评《网络安全法》对数据安全保护之得与失

洪延青 *
（四川大学网络空间安全研究院，四川 成都 610065）

[摘要] 近年来，我国政府高度重视数据在新常态中推动国家现代化建设的基础性、战略性作用，将“ 数据作为国家基础性战略资源 ”。本文研究《网络安全法》是否对数据（或大数据）做出了与其地位相匹配的安全保护规定，以实现“ 安全和发展要同步推进 ”的总体要求。总的来说，《网络安全法》对数据安全和个人数据保护给予了足够的关注，但从“ 数据作为国家基础性战略资源 ”这个层面来看，缺乏清醒意识，在制度设计上没有通盘考虑。

[关键词] 大数据；基础性战略资源；网络安全法；国家层面的数据保护
[中图分类号] D99　　[文献标识码] A　　[文章编号] 1009 - 8054(2017)01 - 0066 - 08

0 引言

近年来，我国政府高度重视数据在新常态中推动国家现代化建设的基础性、战略性作用。[1] 2015 年 9 月国务院印发的《促进大数据发展行动纲要》指出，“ 数据已成为国家基础性战略资源，大数据正日益对全球生产、流通、分配、消费活动以及经济运行机制、社会生活方式和国家治理能力产生重要影响。 ”2016 年 3 月发布的“ 十三五规划纲要 ”还专章提出“ 实施国家大数据战略 ”，明确我国将“ 把大数据作为基础性战略资源，全面实施促进大数据发展行动，加快推动数据资源共享开放和开发应用，助力产业转型升级和社会治理创新。 ”

2016 年 11 月 7 日，《网络安全法》正式对外颁布。如果说网络空间存在两大基本命题——网络安全和信息化的说法成立，《网络安全法》无疑具备我国网络空间“ 基本大法 ”的地位。回到文章开头，既然数据已被认定为“ 国家基础性战略资源 ”，那么《网络安全法》是否对数据（或大数据）[2] 做出了与其地位相匹配的安全保护规定，以实现“ 安全和发展要同步推进 ”的总体要求？对上述问题的探讨，构成了本文的主要内容。本文将首先提出一理论框架，勾勒出数据安全保护的三个层次，随后通过此理论框架检视《网络安全法》关于数据的主要规定，

* 基金项目：国家自然科学基金项目（面向国家战略传播的社会化媒体管理模式研究，课题编号 71573005）

1 在中央政府网站（http://www.gov.cn）的“ 政策 ”一栏中以“ 大数据 ”为关键词进行检索，一共返回 562 份国务院文件，覆盖各个领域。搜索时间为 2016 年 11 月 21 日。

2 网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。见《网络安全法》第 76 条。http://money.163.com/16/1108/15/C5C30SUD002580S6.html

以此得出《网络安全法》在数据安全保护方面的可取之处以及不足。

总的来说，《网络安全法》对数据安全和个人数据保护给予了足够的关注，但从“数据作为国家基础性战略资源”这个层面来看，该法缺乏对保护“国家基础性战略资源”的清醒意识，也就遑论制度设计上做到通盘考虑。此方面，当属《网络安全法》对数据安全保护的最大缺憾。

1 数据安全保护的三个层次

在《网络安全法》通过之际的新闻发布会上，全国人大法工委向外界表明：“制定网络安全法是落实国家总体安全观的重要举措”[1]。纵观《国家安全法》和《网络安全法》，主要保护的对象是整体层面（包括国家和社会）的安全利益和个人层面的安全利益。两部法律共同预设是，纯粹单个企业或组织的安全利益，无需国家直接运用公权力出面保护，现有的刑法、民商法等已经提供了足够的法律手段。[3]

沿着这样的思路出发，并结合《国家安全法》对数据提出的核心要求——安全可控[4]，可以构建出数据安全保护的三个阶梯式层次：首先是最基础的数据安全，其次是个人数据的保护，最高层次是国家层面的数据保护。

