数据安全法：定位、立场与制度构造

许　可

摘　要：《数据安全法》的出台已箭在弦上，但相关基础理论研究却依然薄弱。在“单一安全转向总体安全”以及“数据和信息区隔”的背景下，《数据安全法》与《网络安全法》《个人信息保护法》等法律法规保持融通并相互支援。基于“攻守兼备的数据主权”以及“数据安全和数据利用的平衡”，《数据安全法》得以将数据分级分类，以“重要数据”为规制重心，衍生出包括重要数据识别、报送和泄露通知在内的种种制度设计，从而为一个国内安全有序、国际公正合理的数据新秩序奠定基础。

关键词：数据安全；个人信息；网络安全

［中图分类号］D922.8　　［文献识别码］A　　［文章编号］2096-6180（2019）03-0052-15

引言

2018 年 9 月，《十三届全国人大常委会立法规划》发布，《数据安全法》位列“条件比较成熟、任期内拟提请审议”的 69 部法律草案之中。与酝酿多年的《个人信息保护法》迥异，人们对这部切盼及早出台的法律草案既充满期待，又心存疑惑：《数据安全法》与《网络安全法》《个人信息保护法》的关系如何？其立法目的何在？其重点解决什么问题？为了回应这一系列关切，在《数据安全法》制定的关口，本文借箸代筹，尝试从学理入手，就《数据安全法》的体系定位、立场选择和重点制度提出一己之见，希冀有裨于理论探索和规则完善。

一、《数据安全法》的体系定位

作为面向实践的社会规范，法律不但要通过统一的概念和规范之间逻辑的排列组合体系化内部规则，还要无缝嵌入既有法律体系，推论出规则适用的优先次序，以减少司法和执法过程中的法律搜寻、比较、权衡和说理成本。[1] 因此，《数据安全法》的首要问题就是如何与其他法律保持融通并相互支援，此即“体系定位”问题。

［作者简介］许可，法学博士，对外经济贸易大学助理教授。

（1）苏永钦：《现代民法典的体系定位与建构规则》，《交大法学》2010 年第 1 期，第 61 页。

（一）通过“安全”统合的体系定位

1. 从“单一安全”转向“总体安全”

顾名思义，“安全”是《数据安全法》的立法之基，但这里的“安全”究竟何意？从解释论上观察，“数据的安全”一词源于我国《国家安全法》第 25 条，“国家安全”由此成为我们认识的开始。

在很长一段时期内，国家安全仅仅限于“军事安全”，但 20 世纪 70 年代初的石油危机使各国认识到国家安全的最大威胁可能“来自非军事领域”，包括能源危机、人口爆炸和经济增长凝滞、工业生产的高成本、国际贸易中的巨额赤字以及通货膨胀。[2] 1983 年，美国普林斯顿大学国际关系学者理查德·乌尔曼（Richard H. Ullman）发表《重新定义安全》（Redefining Security）一文，明确提出扩大国家安全内涵，使之包容非军事性的全球问题，把人类的贫困、疾病、自然灾害、环境退化等，均纳入安全研究中。[3] 由此，建立在“战争与和平”之上的“传统安全”，开始向以“发展与和谐”为导向的“非传统安全”转变。联合国在《1993 年人类发展报告》中正式提出了“人的安全”的概念，强调通过“人的发展”（human development）达到安全。1994 年，联合国秘书长加利在《联合国发展报告》中指出，人的安全既要避免诸如来自饥饿、疾病、心理压抑等的长期性威胁，又要保护人们在日常生活中免于突如其来的伤害性灾难，使人类享有平安。[4]

非传统安全的兴起促成了我国政府针对“国家安全”的思维转变。2006 年，《中共中央关于构建社会主义和谐社会若干重大问题的决定》提出要“有效应对各种传统安全威胁和非传统安全威胁”。2014 年，习近平总书记在中央国家安全委员会第一次会议中申明：“既重视传统安全，又重视非传统安全，构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系。”2015 年修订的《国家安全法》，吸取了这一“总体安全观”的精神，将统筹“传统安全和非传统安全”作为国家安全工作的四项内容之一。基于此，我们可以将“国家安全”理解为“国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力”。

2.《数据安全法》和《网络安全法》的协调

对《数据安全法》而言，上述安全概念具有双重意义。一方面，它揭示出“数据安全”本身就是“国家安全”不可分割的一部分。从美国棱镜计划大规模无差别的数据监控，到 2018 年 Facebook 公司 8 700 万个人数据被非法用于美国总统大选，再到以执法部门、情报机关与私营机构间强制数据共享为中心的澳大利亚《2018 年电信和其他法律修正（协助和访问）法案》（the Telecommunications and Other Legislation Amendment (Assistance and Access) Act，下称《协助和访问法》，数据已成为内部安全和外部安全的关键领域，此即“没有信息安全，就没有国家安全”的

〔2〕 刘卫东、刘毅、马丽、刘玉：《论国家安全的概念及其特点》，《世界地理研究》2002 年第 2 期，第 2 页。

〔3〕 Richard H. Ullman, *Redefining Security*, 8 INTERNATIONAL SECURITY 129, 129-153 (1983).

