的局限性以及互联网发展的快速性，因此应保证其具有开放性。认定程序可以采取主动识别和依申报识别两种方式：前者是指由国家行业主管或监管部门按照识别指南主动认定，并以法律文书方式通知运营者；后者是指关键信息基础设施的网络运营者向国家行业

主管或监管部门申报，经有关部门识别后予以认定。

二是规定关键信息基础设施运营者的安全保护义务和权利。一方面，关键信息基础设施运营者的安全保护义务包括：在规章制度层面，负有制定内部安全管理制度、操作规程的义务；在岗位人员保障层面，负有确定安全管理负责人的义务，对该负责人与关键岗位人员进行安全背景审查的义务，对从业人员进行网络安全教育、技术培训以及技能考核等方面的义务；在网络安全监管层面，负有采取技术措施对网络运行状态进行日常监测的义务，以及负有防范计算机病毒和网络攻击、网络侵入等危害网络安全的义务等。另一方面，关键信息基础设施运营者享有的权利应当包括：履行安全保护义务时能获得监管部门支持和协助的权利，被处罚前享有陈述权、申辩权、请求听证权，被处罚后享有申诉权、申请行政复议权以及提起行政诉讼等行政救济权。

三是规定关键信息基础设施安全保护监管机构及其职责分工。根据关键信息基础设施安全保护的实际需要，结合当前政府职能部门的职责范围，明确承担关键信息基础设施安全保护的监管部门，并且进行职责上的合理分工。

四是规定关键信息基础设施安全保护的程序。即明确当关键信息基础设施安全事件发生后，相关监管部门以及关键信息基础设施的运营者开展工作应当遵循的步骤、顺序、方式和时限等程序性要素。

五是规定违反关键信息基础设施安全保护规定应当承担的法律责任。既包括关键信息基础设施的运营者没有依法履行义务应当承担的行政责任、刑事责任，也包括监管部门违反法定职责规定时，其主要负责人、直接责任人员应当承担的行政责任、刑事责任。

（二）构建调整网络服务提供者行为的规范体系。

根据《网络安全法》第76条规定，网络服务提供者属于网络运营者的组成部分。《网络安全法》要求网络服务提供者承担维护网络安全的法律义务与责任，具有法理基础和实践意义。其一，符合收益风险对称原则。网络服务提供者在为网络用户提供资讯服务或者发布广告服务的活动中取得收益，具有营利性质。根据收益风险对称原则，网络服务提供者既然是利益的获得者，理应对网络服务相关联的网络安全风险负有防范义务。其二，符合网络安全共同治理原则。网络服务提供者掌握着先进的技术、拥有从事网络活动的专业人才，更容易了解网络空间的态势、预见网络公共领域有可能发生的安全风险，同时也更有能力采取措施降低甚至消除网络空间潜在的安全风险。但《网络安全法》作为基本法只做了原则性规定，还需完善健全配套法律法规，科学合理设定网络服务提供者的义务与责任，才能更好发挥网络服务提供者在网络安全治理中的作用。

一是明确调整网络服务提供者行为的法律规范体系的形式架构。从网络运行的实践来看，不同类型的网络服务提供者所服务的领域和内容存在差异，因此，调整他们行为的法律规范体系既需要整体上的设计，也需要微观上的类型化规定。就整体设计而言，应当在《网络安全法》的统率下，形成以《信息网络传播权保护条例》《网络安全等级保护条例》《网络产品和服务安全审查办法》等为主体的配套法律法规体系；就微观层面而言，考虑到各种类型网络服务提供者在网络空间发挥的作用不同，应当针对其所从事的专门领域活动分别立法，如已经出台的《互联网信息服务管理办法》《互联网直播服务管理规定》《互联网论坛社区服务管理规定》分别针对互联网信息服务提供者、互联网新闻信息直播业务中的服务提供者、互联网论坛社区服务提供者维护网络安全的法律义务和责任做了专门性规定，这为制定调整其他类型网络服务提供者行为的法律规范提供了借鉴。此外，还应完善《刑法》及其司法解释、《侵权责任法》等法律规范，进一步明晰网络服务提供者因违反《网络安全法》应当承担的刑事责任和民事责任。

二是确定调整网络服务提供者行为的法律规范体系的内容架构。网络服务提供者为网络信息的流转提供信道，因此，如何科学设置其权利和义务，直接关系网络安全的维护和网络社会的发展。网络服务提供者承担的义务主要应当包括：其一，风险存在时负有采取补救措施并报告的义务。即在提供网络服务过程中，发现有安全漏洞的风险时，网络服务提供者负有采取补救措施的义务，同时应当及时告知用户并向其主管部门报告。其二，