1.1 数据安全（data security）

数据安全可以认同为传统所说的信息安全（information security）。信息安全主要追求三性，即所谓的 CIA：保密性（confidentiality），指信息不被泄露给未经授权者的特性。完整性（integrity），指信息在存储或传输过程中保持未经授权不能改变的特性。可用性（availability），指信息可被授权者访问并使用的特性。[5] 也就是说，数据安全保障的是信息或信息系统免受未经授权的访问、使用、披露、破坏、修改、销毁等。[6] 如果用公式表示的话，数据安全 = 保密性 + 完整性 + 可用性。

1.2 个人数据保护（data protection）

回顾欧美在个人数据保护方面的立法和理论，最先出现的是隐私权的概念。隐私权可简

3 当然，当某企业被认定为关键信息基础设施的运营者，国家会将其纳入专门的保护体系，背后的原因也在于其“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益”。见《网络安全法》第 31 条。http://money.163.com/16/1108/15/C5C30SUD002580S6.html

4《国家安全法》第 25 条规定，国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。http://mt.sohu.com/20150706/n416241498.shtml

5 几乎任何一本信息安全教材都会在第一章中介绍 CIA 三性，并将这三性奉为信息安全的基本原则。见 Michael T. Goodrich and Roberto Tamassia, 2013, Introduction to Computer Security[M], Pearson, “Chapter 1: Introduction”.

6 见《网络安全法》总则部分第十条规定：“建设、运营网络或者通过网络提供服务，应当依照法律、法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。”该条文将网络数据的安全概括为完整性、保密性和可用性。http://money.163.com/16/1108/15/C5C30SUD002580S6.html

单理解为“别管我”（leave me alone），即个人私生活不被打扰的权利——“惟我独自享有的他人不得侵犯、干扰、触及的个人生活秘密、宁静的权利”。这是隐私权首次被提出时的经典理解。[7] 可以看出，隐私权是个人用于抵抗外界对其私人领域、私密信息窥探、侵犯的一种对内防御性机制。

随着信息技术的不断发展，人们不断认识到技术运用可能对个人带来各种风险。“个人数据自决理论”应运而生。该理论认为，为保障人格的自由发展，个人应当能自由地决定以何种方式实现人格发展；人格的形成，主要是在人与外界，特别是人与人的交往过程中实现，因此个体需要掌控对外自我披露或表现的程度，以便合理地维持自身与他人之间的人际关系，所以个人应当能自由、自主地决定如何使用个人数据。[2] 也就是说，个人数据保护赋予个人有权控制个人数据出于何种目的，面向何种对象范围，通过何种途径扩散和披露，亦即“个人依照法律控制自己的个人信息并决定是否被收集和利用的权利。”[3-4] 与单纯的、被动的防御性隐私权不同，以个人数据自决理论为基础的个人数据保护，是一种管理信息扩散和披露的机制，是一种面向外部的控制。[5] 如今，欧美在个人数据保护方面的立法，基本都超越了原先隐私权相对狭窄的内涵，转而以个人数据自决为理论基础。[8]

因此，个人数据保护主要在于“保护对个人数据的自主使用，要求他人不得以违反本人意愿的方式对个人数据进行处理。这是因为非经本人同意的数据处理会在社会中造成超出本人预期的结果，并对本人的人格发展造成不可预料的影响，使得本人人格塑造的结果偏离原本的预期。”[6]

行文至此，数据安全和个人数据保护的区别应当比较明显了。首先，没有数据安全，肯定没有个人数据保护，因为信息系统被攻破，数据遭到泄露，那数据保护要求的授权和控制扩散的机制就无从谈起。其次，即便实现了数据安全，并非一定做到了个人数据保护，例如数据很安全地存储在组织机构的信息系统中，但如果没有根据个人授权的范围来处理数据，那就违背了个人的数据保护权利。

这也是为什么在各国的个人数据保护立法中，数据安全部分的规定独立成章，但篇幅不大。以欧盟《通用数据保护条例》为例，立法的重心在于规定个人数据处理的基本原则[9]、数据主

7 1890 年美国法学家沃伦（Samuel D. Warren）和布兰戴斯（Louis D. Brandis）在《哈佛法律评论》上发表了题为《隐私权》（The Right to Privacy）的文章，首次提出隐私权概念。

