美国网络安全信息共享立法及对我国的启示

The Legislation of Cybersecurity Information Sharing in the United States and Its Enlightenment to China

刘金瑞

LIU Jin-rui

【摘　要】　网络安全信息共享已成为各国网络安全立法的重点议题。美国通过一系列政策和行政命令确立了信息共享的基本框架，并于 2015 年通过了《网络安全信息共享法》。该法规定的主要内容包括：联邦政府的网络安全信息共享；非联邦主体的网络安全信息共享；规定私主体的责任豁免以鼓励信息共享；隐私、自由和私权利的保护；限制政府所获网络安全信息的用途；联邦机构向国会定期报告制度。在借鉴美国立法经验的基础上，本文对我国未来立法提出如下建议：尽快建构网络安全信息共享的法治框架；确立网络安全信息共享的公私合作机制；规定相应的责任豁免制度以激励信息共享；平衡维护网络安全与保护私人权利的关系；限定政府所获网络安全信息的特定用途。

【关键词】　网络安全信息共享　网络安全法　美国立法

【中图分类号】DF49　【文献标识码】A　【文章编号】2095－9206（2017）02－0022－09

Abstract: Cybersecurity information sharing has been the core issue of cybersecurity legislation all over the world. The United States has established the basic legal framework of cybersecurity information sharing through a series of policies and orders, and finally passed the Cybersecurity Information Sharing Act (CISA) in 2015. CISA provides: cybersecurity information sharing by federal agencies; cybersecurity information sharing by non-federal entities; immunity from liabilities to encourage information sharing; protection of privacy and civil liberties; limitations on federal use of information shared pursuant to CISA; report to congress on implementation. Based on these experiences, the proposals for legislation regarding to information sharing in our country are as follows: establishing the legal framework of cybersecurity information sharing quickly; setting up a mechanism for cybersecurity information sharing among private-sector and government entities; providing according immunity from liabilities to promote sharing; balancing cybersecurity safeguard and private rights protection; limiting the governmental use of information obtained from sharing.

Key words: Cybersecurity information sharing　Cybersecurity law　Cybersecurity legislation of United States

[收稿日期]　2016－12－30

[作者简介]　刘金瑞，男，1987 年 10 月生，中国法学会法治研究所助理研究员，法学博士，研究方向为网络法、信息法和民法。

[基金项目]　国家社会科学基金特别委托项目“大数据时代依法治国战略”（项目编号：15@ZH012）子课题“大数据时代的数据立法研究”；中国法学会 2016 年度研究课题“我国关键基础设施保护立法研究”[项目编号：CLS（2016）D44]。

近年来，随着网络攻击和网络威胁等愈演愈烈，各国纷纷开始重视并加强网络安全立法，如何使公共部门和私营部门更好地应对网络安全威胁成为全球共同面临的挑战。各国立法中的一个重要共识是，及时交换共享网络安全信息是预防和充分应对网络安全事件的重要举措，网络安全信息共享包括私营部门之间的共享、政府部门之间的共享以及私营部门和政府部门之间的共享三个方面。我国 2016 年 11 月通过的《网络安全法》第 39 条明确规定，对于关键信息基础设施，国家网信部门应当统筹协调有关部门，“促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享”。

但该规定比较原则和简单，并没有规定网络安全信息共享的具体负责机构和实现机制，如何构建我国网络安全信息共享制度成为贯彻《网络安全法》、确保我国网络安全亟待研究的重大问题。作为全球网络信息技术最发达的国家，美国很早就开始研究制定网络安全信息共享的政策立法，并于 2015 年 12 月正式通过了美国《网络安全信息共享法》，这对我国相关制度的构建具有重要的借鉴意义。本文着重介绍和分析美国网络安全信息共享立法的最新进展，在此基础上得出建立我国网络安全信息共享制度的有益启示。