信息网络安全管理义务。主要包括:网络服务应当符合国家的强制性标准;不得设置恶意程序;不得在规定或约定期限内随意终止提供安全服务。其三,对网络用户信息应当规范收集、使用的义务。具有收集用户信息功能的网络服务提供者,应当向用户明示并取得同意;不得篡改、毁损、泄露所收集的用户的个人信息;不得以其他非法方式获取用户的个人信息;不得非法出售或者非法向他人提供用户的个人信息。在网络服务提供者享有的权利方面,主要应当包括:其一,网络使用规则的制定权。《网络安全法》对网络服务提供者的定位是,在一定程度上与网络用户之间存在着管理与被管理的关系,如要求用户在入网时提供真实身份信息,发现用户发布或者传输的信息属于法律法规禁止的范围时,有权立即停止传输该信息并予以删除。为了行使上述管理权,网络服务提供者有权在法律框架下,根据自身提供服务的具体情形,针对网络用户制定相关的使用规则。其二,网络服务合同的订立权。网络服务提供者在不违背现行法律规定与法律精神、不违反社会道德和伦理的前提下,对合同格式条款享有拟定权,并有权与网络用户签订相关合同。三是网络案件中的表达权和获得救济权。主要包括:享有陈述权、申辩权;在受到责令停产停业、较大数额的罚款、吊销相关许可证或营业执照等行政处罚前,享有要求实施处罚的机关举办听证会的权利;对行政处罚决定不服的,享有申请行政复议、提起行政诉讼的权利;对于因行政处罚、刑事处罚违反法律规定使其在财产权、人身权方面受到损害的,有权请求国家赔偿。

(三)构建约束网络信息流通层活动主体行为的规范体系。

网络信息流通层的活动主体除了发布、传播信息的互联网平台外,还包括数量持续增长的网络用户。第43次《中国互联网络发展状况统计报告》显示,截至2018年12月,我国网民规模达8.29亿,互联网普及率达到59.6%。[11]互联网的快速发展,让网民拥有了前所未有的表达权、参与权和监督权,然而,自由一旦被滥用,信息流通领域便会泥沙俱下,导致不实信息、网络谣言的盛行,网络黄赌毒、涉枪以及教唆犯罪等各种有害信息的肆意传播则会危及社会公共秩序和公共安全利益。因此,在依法保障网络自由的同时,还必须遵循《网络安全法》的立法宗旨和原则,针对网络流通层的信息安全保障构建配套法律法规体系。

一是构建治理网络攻击、网络入侵、网络窃密行为的法规体系。网络攻击、网络入侵、网络窃密等违法犯罪行为时有发生,严重威胁我国网络信息系统的安全。在网络攻击方面,行为人利用木马程式、电子邮件、黑客软件、安全漏洞等方式的攻击层出不穷,并且攻击者使用的工具越来越复杂、自动化程度越来越强、防火墙的渗透率越来越高。在网络入侵方面,入侵者运用编写和调试计算机程序的技巧,非法进入他人账户访问并获取隐私数据。在网络窃密方面,行为人(多为境外间谍情报机关)通过网络技术渗入我国一些涉密领域,窃取我国政治、军事、经济、科技等领域的国家秘密。对此,《网络安全法》第27条规定,"任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动。"上述三种行为都是利用网络技术对网络系统实施破坏,故立法者在设计调整网络流通层活动主体行为的法律规范体系时,应将其归为一类网络违法犯罪行为进行规制。

二是构建治理散布传播有害信息行为的法规体系。《网络安全法》实施以来,在党和政府的领导下,社会各界积极参与共同治理,网络有害信息的防治工作取得了明显进步。但是一些网络用户基于谋取经济利益、博取他人眼球、发泄私愤等,在网络上发布传播有害信息的情况依然不容忽视。数据显示,2018年5月、6月、12月全国各级网络举报部门受理的有效举报分别为744.2万件、[12]801.5万件、[13]672.7万件。[14]究其缘由,尽管《网络安全法》规定任何个人和组织应当对其使用网络的行为负责,发送的电子信息"不得含有法律、行政法规禁止发布或者传输的信息"。但《网络安全法》毕竟只是宏观上的规定,并没有明确:何为"有害信息"?其范围是什么?对发布传播有害信息的行为如何处罚?要解决这些问题,尚需进一步构建相关配套法律法规体系。