〔4〕 朱锋：《非传统安全解析》，《中国社会科学》2004 年第 4 期，第 143 页。

真义。另一方面，它赋予“数据安全”以丰富意蕴。详言之，数据安全包括“自身安全”“自主可控”和“宏观安全”三个层面：其一，“数据自身安全”（data security），即通过身份认证、访问控制、安全管理审计、平台基线配置等大数据平台安全技术，以及数据防泄漏、业务数据风险管理、结构化和非结构化数据保护等安全制度，确保数据的保密性、完整性、可用性。所谓“保密性”（secrecy）是指数据不为其他不应获得者获得；“完整性”（integrity）指在传输、存储数据的过程中，确保数据不被未授权地篡改或在篡改后能够被迅速发现；可用性（availability）是指数据满足一致性、精确性、完整性、时效性和实体同一性的要求。其二，“数据自主可控”（data safety），即国家对重要数据实际支配权力，避免被其他组织或国家非法操纵、监控、窃取和干扰。其三，“数据宏观安全”（data harmony），即防控和管理因数据处理、使用引致的国家主权、公共利益和群体安全的威胁。

数据安全内涵的梳理廓清了《数据安全法》和《国家安全法》《网络安全法》的关系。首先，《数据安全法》和《网络安全法》均是《国家安全法》的下位法，平等地统合在“国家安全”麾下。[5] 其次，为了避免两者不当交叉，并发挥互补效果，在《网络安全法》已规定“数据自身安全”（《网络安全法》第 76 条第 2 项的后段）的前提下，《数据安全法》应将“数据自主可控”和“数据宏观安全”作为规制重心。

（二）通过“数据”区隔的体系定位

1.“数据”：传统和现代

作为首部以“数据”为名的法律，“数据”是把握《数据安全法》的关键。那么，何谓数据？一般而论，数据有着传统和现代两种认识。[6] 从元认识论的角度，“数据”（Datum）在拉丁文中意指“已知”，也可以理解为“事实”，更准确地说，是通过数字、表格、图形对事实的客观记录。这种数据的传统观念，表现为日常习见的财务数据、经济数据、统计数据、科学实验数据等。甚至直到计算机发明之后，这种强调数值和量值的“定量小数据”还大行其道。时易世变，20 世纪 80 年代以来，随着信息技术的突飞猛进，文字、声音、图像、视频，乃至客观世界的一切都正在或即将被数字化，恰如尼葛洛庞帝和电影《黑客帝国》所昭示的，人类的数字化生存远非幻想。[7] 在“数字化转型”（digital transform）的历史背景下，现代数据迈向了“定性大数据”，以记录、描摹、再现、重构、发明物质世界和人类活动。[8] 在此意义上，现代数据是数字比特的结构化结合，它是虚拟电子世界的分子单元。

从数据的现代意义出发，首先，《数据安全法》不涉及财政数据、经济数据、统计数据等定量

〔5〕《网络安全法》的“网络安全”也可分为三层，即“数据安全”（data security）、“网络/因特网安全”（Network/Internet security）和“网络空间安全”（Cybersafety）。

〔6〕姜昊：《数据化：由内而外的智能》，中国传媒大学出版社 2017 年版，第 3-4 页。

〔7〕［美］尼葛洛庞帝：《数字化生存》，胡泳译，海南出版社 1997 年版，第一章。

〔8〕［英］维克托·迈尔·舍恩伯格、肯尼斯·库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 28 页。

数据，从而与《统计法》《政府信息公开条例》等法律法规相区隔。其次，《数据安全法》的规制对象应限于在电子介质中形成或存储的“电子数据”，而不是“非电子化数据”。这里的“电子数据”既包括时间连续与数值连续的“模拟数据”，也包括在时间上和数值上均离散的“数字数据”。最后，较诸《网络安全法》第 76 条项下“网络数据”，《数据安全法》不但包括通过网络收集、存储、传输、处理和产生的“网络数据”，也涵盖了线下的电子数据。

2.“数据”和“信息”的区隔

数据与信息的概念厘清，直接影响《数据安全法》和《个人信息保护法》的关系建构，在现有研究中，主要有着三种不同的观点。

其一，数据=信息。[9] 该观点认为：数据和信息具有天然的共生性和一致性，各国或地区立法混用 “数据”与“信息”概念，可资佐证。[10] 例如，在个人信息保护立法中，1973 年《瑞典数据保护法》、1978 年《德国联邦数据保护法》以及 2018 年生效的欧盟《一般数据保护条例》（General Data Protection Regulation, GDPR）均将“数据”（data）作为保护对象。相反，韩国、日本分别使用“정보”（信息）、“情報（信息）”作为法律名称。我国香港、澳门特别行政区和台湾地区的相关立法，虽使用“data”这一英文词语，但相应中文词语却是“资料”，根据其释义，“资料”更多指向具有实质内容的“信息”。美国法的最新发展进一步体现出“信息”和“资料”的混用。传统上，美国将个人信息置于“信息隐私”（information privacy）的规则之中，而维多利亚州在 2014 年出台《隐私和数据保护法》（Privacy and Data Protection Act），以期为个人信息收集、处理以及数据安全提供统一的法律基础。在该趋势下，2016 年，美国学者 William McGeveran 出版了名为《隐私和数据保护法》（Privacy and Data Protection Law）的法学院教材，在学理上拓展了这一新兴领域。[11]