一、美国网络安全信息共享立法的历程和框架

美国早在克林顿政府时期就开始制定网络安全信息共享的政策和立法。1998 年 5 月，克林顿签署颁布《第 63 号总统决策指令》（PDD－63），规定联邦调查局内部的“国家关键基础设施保护中心”（National Infrastructure Protection Center，NIPC）维持政府和私营部门之间相关信息的流通和共享；与之相对，规定私营行业建立信息共享和分析中心（Information Sharing and Analysis Center，ISAC），负责收集、分析和共享其成员间的安全事件信息和应对信息，促成政府和私营行业之间的信息交换。这一设想最后发展成每个行业都有其自身的信息共享和分析中心。相较于关键基础设施保护行业协作委员会（sector coordinating council），ISAC 是 24 小时、365 天全天候运行的，该中心负责通报、分析和共享设施运营者的安全事件报告和来自政府的网络安全威胁信息。

美国在“9·11”事件之后，于 2002 年通过了《国土安全法》，成立了国土安全部。虽然 PDD－63 将 ISAC 设想成交换关键基础设施信息最主要的渠道，但国土安全部还是依据自身的授权发展出了一系列其他的信息交换系统和机制，主要包括设立“关键基础设施保护行政通知服务处”（Infrastructure Protection Executive Notification Service，ENS），该部门直接联系国土安全部和主要产业公司的首席执行官，ENS 负责向合作伙伴警示关键技术设施安全事件、发布警告产品和组织电话会议；运营“关键基础设施警告网络”（Critical Infrastructure Warning Network，CWIN），该网络不依靠公共交换电话网和互联网，为国土安全部与其他联邦、州和地方政府机构、私营行业和国际机构提供安全通信。

国土安全部还开发了国土安全信息网络（Homeland Security Information Network，HSIN），最初是作为联邦、州和地方层级政府执法机构交流和分析威胁信息的主要通信网络。现在 HSIN 提供 50 个州、5 个领地、50 个城市以及国土安全部的国家行动中心（National Operations Center）的实时连接。HSIN 现在正扩展到包含每个关键基础设施行

业（称为 HSIN-CI），作为关键基础设施保护伙伴关系模式的一部分。除了行业协作协会，美国计算机应急中心（US-CERT）〔1〕也接受安全事件报告，公布最新的计算机漏洞威胁信息以及特定安全事件应对信息，也负责国家网络警报系统（National Cyber Alert System），任何组织或者个人都可以订阅这一系统的通报信息。

此外，《国土安全法》还界定了“信息共享和分析组织”（Information Sharing and Analysis Organizations，ISAO），其是指“以收集、分析、交流或者披露关键基础设施信息为目的，公共部门或私营行业组织建立或雇用的正式或非正式组织”，“以有助于保护、检测、减轻或者恢复关键基础设施损害所造成的影响”。〔2〕可以发现，PDD－63 建立的 ISAC 是行业导向的，而 ISAO 没有此种要求。

奥巴马政府成立之后，积极推进网络安全的综合性立法，最主要内容就是关键基础设施保护和网络安全信息共享。但因为争议较大，相关立法设想在国会一直无法通过，奥巴马政府转而通过行政命令继续推进网络安全信息共享。2013 年 2 月，《第 13636 号行政命令》（E. O. 13636）〔3〕要求将“增强网络安全服务”项目推广至所有关键基础设施相关部门，面向私营公司制定推广自愿性信息共享计划。2015 年 2 月，《第 13691 号行政命令》（E. O. 13691）〔4〕要求国土安全部长支持信息共享和分析组织（ISAO）的发展，以促进网络安全信息分享。

虽然通过一系列行政命令建立了网络安全信息共享的基本框架，但因为限于总统行政权力有限，行政命令无法创设新的机构，也无法规定鼓励企业共享网络安全信息的责任豁免制度，奥巴马从第二任期开始继续推进相关国会立法。仅第 114 届国会，就提出了 H. R. 234、H. R. 1560、H. R. 1731、S. 456 和 S. 754 等五部法案，这些法案经过了参议院和众议院的数次审议和多次修改。2015 年 10 月 27 日，美国参议院以 74 票赞成、21 票反对的表决结果，通过了《网络安全信息共享法案》（Cybersecurity Information Sharing Act，CISA）。2015 年 12 月 28 日，奥巴马总统签署了包含该法案的 2016 综合预算法，《网络安全信息共享法》（CISA）正式生效。

二、美国《网络安全信息共享法》的主要内容

《网络安全信息共享法》（CISA）〔5〕是美国关于网络安全信息共享的第一部综合性立法，也是奥巴马政府最重要的网络安全综合性立法成果。该法授权政府机构、企业以及公众之间可以在法定条件和程序下共享网络安全信息，并将网络安全信息界分为“网络威胁指标”（cyber threat indicator）和“防御措施”（defensive measure）两类信息。

所谓的“网络威胁指标”是指描述或识别以下情形的必要信息：（1）恶意侦查，包括看起来是为了收集与网络安全威胁或安全漏洞相关的技术信息的通信流量异常；（2）突

〔1〕 承担了国家关键基础设施保护中心（NIPC）的大部分职能。

〔2〕 Critical Infrastructure Information Act of 2002, 6 U. S. C. 131 (5).