三是构建治理侵犯公民个人信息行为的法规体系。近年来,使用黑客软件窃取信息出售、通过QQ群交换并出售信息,以及设网站查询开房记录牟利等非法窃取、出售公民个人信息的案件屡屡发生。2009年2月至2017年12月间,全国法院新收

侵犯公民个人信息刑事案件3086起，审结2826起，生效判决人数4942人。[15](p10)此外，第43次《中国互联网络发展状况统计报告》显示，2018年有49.2%的网民遇到过网络安全问题，其中属于遇到个人信息泄露的比例高达27.3%。[11]上述数据表明，当前个人信息泄露的情形依然十分严重。为有效保护公民个人信息，《网络安全法》第44条已明确规定，“任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息”。尽管已经有《刑法》《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规与《网络安全法》共同为公民个人信息提供立法保障，但上述法律法规仍然存在着诸如受保护的个人信息范围不一致、偏重于刑事责任的追究、忽视事前防范管理等问题。要解决这些问题，亟须在完善上述法律法规的同时，适时出台《个人信息安全保护法》，以形成治理侵犯公民个人信息行为的法规体系。

四、结语

没有网络安全就没有国家安全。[16]就网络安全的保障而言，法治是最可靠的手段。“法治应包含两重意义：已成立的法律获得普遍的服从；而大家所服从的法律又应该本身是制订得良好的法律。”[17](p199)《网络安全法》的颁布与实施为我国网络安全治理奠定了法治基础，作为提供原则性规范指引的基本法，尚需要针对网络安全专门领域的立法以及相关立法与之配套。无论是从法理上还是从网络安全维护的实践层面来看，对网络社会分层结构的正确认识，有助于实现网络法律规范调整对象的类型化，促进《网络安全法》与配套法律法规之间、各配套法律法规之间的和谐相处、互为补充，共同构建科学有效的网络安全立法体系，为提升网络安全治理的社会化、法治化、智能化、专业化水平打下牢实的基础。

参考文献：

[1]李春玲.社会分层理论[M].北京：中国社会科学出版社，2008.

[2]中共中央马恩列斯著作编译局.马克思恩格斯全集：第6卷[M].北京：人民出版社，1961.

[3][英]弗兰克·帕金，马克斯·韦伯[M].刘东，谢维和，译.成都：四川人民出版社，1987.

[4]中共中央著作编译局.马克思恩格斯选集：第1卷[M].北京:人民出版社，1997.

[5]王思斌.社会学教程[M].北京:北京大学出版社，2016.

[6]徐小龙.帕累托的精英理论评析[J].理论观察，2007，(5).

[7]周启瑞.网络社会分层研究[D].长沙：湖南师范大学.2007.

[8]黄哲.网络社会分层与地位不平等[J].云南民族大学学报(哲学社会科学版)，2004，(3).

[9]周汉华.论互联网法[J].中国法学，2015，(3).

[10]《网络空间研究》编辑部.《关键信息基础设施安全保护条例（征求意见稿）》各方意见综述[J].网络空间研究，2017，(7).

[11]中共中央网络安全和信息化委员会办公室.CNNIC发布第43次《中国互联网络发展状况统计报告》[EB/OL].http://www.cac.gov.cn/2019-02/28/c_1124175686.htm，2019-02-28.

[12]中国互联网违法和不良信息举报中心.2018年5月全国网络举报受理情况[EB/OL].http://www.12377.cn/txt/2018-06/29/content_40402447.htm，2018-06-29.

[13]中国互联网违法和不良信息举报中心.6月份全国网络违法和不良信息有效举报801.5万件[EB/OL].http://www.gxjubao.org/html/2018/gzdt_0814/991.html，2018-08-14.

[14]国家网信办举报中心.2018年12月全国网络举报受理情况[EB/OL].http://www.12377.cn/txt/2019-01/17/content_40646438.htm，2019-01-17.

[15]喻海.侵犯公民个人信息罪的司法适用态势与争议焦点探析[J].法律适用，2018，(7).

[16]宋心蕊.没有网络安全就没有国家安全——三论学习贯彻习近平总书记全国网信工作会议重要讲话[N].光明日报，2018-04-24(3).

[17][古希腊]亚里士多德.政治学[M].吴寿彭，译.北京:商务印书馆，1996.

责任编辑　王　京