其二，数据＞信息。[12] 现代管理学之父德鲁克将信息定义为：“被赋予相关性和目的性的数据。”该观点认为：单纯的数据本身并无实际意义，只有经过解释、对实体行为产生影响时才有意义，才能成为信息。基于此，数据是比信息更基础的素材，数据加上背景或者语境，进而演化成呈现序列的数据组合——信息，从信息中寻找出规律就成了知识，数据、信息、知识及智慧之间形成一个金字塔结构，一个递进式 DIKW 体系（Data-Information-Knowledge-Wisdom）。就此而言，信息是数据的子集，数字是比信息更大的范畴。

其三，数据＜信息。[13] 梅夏英教授在《数据的法律属性及其民法定位》一文中指出：信息的外延大于数据。数据只是信息表达的一种方式，除数据外，信息还可以通过其他方式来表达。亦即信息因其内容而具有意义，但这些具有特定意义的信息并不仅仅由数据来传播。

〔9〕 高富平：《个人信息保护：从个人控制到社会控制》，《法学研究》2018 年第 3 期。

〔10〕 梅夏英：《数据的法律属性及其民法定位》，《中国社会科学》2016 年第 9 期，第 168 页。

〔11〕 William McGeveran, PRIVACY AND DATA PROTECTION LAW (2016).

〔12〕 祝振媛、李广建：《“数据—信息—知识”整体视角下的知识融合初探》，《情报理论与实践》2017 年第 2 期，第 13 页。

〔13〕 梅夏英：《数据的法律属性及其民法定位》，《中国社会科学》2016 年第 9 期，第 168 页。

与上述三种观点不同，我们倾向于按照国际标准化组织（International Organization for Standardization, ISO）的定义，将数据看作“信息的形式化方式体现，该体现背后的含义可被再展示出来，且该种体现适于沟通、展示含义或处理”。〔14〕据此而言，作为信息存储、传输和处理的方式，数据只是信息的外在表现而不涉及其内容，信息则是人们对数据的解读。由此，信息和数据构成了同一个事物的不同侧面，前者是符号的社会、语言意义，而后者是形式化的符号本身。〔15〕数据与信息的一体两面关系，映射到电子空间中，便成为“按照一定规则排列组成的人工符号”和“通过机器人为读取的意义”。数据和信息一般是统一的，但在特殊情形下，也会发生分离。例如，一部手机记录着大量好友的姓名、电话号码、地址等个人信息，假设手机不慎掉入大海，则所有的数据因海水侵蚀而毁损灭失，但好友的信息却依然如故。数据和信息的二分产生不同的法律权利和制度安排，两者在权利主体、权利标的、权利性质和权利内容上均有所差异。〔16〕

3.《数据安全法》与《个人信息保护法》的协调

我国既有法律对“数据”一词多有涉及。除《网络安全法》外，我国《民法总则》在基本法的层面上也有所规定。其第 127 条规定：“法律对数据、网络虚拟财产的保护有规定的，依照其规定。”但是，这一倡导性规定不但没有在法律上回答“何谓数据”，而且没有对数据权属和保护方式加以明确。为了进一步阐释其含义，有必要从历史解释的角度探求立法本旨。

2016 年 7 月 5 日，全国人大常委会初审《民法总则（草案）》时，“数据”一词出现在第 108 条“民事主体依法享有知识产权。知识产权是指权利人依法就下列客体所享有的权利：……（八）数据信息……”。该草案发布后，该条款引发了广泛争议。首先，“数据信息”将数据和信息并列，缺乏概念的明确性，其次，将“数据信息”纳入知识产权的客体之中，这一具文不仅在我国 1982 年《民法通则》中并未表述及，也不符合《建立世界知识产权组织公约》《与贸易有关的知识产权协定》的规定。为此，2016 年 11 月 18 日，全国人大常委会二审《民法总则（草案）》将“数据信息”移除出知识产权的客体范围，并将“数据信息”修改为“数据”，形成了第 124 条“法律对数据、网络虚拟财产的保护有规定的，依照其规定”，并最终在 2017 年获得通过。由此推论，《民法总则》将“数据”和“信息”视为两种不同的法律概念。

《数据安全法》中的“数据”可参照我国对“电子数据”并借鉴我国台湾地区就“电磁记录”的相关规定，定义为“在电子、磁性、光学或其他类似方式形成并存储、供计算处理的电磁记录”，从而与数据上载荷或记录的“信息”相区隔。以此观之，《数据安全法》和《个人信息保护法》就不再是平等交叠关系，而是一套立体调整架构。质言之，《数据安全法》系底层立法，旨在为电子数据确立基础性的安全规则；《个人信息保护法》系上层立法，通过规范个人信息的收集和使用，以保护蕴含于信息内的自然人人格。当然，两者并非截然分离，在数据安全问题导致个人信息权

〔14〕“Reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing”, *See* ISO/IEC 2382:2015, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en (last visited April.15, 2019).