8 有必要说明的是，欧洲严格区分个人数据保护和隐私两个概念。最明显的是在《欧盟基本权利宪章》（Charter of Fundamental Rights of the European Union）中，个人数据保护和隐私分属两个不同的权利，由第七条和第八条分别规定。欧洲最新的《通用数据保护条例》（GDPR）正文中没有用到隐私（privacy）这个词。而在美国立法中的隐私，除了最开始的“别管我”的概念，现在已经包含了“个人数据自决”的内涵。基本上可以认为，美国法律中的隐私概念等价于欧洲的个人数据保护概念。欧盟《通用数据保护条例》全文见 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

9 见欧盟《通用数据保护条例》第二章。基本原则包括“合法、公平、透明原则”、“目的拘束原则”、“数据最小化原则”、“准确性原则”、“存储限制原则”、“安全原则”、“问责原则”。欧盟《通用数据保护条例》全文见 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

体的权利[10]、数据控制者和处理者的义务配置等。保障数据安全仅仅是数据控制者和处理者众多义务之一，其更重要的义务是在数据的收集、存储、使用、共享、公开、跨境传输等环节中提供各种机制，使得数据主体得以行使其个人数据的“自决权”。例如充满争议的被遗忘权，是 GDPR 的一大创新。显然被遗忘权无关乎数据安全，而是赋予个人在特定情况下删除与其相关的个人数据的权利。

如果用公式来表达数据保护与数据安全之间的关系：个人数据保护 = 数据安全 + 个人数据自决权利 + 数据控制者等相关方满足个人数据自决权利的义务。

1.3 国家层面的数据保护

先看三个例子：据阿里巴巴 2016 年 11 月 2 日公布的 2016 年 9 月底的季度业绩显示，淘宝中国平台活跃买家高达 4.39 亿户。[7] 根据淘宝的隐私权政策，淘宝买家至少需要提交以下信息：姓名、性别、出生年月日、身份证号码、护照姓、护照名、护照号码、电话号码、电子邮箱、地址等。[8] 结合上述信息推知，阿里巴巴至少掌握了 4 亿我国公民的基础个人信息；而且借助于买家支付、收货等场景，其掌握的数据真实性甚至远超政府机关。单个公民的基础信息，无疑属于应当保护的个人信息。而一家私营企业汇聚了如此海量的公民个人信息库，其意义显然超脱了保护个人权益的层面。

第二个例子，2016 年 11 月俄罗斯知名网络安全厂商卡巴斯基公开抗议微软挤压第三方杀毒软件在 win10 操作系统的生存空间。[9] 表面上看来，该事件事关商业竞争。但更进一步考量，此事关乎国家安全。习近平总书记指出的，维护网络安全的关键在于“全天候全方位感知网络安全态势”[10]。因此，没有关于网络攻击、威胁来源、恶意地址等网络安全信息汇聚形成的安全大数据，也就根本无法做到“知己知彼”。微软排斥其他杀毒软件在其生态中的运作，客观上造成了独掌围绕其平台产生的安全大数据的结果。

第三个例子关乎住房空置率。据业内说法，空置率主要是指在统计时刻内没有被使用的住房除以全社会总住房所得出的空置率。而一旦“房屋空置率超过 5% 到 10%，房地产市场就出现较大问题了：房屋闲置比较严重，严重的供过于求，租金、房价要开始回落了”。而且，“住房空置率反映了社会资源浪费的问题。空置率高企反映了近些年来住房的投资属性被无限放大、夸大，而住房的居住属性被淡化、弱化的现实，其背后则反映了中国社会贫富严重分化的现实”。[11] 在我国，房价目前已是政府、百姓最关心的事情之一。因此，特别是在政府出台调控措施时，空置率很可能成为“对宏观经济调控政策、措施有较大影响的统计报告”，或者是“反映重大经济、社会问题的统计数据和统计报告”，属于国家机密的范畴。[11] 这也从侧面说明了为何一些地方统计部门曾就当地住