〔3〕 See Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Federal Register 78, No. 33, February 19, 2013, pp. 11737～11744.

〔4〕 See E. O. 13691: Promoting Private Sector Cybersecurity Information Sharing, Federal Register, Vol. 80, No. 34, February 20, 2015, pp. 9347～9353.

〔5〕 See Cybersecurity Information Sharing Act of 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754, last visited on Jan. 8, 2017.

破安全措施或者探侦安全漏洞的方法；（3）安全漏洞，包括看起来显示安全漏洞存在的异常活动；（4）造成合法访问信息系统或信息系统所存储、处理或传输信息的用户不经意使得安全措施失效或安全漏洞被探侦的方法；（5）恶意的网络命令或控制；（6）安全事件所造成的实际或可能的损害，包括特定安全威胁所泄露信息的描述；（7）其他并非法律禁止披露的网络安全威胁的属性；（8）上述情形的任意组合。〔6〕

所谓的“防御措施”是指检测、防止或减轻信息系统或信息系统所存储、处理或传输信息的已知或者可能的网络安全威胁或安全漏洞的行为、设备、程序、签名、技术或其他措施。但应排除破坏、瘫痪、提供未经授权访问或实质性危害信息系统或者信息系统数据的措施，只要这些系统或者数据不属于实施该措施的私主体、不属于向实施该措施的私主体授权提供同意或已经提供同意的其他主体或联邦主体。〔7〕CISA 围绕“网络威胁指标”和“防御措施”建立了美国网络安全信息共享的基本法治框架。

（一）规定了联邦政府的网络安全信息共享

CISA 授权联邦政府共享非机密的“网络威胁指标”和“防御措施”；授权不仅可以在政府机构间分享此种非机密的信息，也可以与企业和公众分享；机密的网络安全信息在政府机构之外的共享，仅限于具有适当安全资质的主体；要求联邦政府定期发布“网络安全最佳实践”，以帮助小型企业应对其面临的网络安全挑战。〔8〕

CISA 要求制定专门的程序来实现上述分享，这一程序要满足以下要求：（1）确保联邦政府有能力在满足保护机密信息的前提下，实现网络安全信息的实时分享；（2）最大可能地整合联邦机构、非联邦主体在信息共享方面已有的程序、角色和职责，这包括分行业的信息共享和分析中心（ISAC）；（3）对接收错误的或者违反 CISA 及其他法律要求的网络安全信息的主体，要建立及时通知程序；（4）要求联邦机构采取安全措施保护共享的网络安全信息不受未经授权的访问或获取；（5）要求联邦机构审查或者利用技术手段移除任何与网络安全没有直接关系的、在分享时知道是特定主体的个人信息或可以识别特定个人的信息；（6）对个人信息已明知或者确定被联邦机构违反 CISA 而共享的美国人〔9〕，要建立及时通知程序。〔10〕

（二）规定了非联邦主体的网络安全信息共享

CISA 授权非联邦主体为了网络安全目的（cybersecurity purposes）可以与联邦机构和其他非联邦主体共享“网络威胁指标”和“防御措施”。所谓的“网络安全目的”是指保护信息系统或者信息系统所存储、处理或传输的信息免受网络安全威胁或安全漏洞。〔11〕所谓的非联邦主体包括私主体、非联邦政府机关以及州、部落或地方政府。〔12〕这里的联邦机构包括了美国国防部（含国家安全局）、国家情报总监办公室、国土安全部、司法部等重要情报部门。

CISA 要求非联邦主体采取安全措施保护共享的网络安全信息不受未经授权的访问

〔6〕 See CISA, Sec. 102 (6).
〔7〕 See CISA, Sec. 102 (7).
〔8〕 See CISA, Sec. 103 (a).
〔9〕 此处的美国公民既包括美国公民，也包括依法获得永久居住权的外国人。
〔10〕 See CISA, Sec. 103 (b).
〔11〕 See CISA, Sec. 102 (4).
〔12〕 See CISA, Sec. 104 (c).