〔15〕纪海龙：《数据的私法定位与保护》，《法学研究》2018 年第 6 期，第 73 页。

〔16〕许可：《数据保护的三重进路》，《上海大学学报（社会科学版）》2017 年第 6 期，第 24 页。

益受到侵害之时，《个人信息保护法》可援引《数据安全法》中的义务性规定，以支持政府机关执法或权利人主张权利。

二、《数据安全法》的立场选择

任何法律都不是中立的，它必然有着自己的立场选择和价值判断。立场选择揭示了立法者的主观意图或法律的客观功能，堪称“法的灵魂”。然则，何谓《数据安全法》的基本立场？

（一）攻守兼备的数据主权

数据主权之于《数据安全法》，就如网络主权之于《网络安全法》，它不但是我们坚守的国家立场，也是处理数据安全的根本指针。尽管早在 2015 年 8 月，国务院《促进大数据发展行动纲要》已经提出“增强网络空间数据主权保护能力”，但数据主权的制度设计却始终没有成型。

1. 从“网络主权”到“数据主权”

要理解数据主权，必须从更广义的概念——“网络主权”开始。《国家安全法》首次将“网络空间主权”以法律形式予以明确。2015 年 12 月 16 日，习近平主席在第二届世界互联网大会的主旨演讲中，进一步将“尊重网络主权”列为全球互联网治理体系四项原则的核心。2016 年，《网络安全法》第 1 条便开宗明义地申明“维护网络空间主权”的立法主旨。2017 年 3 月 1 日，中国政府发布《网络空间国际合作战略》，全面分析了网络空间的机遇和挑战，明确“和平、主权、共治、普惠”作为网络空间国际合作的基本原则。

针对网络空间物理层、代码层和数据层的三层结构[17]，各国有着迥然不同的主权诉求。首先，作为网络空间基础设施，物理层（如计算机、服务器、移动设备、路由器、光纤、交换机、移动设备）的主权已获得公认。北约卓越合作网络防御中心（Cooperative Cyber Defence Centre of Excellence, NATO CCD COE）邀请国际专家小组编写的《适用于网络战争的塔林手册》（下称《塔林手册》）开篇即确定了网络空间主权：“一国可以对其主权领土之内的网络基础设施和行为实施控制。”[18] 类似地，时任美国国务卿顾问的高洪礼（Harold Hongju Koh）在 2012 年网络部队（US Cyber Command）会议上表示：支持互联网和网络活动的物理基础设施受制于领土国家的管辖权。[19] 就此而言，网络空间的物理层和电力、公路等公共基础并无二致。其次，对于代码层——特别是负责网络互联和传输的通信协议软件——的主权则存在着分歧。目前，ICANN（The Internet Corporation for Assigned Names and Numbers）、RIRs、ISOC、IAB、IETF、IRTE、ISO、W3C、INOG 等组织为互联网的稳定运行提供着技术支持，它们掌控的域名、号码、标准、监管构成并最终确定了用户使用网络的方式和限度。尽管上述组织的早期成员奉行内部“大体一致”的决策原则，

---

〔17〕这里综合了 Stephen K. Gourley 和劳伦斯·莱斯格对网络空间的定义，*see* Panayotis Ynakogeorgos, Adam Lowther, CONFLICICT AND COOPERATION IN CYBERSPACE 278-279；[美] 劳伦斯·莱斯格：《思想的未来》，李旭译，袁泳审校，中信出版社 2004 年版，第 23 页。

〔18〕 Michael N. Schmitt, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 15 (2013).

〔19〕 Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT' L. J, (2012).

但随着网络空间日益膨胀，政府开始介入，一种自治为表、控制为里的治理模式形成了。正如弥尔顿·穆勒（Milton Mueller）所指出的，当 ICANN 以自上而下的非政府实体形象展示给公众的时候，ICANN 事实上在契约和政治上都受制于美国政府；作为单边全球主义(unilateral globalism)的表现，ICANN 可以被理解为一种对于全球治理问题的霍布斯解决方式。[20] 这种单一国家控制的治理模式受到发展中国家的普遍反对，网络主权的呼声开始兴起。

区别于物理层和代码层，网络空间数据层的主权是各国论战的主要舞台，《塔林手册 2.0》甚至用“分裂”（split）一词来描述各国对“数据主权”的态度。这首先因为，在大数据和云计算时代，数据已经成为一个国家的基础性战略资源，各国纷纷主张对本国数据进行生产、开发、利用的权利。[21] 其次，数据所负载的信息还关涉文化、特性、价值观和意识形态，因此产生的深层次冲突难以弥合。最后，除了抽象的价值之争，数据控制者、使用者、存储者在地理位置上的分离以及所引发的跨境流动、主体识别和权力行使更是国家主权所面临的具体问题。但无论如何，只要我们承认数据事关国家安全、经济安全、社会稳定和民众福祉，国家对于数据的主权控制就当然是网络主权的题中应有之义。