10 见欧盟《通用数据保护条例》第三章。权利主要包括知情权、查询权、纠错权、删除权（被遗忘权）、限制数据处理的权利、携带数据的权利、反对数据处理的权利、不受对个人有显著影响的、以自动化方式做出的决定的权利等。

11 见“国家统计局关于印发《经济工作中国家秘密及其密级具体范围的规定》中有关统计工作条目的解释的通知”，http://www.stats-fj.gov.cn/xxgk/fgwj/gfxwj/201211/t20121114_35768.htm

房空置情况做过调查。但对调查结果一直讳莫如深。[12] 过去，学者或民间力量为算得空置率只能通过“数黑灯”或入户抽样调查，现如今，只需结合海量的快递订单、水电运行等数据，在某一区域甚至全国范围内得出准确的房屋空置率并非难事。

这三个例子均表明，大数据对国家发展、治理、安全等方面越来越重要的意义。首先，阿里巴巴掌握的人口信息，规模和颗粒度均可比拟公安机关的国家人口基础信息库，准确性甚至更胜一筹。对国家来说，人口基础数据一旦泄露，很可能对国家安全造成严重危害[12]，因此国家人口基础信息库是作为涉密系统来建设和管理。所以，国家层面的数据保护首先应要求阿里保障其掌握的大数据的安全，也就是前文讲到的保密性、完整性、可用性。

其次，除数据安全之外，由于某些特定大数据对国家来说具有基础性、战略性的作用，国家应当具有一定的支配权。例如阿里巴巴汇聚的我国人口大数据，如果不将其划成涉密系统的话，则国家至少应当有权要求其不得对外共享、交易，并且不得向境外的组织、个人提供。对于第二个例子中，鉴于微软操作系统在我国用户数量庞大，国家应当有权要求微软不得独占，乃至于要求其与主管部门共享 win10 平台产生于我国境内的网络安全大数据。这不仅是因为海量用户产生的安全大数据对维护国家网络安全至关重要，失去此数据很可能造成威胁情报上的盲区；另一原因是如果说安全大数据可以用于提升安全水平，反过来，安全大数据当然可以很轻易地被恶意分子用于分析系统和空间的漏洞和脆弱性，找到攻击的切入点，因此有必要严格管控。

第三个例子中，淘宝、顺丰等企业显然拥有了海量的快递订单数据，而目前，支付宝、微信等应用集成了生活缴费功能，获得越来越多家庭的青睐。上述两类数据并非属于国家秘密。但两者一结合，很容易综合分析得出受严格保护的国家机密数据。大数据的发展，事实上导致了国家秘密和非国家秘密之间的界限不断在模糊。对于“单独或者与其他信息相结合分析后，有可能对国家安全和公共利益造成不利影响的数据”，本文称之为敏感数据。显然，敏感数据要比实践中认定的“国家秘密”范围要大得多。虽然将所有敏感数据都纳入“国家秘密”这样由公权力直接管控的强制机制内不是个现实的选项，但客观上确实存在强烈的需求来防范敏感数据被敌对国家或势力恶意使用（malicious use of big data），例如在关键时间节点恶意发布有关信息危害我国经济安全。

因此，国家层面的数据保护，除了数据安全及对数据一定的支配权外，还包括控制敏感数据可出于何种目的，面向何种对象范围，通过何种途径扩散和披露。综上，国家层面的数据保护 = 数据安全 + 数据支配权 + 防止敏感数据遭恶意使用对国家安全的威胁。

2 检视《网络安全法》关于数据的主要规定

《网络安全法》对数据的主要规定如表 1 所示。可以看到，数据安全保护的三个层次均

12 土耳其现有人口 8 千万。2016 年 4 月，土耳其国家警察部门所持有的将近 5 千万土耳其公民的个人信息遭泄漏，并在黑市上售卖。这些数据中包含土耳其前任、现任国家领导人的个人和亲属信息。见 Doug Olenick,“50 million exposed in Turkish data breach”, April 04, 2016, https://www.scmagazine.com/50-million-exposed-in-turkish-data-breach/article/528739/