或获取，遵从关于这些信息合法使用或共享限制的规定，并且审查或者利用技术手段移除任何与网络安全没有直接关系的、在分享时知道是特定主体的个人信息或可以识别特定个人的信息。〔13〕

CISA 理顺了联邦政府接收网络安全信息的机制，规定国土安全部（DHS）应该发展和实施特定的能力和程序（capability and process）来实时接收非联邦主体分享的网络威胁指标和防御措施，并将这些网络安全信息在联邦机构之间通过信息系统自动共享。〔14〕这些程序包括自动指标共享程序（Automated Indicator Sharing，AIS）、电子邮件、网络表格等。不过，联邦机构和非联邦主体关于已经共享的网络安全信息的沟通，以及联邦监管机构与被监管主体关于网络威胁的沟通并不适用国土安全部的专用程序。〔15〕

国土安全部的信息共享程序，不是限制或禁止非联邦主体其他的向联邦机构合法披露网络安全信息的行为，这包括报告犯罪活动、参与联邦调查以及遵守其他法定或意定的合同要求。〔16〕

（三）规定私主体的责任豁免以鼓励信息共享

CISA 授权私主体可以监视信息系统和实施防御措施。为了网络安全目的（cybersecurity purposes），私主体可以监视其自身的信息系统、经其他主体授权或书面同意的其他非联邦主体和联邦机构的信息系统以及在这些信息系统中存储、处理或者传输的信息。〔17〕此外，CISA 也授权私主体为了网络安全目的可以对其自身的信息系统、经其他主体授权或书面同意的其他非联邦主体和联邦机构的信息系统实施防御措施。〔18〕

CISA 明确规定，私主体监视信息系统和信息、共享和接受网络安全信息，只要符合 CISA 的法定要求，就不会因此而承担法律责任。〔19〕

CISA 并非设定了网络安全信息共享的强制性义务，其规定不能解释为允许联邦机构：要求非联邦主体向联邦机构或非联邦主体提供信息；以非联邦主体向其或其他非联邦主体提供网络威胁指标，作为其与该非联邦主体共享网络威胁指标的条件，或者作为该非联邦主体获得联邦拨款、合同或采购的条件。任何私主体不会因选择不参加自愿的网络安全信息共享而承担法律责任。〔20〕

CISA 对于网络安全信息共享和网络安全协助规定了反垄断责任的豁免。两个或多个私主体，为了网络安全目的交换或提供网络威胁指标，提供防止、调查或减轻网络安全威胁的协助，并不构成对反垄断法的违反。〔21〕当然，CISA 并不允许联合定价、市场垄断等破坏市场竞争的行为。〔22〕

---

〔13〕 See CISA, Sec. 104 (d).
〔14〕 See CISA, Sec. 105 (c).
〔15〕 See CISA, Sec. 105 (c) (1) (B).
〔16〕 See CISA, Sec. 105 (c) (E).
〔17〕 See CISA, Sec. 104 (a).
〔18〕 See CISA, Sec. 104 (b).
〔19〕 See CISA, Sec. 106.
〔20〕 See CISA, Sec. 108 (h) (i).
〔21〕 See CISA, Sec. 104 (e).
〔22〕 See CISA, Sec. 108 (e).

（四）规定了隐私、自由和私权利的保护

根据上文所述，CISA 规定联邦机构和非联邦主体都要审查其所共享的网络安全信息中的个人信息，并移除与网络安全威胁没有直接关系的个人信息。除此之外，CISA 要求国土安全部长和司法部长联合制定隐私和公民自由保护指南，这一指南需要包括以下内容：（1）限制本法规定的联邦政府活动对隐私和公民自由的影响；（2）限制含有个人信息的网络威胁指标的接收、留存、适用以及传播，对相关网络威胁指标规定特定留存期限，对与本法授权使用无直接关系的信息，规定建立发现后及时移除程序；（3）采取安全措施保护含有个人信息的网络威胁指标不受未经授权的访问或获取，包括规定政府机构工作人员违反指南时的适当惩处；（4）对于已明知或者确定所共享的信息不构成网络安全指标的主体，要建立通知程序；（5）最大程度保护含有个人信息的网络威胁指标的秘密性，并且告知接收者只能在本法授权的目的下使用这些指标。[23]