2. 数据主权：守势与攻势

按照数据流向的不同，数据主权的行使可分为“守势”与“攻势”。所谓“守势”，即强调对数据出境的管控。各国对数据流向一般通过“数据出口限制”和“数据本地化”两种方式加以限制。前者如美国《出口管理条例》（The Export Administrative Regulations）和《国际军火交易条例》（International Traffic in Arms Regulations）对部分重要数据的出口进行许可管制。此外，欧盟 GDPR 第五章只允许个人数据流入欧盟认可的能提供“充分保护”或“适当保障措施”的国家或地区，亦是典型的立法例。后者如俄罗斯《关于信息、信息技术和信息保护法》和《个人数据法》严格要求互联网信息服务组织传播者、信息拥有者以及运营商将数据留存于俄罗斯境内。截至 2016 年，全球已有超过 60 个国家作出数据本地化存储的要求[22]，除俄罗斯和印度外，还包括欧盟、加拿大、澳大利亚、印度等发达国家。

所谓数据主权的“攻势”，即强调数据的跨境调取。从当前的国际趋势上看，网络强国均积极谋求跨境的数据管辖权。2018 年美国《澄清境外数据合法使用法案》（the Cloud Act）一改之前的“数据存储地标准”，转而采用“数据控制者标准”，规定无论通信、记录或其他信息是否存储在美国境内，数据控制者均有义务遵循美国的强制性命令向其提供。两个月后，欧盟提出《电子证据跨境调取的议案》（“E-evidence 议案”），建立了欧洲数据保存令（European Preservation Order）规

〔20〕 Milton Mueller, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 61-62 (2013).

〔21〕 黄志雄：《网络主权论》，社科科学文献出版社 2017 年版，第 27 页。

〔22〕 Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization*, Global Commission on Internet Governance Paper Series, https://www.cigionline.org/publications/tracing-economicimpact- of-regulations-free-flow-of-data-and-data-localization (last visited Apr. 15, 2019).

则，据此，欧盟成员国的执法或司法当局强制要求欧盟境内的网络服务提供商保存特定数据，以便主管当局获取。无独有偶，英国《犯罪（境外提交令）法案》也通过“境外提交令”（overseas production orders）机制，赋予法院命令企业提交境外数据的权力。

3.《数据安全法》的应然立场

我国更看重“守”还是“攻”？一方面，我们当然要重视“守”。《网络安全法》第 37 条确立了“关键信息基础设施运营者”的数据本地化义务，但管辖对象显然过窄。为此，中央网信办起草的《个人信息和重要数据出境安全评估办法》（征求意见稿），将出境安全评估的适用主体拓展到“所有网络运营者”。不过，《个人信息和重要数据出境安全评估办法》只是部门规章，这一突破缺乏明确的上位法依据。更重要的是，“数据本地化”和“数据出境限制”分属不同的制度，两者在规制范围、目的和实施方式上均有所差异，不应混同。〔23〕上述合法性缺陷亟待《数据安全法》弥补。此外，面对美国和欧盟的数据跨境调取，2018 年 10 月，我国《国际刑事司法协助法》适时出台，规定“非经中华人民共和国主管机关同意，中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和本法规定的协助”。然而，该规定仅限于刑事领域，《数据安全法》有必要作出更细致、更全面的规定。

另一方面，我们还要重视“攻”。随着企业全球化布局和“一带一路”的深入，我国利益已经和异国他乡休戚相关，数据主权也面临着“攻守易型”。为此，《数据安全法》应越过“属地管辖”的樊篱，向更灵活和宽泛的管辖权迈进。但是，在秉持合作和善意的国际法准则下，我国不应仿效美国《澄清境外数据合法使用法案》以“数据控制者”为锚的“长臂管辖”，而应借鉴欧盟 GDPR 的“保护管辖原则”，修改我国《网络安全法》第 75 条针对“关键信息基础设施”的域外效力〔24〕，明确数据安全的“效果管辖原则”。据此，无论数据是否存储于我国，只要其处理和使用在我国领土之内产生或意图产生不利影响，均属我国管辖。〔25〕为避免管辖权的过分扩张，这里的“影响”应做狭义理解，即仅限于“直接、可预见和实质性”的影响。

毫无疑问，攻守交替间，容易陷入“以子之矛，攻子之盾”的自我抵触的窘境。而这恰恰需要立法者的智慧，在具体场景下折中调和，有取有舍。正如习近平主席在第五届世界互联网大会的贺信所言，我们应以共进为动力、以共赢为目标，采取灵活、务实的数据主权制度，让网络空间命运共同体更具生机活力。

（二）数据安全与数据利用的权衡

《网络安全法》第 1 条和第 3 条分别体现出安全和发展两大价值取向，《数据安全法》亦须权

〔23〕 刘金瑞：《关于〈个人信息和重要数据出境安全评估办法（征求意见稿）〉的意见建议》，《中国信息安全》2017 年第 6 期，第 77 页。

〔24〕 该条规定，“境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任”。

〔25〕 Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 133, 133-134 (2013).