有涉及，而且对数据安全和个人数据保护这两个维度着墨最多。首先，保障数据完整性、保密性和可用性的目标，在《网络安全法》的总则部分第 10 条就予以明确。第 21 条规定了网络运营者（包括关键信息基础设施的运营者）的安全保护义务，明确提出“ 防止网络数据泄露或者被窃取、篡改 ”是安全保护的目的之一。第 31 条更是从数据泄露可能造成的危害这个角度来界定关键信息基础设施的范围。第 27 条则是要求任何人不能提供专门用于窃取网络数据的程序和工具。

表 1 《网络安全法》对数据的主要规定

维度	条文
数据安全	第 10 条：“ 维护网络数据的完整性、保密性和可用性 ”
	第 21 条：“ 防止网络数据泄露或者被窃取、篡改 ”
	第 27 条：“ 不得提供专门用于……窃取网络数据等危害网络安全活动的程序、工具 ”
	第 31 条：“ 一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施 ”
个人数据保护	第 40 至 44 条
国家层面的数据保护	第 37 条：“ 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。 ”
	第 51 条：“ 国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作 ”
	第 52 条：“ 负责关键信息基础设施安全保护工作的部门，应当……按照规定报送网络安全监测预警信息 ”

其次，个人数据保护方面。《网络安全法》不仅继承了我国现有法律关于个人信息保护的主要条款内容，而且根据新的时代特征、发展需求和保护理念，创造性地增加了部分规定，例如第 40 条明确将收集和使用个人信息的网络运营者，设定为个人信息保护的责任主体；第 41 条增加了最少够用原则；第 42 条增设了个人信息共享的条件；第 43 条增加了个人在一定情形下删除、更正其个人数据的权利；第 44 条在法律层面首次给予个人信息交易一定的合法空间。可以说，五条关于个人数据的规定，注重保障个人对自己信息的自主权和支配权，且条条有创新，与现行国际规则及美欧个人信息保护方面的立法实现了理念上的接轨。[13]

相比前两个维度，《网络安全法》在国家层面的数据保护不成体系，给人“ 蜻蜓点水 ”的感觉。第 51、52 条对网络安全信息做出了规定，但规定的对象仅是国家网信部门、负责关键信息基础设施安全保护工作的部门，要求前者加强安全大数据的收集，要求后者及时报送安全信息。回到前文提到的卡巴斯基与微软的争端，第 51 条加强收集网络安全信息的要求是否意味着网信部门有权阻止微软打造其封闭的安全生态，强制要求其对包括国产杀毒软件在内的第三方安全厂商开放？如果不是，那该条是否意味着网信部门有权要求微软与国家共享其安全生态在境内产生的网络安全信息？上述问题的答案不得而知。

再看第 37 条，这是除数据安全层面外，《网络安全法》对关键信息基础设施上的数据的唯一规定。第 37 条要求关键信息基础设施的运营者在境内运营中收集和产生的个人信息和重要数据应当在境内存储。此举在一定程度上避免了对大量的个人信息和对国家的敏感数据留到

境外，但并不能完全杜绝像阿里巴巴这样掌握国家大量基础数据的公司，将数据转卖至境内具有外资背景的公司。这些公司无需将数据转移至国外，只要在境内完成分析，就能在不违反《网络安全法》的情况下，达到危害我国国家安全的目的。

3 总体评价

综上，《网络安全法》对数据的安全保护，主要着眼于两方面：一是要求各类组织切实承担起保障数据安全的责任，即保密性、完整性、可控性。二是保障个人对其个人信息的安全可控。但对于国家层面的数据保护，可以说《网络安全法》仅仅规定了关键信息基础设施上的重要数据应当留存本地。

据前文推导出的公式来看，如果将数据真正当成“基础性战略资源”，则国家层面的数据保护至少包含了三项主要内容：数据安全、数据支配权、防止敏感数据遭恶意使用对国家安全的威胁。在这三个方面，《网络安全法》都欠缺清晰的思路。首先数据安全层面，该法对构成“基础性战略资源”的数据安全保障依附于对关键信息基础设施的保护之上，数据本身没能构成独立的保护对象。其次，对构成“基础性战略资源”的数据的支配权，该法仅仅提出留存境内的要求。而如前述的例子，为保护国家和公共安全，对数据支配的要求显然应具有更丰富的内涵。最后，对防止敏感数据遭恶意使用对国家安全的威胁，该法完全没有涉及。