CISA 明确规定，与联邦政府共享的网络安全信息，并非放弃其本身的法定特权和保护，包括商业秘密的保护；并不适用联邦、州和地方信息自由法公开披露的规定；并不适用行政法上单方面接触（ex parte communications）的限制；最初共享这些信息的非联邦主体的商业性、金融性和财产性信息仍受保护。[24]

（五）限制政府所获网络安全信息的用途

CISA 限制政府通过共享获得的网络安全信息的用途，以避免政府利用这些信息对分享主体造成不利。对于通过合法共享而获得的网络威胁指标和防御措施，联邦政府的披露、留存或者使用只限于以下情形：（1）网络安全目的；（2）识别网络安全威胁或者安全漏洞；（3）应对、防止或者减轻特定的死亡威胁、严重的人身或经济损害，包括恐怖主义行为或大规模杀伤性武器的使用；（4）应对、调查、追诉、防止或者减轻对未成年人的严重威胁，任何可能由（3）所列情形引发的犯罪行为，或者与欺诈、身份盗窃、间谍、审查或商业秘密保护相关的特定犯罪行为。[25]

对于通过合法共享而获得的网络威胁指标和防御措施，州、部落或地方政府不得用于监管[26]非联邦主体的合法行为或非联邦主体根据强制性标准而采取的行为。但是州、部落或地方政府在防止或减轻信息系统网络威胁的监管权范围内，可以将这些网络安全信息用于通报特定信息系统监管措施的进展或实施。[27]

（六）规定了联邦机构向国会定期报告制

CISA 规定了联邦主要机构向国会定期报告制度，以利于国会获知信息共享的成效和确保对政府活动的监督。要求报告的内容包括：信息共享措施的实施情况；信息共享政策、程序和指南的遵从情况；通过将个人数据从共享的信息中移除来保护个人隐私的情况，以及这些保护措施的充分性；美国所面临网络安全威胁的情况等。CISA 还规定了该法的“日落条款”，该法将于 2025 年 9 月 30 日停止适用，即该法的适用期限大概为十年。

根据 CISA，美国国土安全部会同有关部门制定了四个相关程序和指南。除了 2016

---

[23] See CISA, Sec. 105 (b).

[24] See CISA, Sec. 105 (d) (1) — (4).

[25] See CISA, Sec. 105 (d) (5).

[26] 包括采取强制措施。

[27] See CISA, Sec. 104 (d) (4) (C).

年 2 月制定的联邦政府向非联邦主体共享网络威胁信息的程序规定之外，还包括 2016 年 6 月 15 日发布的“非联邦主体向联邦机构共享网络威胁信息指南”、“联邦政府接收网络威胁信息程序”和“隐私和公民自由保护指南”。〔28〕

在美国，CISA 和类似网络安全信息共享立法引发的争议主要包括：（1）企业采取技术措施监控自身的网络设施和共享网络威胁信息等，可能违反《电子通信隐私法》（ECPA）等隐私权保护的法律规定〔29〕，CISA 对此虽然规定了企业责任豁免，但争议仍然存在。（2）规定豁免企业共享信息的法律责任，有两方面的争议：一方面私主体对这种豁免仍存在不信任，联邦机构可能以此作为不利于当事人的证据用于行政执法等；另一方面，责任豁免如涉及舍弃第三方私主体的合法权益，其正当性受到质疑。（3）共享信息可能会侵害企业的商业利益。类似商业秘密等商业信息，可能发生泄露而被竞争对手获取。因此，企业一般不愿与政府共享涉及商业利益的信息，此类立法的成效有限。（4）CISA 可能会便利政府监控项目的实施。2015 年 6 月，美国通过《美国自由法》，根据该法规定，美国国家安全局会逐步将大规模电话元数据收集项目转给电信公司，待有证据确认某人或某个组织有恐怖活动嫌疑时才可向电信公司索取相关数据。CISA 授权私主体可以监视信息系统及传输的信息，私主体可以主动与政府共享网络安全信息，这实际上为政府通过企业监控网络提供了可能的便利条件。