衡数据安全和数据利用两大价值。为此，我们有必要重新审视安全的含义。

1. 从“绝对安全”转向“相对安全”

“无危则安，无缺则全”，在中国传统观念中，“安全”意味着没有危险且尽善尽美。然而，在当今风险社会（risk society）中，这种绝对的安全观念已经不合时宜。正如卢曼所洞见的：我们生活在一个除了冒险别无选择的社会。无时不在、无处不在的风险弥散在周围，更重要的是，我们作为集体或个人作出的每个决定、每种选择、每种行动同时也在制造着新的风险。[26] 这从反面证明了风险的绝对性：人们用于应对风险的规制方式, 本身就是滋生新型风险的罪魁祸首。由于社会系统的复杂性和偶然性的高度抽象综合，无论是冒险取向还是安全取向的制度，都可能蕴含运转失灵或由相对无知导致的决策失误风险。[27] 风险滋生风险，这是现代性的必然结果。最后，风险并非全然客观，而是人为建构和社会定义的“构想”（conception），是一种想象的现实。在某种意义上，风险的本质并不在于发生，而在于人们认识到它“可能发生”。总之，只要民众在主观上相信风险的存在，风险就是真实有效的。正因如此，“不安全感”可能并非源于实际风险的增加，而是由有影响力的社会成员的呼声所引发。[28] 一旦人们认识到风险不可避免，“相对安全”便取代了“绝对安全”，成为法律的理性目标。

“相对安全”意味着安全可以衡量，人的身心安全程度及其事物保障的可靠程度可称为“安全度”，“危险性”（D）是安全度（S）的互为补数，即 S=1-D。简言之，当危险性低于某种程度时，人们就认为是安全的。[29] 这一公式奠定了政策法律的基调: 不是要根除或被动防止风险，也非简单考虑风险的最小化，而是设法控制不可欲的、会导致不合理危险的风险, 并尽量公正地分配风险。[30] 基于此，《数据安全法》并非要消除一切数据风险，而是通过持续的危险识别和风险管理过程，将损失降低并保持在可接受的水平以下。

2. 发展是安全的目的

既然安全不是绝对的，就不能绝对地追求安全。习近平总书记在 2016 年 4 月 19 日网络安全和信息化工作座谈会上指出：网络安全是动态的而不是静态的，开放的而不是封闭的，相对的而不是绝对的，因此一定避免不计成本追求绝对安全，那样不仅会背上沉重负担，甚至可能顾此失彼。这里的“彼”就是我国的信息化以及更广泛的经济发展。

信息网络之所以能成为“促进发展的机器”，来自它与“颠覆性创新”机制的耦合。哈佛商学院克里斯滕森（Clayton M. Christensen）教授与加拿大学者雷纳（Machael E. Raynor）在《创新者的解答》一书中将创新区分为“颠覆性创新”与“维持性创新”，前者才是经济变革的真正

〔26〕 杨雪冬：《全球化、风险社会与复合治理》，《马克思主义与现实》2014 年第 4 期，第 61 页。

〔27〕 劳东燕：《公共政策与风险社会的刑法》，《中国社会科学》2007 年第 3 期，第 128 页。

〔28〕 Barbara Adam, Ulrich Beck, Joost Van Loon, THE RISK SOCIETY AND BEYOND: CRITICAL ISSUES FOR SOCIAL THEORY 47-48 (2000).

〔29〕 苗金明：《安全法学导论：风险、理性与安全》，清华大学出版社 2014 年版，第 9 页。

〔30〕 劳东燕：《公共政策与风险社会的刑法》，《中国社会科学》2007 年第 3 期，第 128 页。

源泉。[31] 作为数字经济的核心生产要素，数据正成为经济转型和发展的新引擎，以及社会治理的有效工具。正是建立在海量数据之上，大数据、云计算、人工智能等新技术、新产业才有可能实现颠覆性创新。为了维持这种发展态势，我国《网络安全法》专设“网络安全支持与促进”一章，特别指出鼓励数据开放和利用，其第 42 条第 1 款还赋予了利用匿名化数据的自由，这一被称为“大数据条款”的规定为企业创新打开了大门。《数据安全法》亦应延续这一思路，充分认识到数据价值，将数据安全和数据利用看作一体之两翼、驱动之双轮，只要数据利用不会导致不合理危险，就应允许并积极推动其发展，通过激励相容的制度设计，最终令数据安全和数据利用协调一致、齐头并进，建久安之势、成长治之业。