在国务院和各部门的发文中，够得上“基础性战略资源”的只有数据（或大数据）和档案。冠以“战略资源”的有土地、草原、稀土、石油、天然气、粮食、水、森林、矿产、煤炭等。[13] 从字面上来看，显然加上“基础性”这样的限定，意味着更加重要。但如果将《网络安全法》对数据的保护，与国家对档案、土地、稀土、石油、森林等资源的现行管理体制相比，相信不用专业知识也能直观地看到前者尚未形成全面、完整的体系。

在此方面，《网络安全法》错失了对新兴“基础性战略资源”的保护做顶层设计的机会，再一次体现出真正做到“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”，是多么困难的一件事。

参考文献：

[1] 中国首部网络安全法通过 明确网络空间主权原则 [EB/OL].（2016-11-07）[2016-12-10]. http://money.163.com/16/1107/20/C5A0TCFH002580S6_all.html.

[2] 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(03):102-103.

[3] 王利明 . 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心 [J]. 现代法学 ,2013(04):64.

[4] 王利明 . 隐私权概念的再界定 [J]. 法学家 ,2012(01):108-120.

[5] 廖宇羿 . 我国个人信息保护范围界定——兼论个人信息与个人隐私的区分 [J]. 社会科学

13 在权威数据库“北大法宝”中搜索得出。www.pkulaw.cn

研究 ,2016(02):72.

[6] 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(03):102-103.

[7] 阿里巴巴集团 . 阿里巴巴集团公布 2016 年 9 月底季度业绩 [EB/OL].(2016-11-02)[2016-12-10].http://www.alibabagroup.com/cn/news/article?news=p161102.

[8] 淘宝网 . 法律声明 [EB/OL].(2016-11-30)[2016-12-10]. https://www.taobao.com/go/chn/tb-fp/2014/law.php?spm=a21bo.50862.1997523009.38.26IY3m.

[9] Kevin Townsend.Kaspersky Lab Accuses Microsoft of Aggressive Attitude Towards Endpoint Security Firms With Windows 10 [EB/OL].(2016-10-15)[2016-12-10]. http://www.securityweek.com/security-firms-allege-microsoft-anti-competitive .

[10] 近平在网络安全和信息化工作座谈会上的讲话 [EB/OL]. （2016-04-19）[2016-12-10]. http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm .

[11] 孟斌 , 曹建海 , 姜炜等 . 空置率为何成了机密 [J]. 中国财富 , 2010(10): 90.

[12] 网易策划 . 住房空置率：一直在争论，从未有定论 [EB/OL] .(2015-12-04)[2016-12-10]. http://gz.house.163.com/special/gz_kongzhilv/ .

[13] 洪延青 . 网络安全为人民 ’ 的实在举措——评《网络安全法》关于个人信息保护的有关规定 [EB/OL].(2016-11-10) [2016-12-10]. 中国网信网 .http://www.cac.gov.cn/2016-11/10/c_1119889930.htm.

作者简介 :

洪延青，博士，主要研究方向为网络安全法律和政策，数据安全和个人信息保护。

On the gain and loss of Cybersecurity Law of China on Data Protection

HONG Yan-qing

（Cybersecurity Research Institute of Sichuan University, Chengdu Sichuan 610065,China）

[Abstract] In recent years, Chinese government attaches great importance to the fundamental and strategic role of data in driving country ’ s modernization in the New Normal. In various guiding document issued by the State Council, data has been labeled as “ nation ’ s fundamental strategic resources ” . This article asks whether the Cybersecurity Law of China has provided protection to data proportional to its status and importance. Overall speaking, the Cybersecurity Law has done a fairly good work on data security and personal data protection. With regard to data as “ nation ’ s fundamental strategic resources ” , this Law does not provide with systemic thinking, let alone comprehensive institutional designs for protective measures.

[Keywords] big data;fundamental strategic resources;Cybersecurity Law; national-level data protection