三、美国网络安全信息共享立法对我国的启示

虽然网络安全信息共享制度存在一定的争议，但鉴于其在实践中已被证明确实是维护网络安全的有效制度设计，我国《网络安全法》第 39 条也已明确规定要促进关键信息基础设施的网络安全信息共享，建议借鉴美国等国家在网络安全信息共享方面的立法经验，结合我国的具体国情，尽快立法确立我国网络安全信息共享制度。

（一）尽快建构网络安全信息共享的法治框架

《网络安全法》通过之后，作为重要配套规定的《关键信息基础设施安全保护条例》（以下简称“条例”）正在加紧制定，而促进网络安全信息共享，正是规定在《网络安全法》保护关键信息基础设施的部分。虽然网络安全信息共享制度不仅适用于关键信息基础设施，但建议抓住此次立法契机，在条例制定中确立我国网络安全信息共享制度的基本框架。

建议明确由国家网信部门负责统一领导协调我国网络安全信息共享工作，公安部、工信部等其他部委根据未来关键信息基础设施保护的分工来分别负责所主管行业领域的网络安全信息共享。网络安全信息共享法治的基本框架应该着重考虑以下问题：（1）所共享的网络安全信息的类型；（2）网络安全信息共享的主体；（3）网络安全信息共享的目的限定；（4）所共享的网络安全信息的分级；（5）网络安全信息共享的体制机制。

（二）确立网络安全信息共享的公私合作机制

为充分实现网络安全信息的交换共享，应该建立网络安全信息共享的政府企业合作

〔28〕 See DHS, DOJ Release 4 Final Guidance Documents on Cyber Threat Data Sharing, http://www.executivegov.com/2016/06/dhs-doj-release-4-final-guidance-documents-on-cyber-threat-data-sharing/, last visited on Jan. 8, 2016.

〔29〕 See Aaron J. Burstein, Amending the ECPA to Enable a Culture of Cybersecurity Research, *Harvard Journal of Law & Technology*, 2008, 167.

机制。在政府部门分工确定主管行业的基础上，鼓励引导各个行业领域成立自身的行业协作委员会，授权政府主管部门和相应的行业协作委员会建立公私合作伙伴关系。

公私合作伙伴关系的主要职能在于：私营部门通过这一机制反映自身面临的网络安全威胁，并协助主管部门制定行业网络安全信息共享计划；国家网信部门等国家机关通过这一机制广泛征求产业界的意见，在制定网络安全信息共享政策和标准等过程中，充分反映行业的最佳实践。

应该授权国家网信部门建立专门的网络安全信息共享国家中心，发展相应的信息交换技术和共享标准；授权网信部门推动建立政府内部、政府与行业之间的网络安全信息交换组织；定期公布行业的最佳实践，为中小企业网络安全信息共享提供建议指南。应该授权政府各主管部门根据网络安全信息的分级，积极发展多层次多渠道的网络安全信息交换和共享机制。

（三）规定相应的责任豁免制度以激励信息共享

虽然我国关键信息基础设施的具体保护范围有待进一步明晰，但建议对极其重要的关键信息基础设施规定强制性的监管义务和标准，此种强制性要求应包括网络安全信息报告和共享的义务。

为激励相应的主体尤其是私营主体主动与政府部门共享网络安全信息，建议规定相应的责任豁免制度，即规定企业在遵循法定强制标准和按照法定要求共享网络安全信息的情况下，减轻或免除因此而产生的法律责任。例如，对于遵守监管标准的关键基础设施运营者，可以考虑规定其信息系统被恶意攻击而导致大规模数据泄露时，可只向消费者承担补偿性赔偿责任，而非承担惩罚性赔偿责任。

为了提升企业发现网络安全漏洞的能力和打消其因分享信息而承担责任的顾虑，应授权私营主体监视其负责运营的网络信息系统以及系统内存储、处理和传输的数据，并规定不承担因此而产生的法律责任。两个或多个私主体，为了网络安全目的交换网络安全信息或提供相互协助，应规定一般不构成对反垄断法的违反。对于并未纳入强制监管范围的私营主体，其可自愿加入网络安全信息共享机制，只要其按法定要求共享相关信息，可以规定豁免其相应的法律责任。