三、《数据安全法》的重点制度

《数据安全法》制度纷繁多样，但“壹引起纲，万目皆张”， 这里试图从数据分类制度开始，逐一剖析“重要数据”的关键疑难问题。

（一）数据分类制度

作为数据的基本法，《数据安全法》固然要以所有“电子数据”，特别是“大数据”为规制对象，明确政府和企业相应的责、权、利，实现对数据安全的全方位规定，但从立法宗旨和技术上看，数据必须予以“类型化”，从而将《数据安全法》的法律规则与生活事实相互对应和调试。[32] 然则，数据应如何分类？

从技术层面，数据可以分为静态电子数据和动态电子数据，内容信息电子数据、附属信息电子数据与系统环境数据，封闭系统中电子数据、开放系统中电子数据与双系统中电子数据，电子设备生成数据、存储数据与混成数据，绝对电子数据和非绝对电子数据，等等。[33] 这种分类具有外延上的周延性，但由于其缺乏规范意蕴和制度后果，不宜作为《数据安全法》的分类依据。

从主体层面，数据可以分为个人数据、企业数据和政府数据。所谓个人数据，即能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种数据。所谓企业数据，即企业在生产经营数据中生成、存储和处理的数据，包括元数据、引用数据、主数据、企业结构数据、交易活动数据、交易审计数据等。所谓政府数据，即由政府收集、储存和处理的数据，包括信用、交通、医疗、卫生、就业、社保、地理、文化、教育、科技、资源、农业、环境、安监、金融、质量、统计、气象、海洋、企业登记监管等领域的公共数据，也包括涉及军事、外交、国防领域、国家安全的秘密数据。这种首创于欧盟的分类方法，已经受到了诸多批评。[34] 首先，这

〔31〕［美］克莱顿·克里斯坦森、[加]迈克尔·雷纳：《创新者的解答》，中信出版社 2010 年版，第 22-24 页。

〔32〕［德］亚图·考夫曼：《类推与“事物本质”——兼论类型理论》，吴从周译，台湾学林文化事业有限公司 1999 年版，第 91 页。

〔33〕汪振林：《电子数据分类研究》，《重庆邮电大学学报（社会科学版）》2015 年第 3 期，第 22 页。

〔34〕基于《一般数据保护条例》和《非个人数据在欧盟境内自由流动框架条例》，欧盟形成了“个人数据”和“非个人数据”的二元规制架构。批评的意见可参见 Inge Graef , Raphael Gellert, Nadezhda Purtova, Martin Husovec , *Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal* Data, https://ssrn.com/abstract=3106791 (last visited Apr. 15, 2019).

种分类与现有实践不符。事实上，同一个数据集往往同时包含多种类型数据，将相互混合的数据区分开来，即使不是不可能的，也非常困难。其次，三种数据的范围可能相互交叉。通过匿名化或爬虫技术，个人数据和政府数据均可以转化为企业数据，由于难以准确识别转化的时点，法律适用面临困难。最后且最重要的是，立法旨在遵循公平正义的要求平衡各方利益，而基于主体的数据分类未必体现相应主体的利益。例如，政府数据可能体现的是个人利益，如信用数据以及为了个人所得税减免进行的数据收集；个人数据也可能是企业利益的一部分，如“脉脉与新浪微博不正当竞争纠纷案”对企业数据利益的认可。〔35〕

基于上述分类的不足，同时考量规制目的，《数据安全法》可以根据对“国家安全”的影响效果，将数据分为“一旦泄露、破坏或者非法利用就严重危及国家安全的重要数据”和除此以外的“一般数据”。《数据安全法》应聚焦于“重要数据”的风险预防和管控。这一思路与国家顶层设计相契合。2017 年 12 月 8 日，习近平总书记在中共中央政治局第二次集体学习时强调：“要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”这里的“关键数据”即“重要数据”。从立法技术上，《数据安全法》将调整重心限定在“关键（重要）数据”上，不但有利于与《网络安全法》和《个人信息保护法》等法律衔接，而且有丰富的域外经验可资借鉴，还便于后续的执法工作。

（二）重要数据识别制度

一切类型皆系不确定概念〔36〕，重要数据同样如此。出于法律适用的目的，重要数据必须进一步明确其外延，对此，我国相关法律法规已进行了一系列尝试。

其一，以“关键信息基础设施”为锚点的明确化。我国《网络安全法》第 37 条将“重要数据”和“关键信息基础设施”相联结。而根据其第 31 条，所谓“关键信息基础设施”，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的网络和系统。显然，“关键信息基础设施”本身就是一个不确定概念，以至于中央网信办《关键信息基础设施安全保护条例》（征求意见稿）第 18 条也不得不把“其他重点单位”作为其定义的兜底条款。用新的不确定性来消除旧的不确定性，显然治丝益棼。更重要的是，类型组成要素的不固定性使其能容许不同的特征组合，而试图通过“关键信息基础设施”的单一要素框定“重要数据”，不免窄化了“重要数据”的范围。

其二，通过定性和列举的方式明确化。《个人信息和重要数据出境安全评估办法》（征求意见稿）和《数据出境安全评估指南（草案）》“附录 A 重要数据识别”将可能危害国家安全、国防利益、国际关系、国家经济秩序和金融安全、国家财产、个人合法权益、国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施安全的数据均囊括其中，并列出了石油天