（四）平衡维护网络安全与保护私人权利的关系

在网络安全信息共享中，应尤其重视对私人权利的保护。建议规定政府或其他主体保存、使用或者传播网络安全信息时，必须保护这些信息里任何可识别的个人信息不被未经授权地披露、处理或者使用。所共享的网络安全信息，应该移除或匿名化其中与网络安全威胁没有直接关系的个人信息；对于无法移除或匿名化的个人信息，应最大程度地确保其用于法定目的而不被泄露滥用，规定留存这些个人信息的合理期限。在含有个人信息的网络安全信息发生意外泄露事件时，应及时通知这些个人信息所涉及的权利主体。

建议规定与政府共享网络安全信息和政府使用网络安全信息时，不能侵害个人隐私、商业秘密和其他合法权益，规定这些信息不适用信息公开的披露义务，不适用行政法上单方面接触的限制，政府不得利用这些信息对自愿分享主体实施对其不利的监管措施。

（五）限定政府所获网络安全信息的特定用途

我国《网络安全法》第 30 条规定：“网信部门和有关部门在履行网络安全保护职责

中获取的信息，只能用于维护网络安全的需要，不得用于其他用途”，确定了政府履行网络安全保护职责所获信息用途特定的原则，所获得的相关信息只能用于维护网络安全的需要，此原则同样应适于网络安全信息共享领域。

建议进一步细化该原则性规定在网络安全信息共享领域的适用，借鉴美国 CISA 立法的相关条文，建议规定：对于通过合法共享而获得的网络安全信息，政府部门的披露、留存、处理或者使用只限于以下情形：（1）为了网络安全目的；（2）识别网络安全威胁或者网络安全漏洞；（3）应对、防止或者减轻对人民群众可能造成或已经造成的重大人身威胁和财产损害；（4）应对、调查、追诉、防止对未成年人的严重威胁，以及与国家安全、恐怖主义、电信诈骗、身份盗窃、间谍、商业秘密保护相关的特定犯罪行为。

参考文献

[1] Aaron J. Burstein. Amending the ECPA to Enable a Culture of Cybersecurity Research [J]. Harvard Journal of Law & Technology, 2008.

（责任编辑：于文豪　赵建蕊）

（上接第 10 页）

我国现有立法没有明确规定数据资产所有权的归属，笔者建议建立数据二元所有权，将数据分为基础数据和增值数据，两者确立不同的所有权。用户作为个人数据的提供者，拥有个人基础数据的所有权，这是数据资产权属的基本原则。数据处理者享有经个人数据主体同意基于基础数据进行加工编辑分析而产生的增值数据所有权，例如搜索引擎记录、电子商务记录、用户使用习惯、潜在用户群等数据信息。

参考文献

[1] 吴晓灵．谁的数据谁做主［EB/OL］．中国证券网，2016－07－10［2016－10－10］．http：//news.cnstock.com/news/sns_bwkx/201607/3838818.htm.
[2] 陈筱贞．大数据权属的类型化分析——大数据产业的逻辑起点［J］．法制与经济，2016（3）．
[3] 杨立新，陈小江．衍生数据是数据专有权的客体值的数据［N/OL］．中国社会科学报，2016－07－13［2016－09－05］．http：//ex.cssn.cn/bk/bkpd_qklm/bkpd_qkszh/201607/t20160713_3119714.shtml.
[4] 梅夏英，刘明．大数据时代下的个人信息范围界定［J］．中国法学，2014 年专刊．
[5] ［德］克里斯托弗·库勒．欧洲数据保护法：公司遵守与管制［M］．第二版．旷野，杨会永等译．北京：法律出版社，2008：99.
[6] 徐琦．大数据时代美国隐私保护之困［J］．中国传媒科技，2013（9）．
[7] 华劼．网络时代的隐私权［J］．河北法学，2008（6）．
[8] 谢远扬．信息论视角下个人信息的价值——兼对隐私权保护模式的检讨［J］．清华法学，2015（3）．
[9] 王融．关于大数据交易核心法律问题——数据所有权的探讨［J］．大数据，2015（2）．

（责任编辑：于文豪　赵建蕊）