〔35〕 参见北京知识产权法院（2016）京 73 民终 588 号民事判决书。

〔36〕 李可：《类型思维及其法学方法论意义》，《金陵法律评论》2003 年秋季卷，第 108 页。

然气、煤炭、石化、电力、通信、电子信息、钢铁、装备制造等 27 种数据类型。这一规定虽然纤悉无遗，但却漫漶无边，有失操作性，给政府执法和企业守法造成困难。

类型的学理研究表明，类型只能通过“同一利益状态”和“相似构成要件”来把握〔37〕,故此，对重要数据的识别一方面要回到规范利益，也就是前述“数据宏观安全”之中，另一方面应将侵犯国家对“数据自主可控”权力作为规范要件。质言之，“重要数据”是指一旦违反国家意志（国际公约、法律、法规、规章）泄露、窃取、篡改、毁损、丢失或滥用，就可能危害国家主权、公共利益和群体安全的数据。由此，还可以作出如下推论：（1）《数据安全法》下的重要数据不包括宏观统计数据、经济数据等定量数据〔38〕；（2）仅仅与个人或企业利益相关的数据不属于重要数据，但与巨量自然人（如超过 100 万人）休戚相关的数据足以构成；（3）合法公开的数据意味着国家放弃了控制权，不应视为“重要数据”；（4）对合法数据进行汇聚、整合并未侵害国家对数据的自主控制，即使可能分析出国家秘密或敏感信息，相关数据也不应视为“重要数据”。就此而言，《数据出境安全评估指南（草案）》犯了逻辑学中的“分称谬误”。〔39〕

当然，只有定性是不够的，从操作的角度，还可以借鉴美国“受控非秘信息”（Controlled Unclassified Information）制度，在可能范围内明晰重要数据边界。2011 年，美国《受控非密信息》13556 总统令通过严密的登记制度，详细列出了农业、受控技术信息、关键基础设施、应急管理、出口控制、金融、地理产品信息、信息系统漏洞信息、情报、国际协议、执法、核、隐私、采购与收购、专有商业信息、安全法案信息、统计、税收等门类。〔40〕我国《数据安全法》可借鉴其经验，结合我国政府机构、重点行业及其主管部门的意见，先列举核心数据类型，而后再根据实践发展进一步拓展范围。这里需要说明的是，重要数据如非国家秘密，其依然可以处理、流通和对外提供，只是受到严格限制。为此，《数据安全法》应鼓励重要数据的控制者在相关数据文件上以电子标记方式标明访问权限、流通限制及其解除时间。

（三）重要数据流通制度：以企业协助执法为例

企业和政府是《数据安全法》中最关键的两大主体，因而企业执法协助和向政府报送数据成为重要数据流通的核心制度。

企业的数据执法协助已经被各国普遍认可。早在 1994 年，美国就通过了《通信协助执法法》。次年，欧盟发布《数据存留指令》（Directive 2006/24/EC），要求通信网络及其服务提供者将数据留存，以协助执法机关进行严重犯罪与恐怖主义犯罪调查时参考使用。此后，英国、德国、荷兰、日本、新西兰等国纷纷制定了类似的法律，执法协助义务由此成为国际通行做法。2018 年 12 月 8

〔37〕 刘士国：《类型化与民法解释》，《法学研究》2006 年第 6 期，第 16 页。

〔38〕 相反的观点参见中央网信办、工信部在 2018 年 9 月开展的“个人信息和重要数据安全专项调查”中《专项调查问题列表与答复》对“重要数据”的界定。

〔39〕 该谬误假定整体的各个组成部分必定拥有整体的属性。相关规定可参见《数据出境安全评估指南（草案）》“附录 A 重要数据识别”第一段：汇聚、整合、分析后可分析出国家秘密或敏感信息的数据构成“重要数据”。

〔40〕 孙宝云：《论美国“敏感信息”管理过程的公开化及启示》，《情报杂志》2015 年第 4 期，第 153 页。

日，澳大利亚议会通过《协助和访问法》，授权国家安全情报机构、澳大利亚联邦警察、澳大利亚犯罪调查委员会和国家警察机关，向所有的通信提供者（包括运营商、通信设备供应商、终端设备厂商以及任何其他与通信相关的服务、设备或软件提供者），发出技术协助通知、技术能力通知以及计算机访问令和协助令，借此强制组织或个人提供加密信息的访问权限和信息。

我国亦不例外。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上指出：“一些涉及国家利益、国家安全的数据，很多掌握在互联网企业手里，企业要保证这些数据安全。企业要重视数据安全。”“要建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制。”目前，关于企业向政府机关报送数据的规定主要限于特定领域和特定事由，包括但不限于：《网络安全法》第 28 条、《电子商务法》第 25 条、《反恐怖主义法》第 18 条和《互联网信息服务管理办法》第 14 条。为此，《数据安全法》应统一法律法规的不同规定，就企业数据报送作出顶层设计。

与此同时，我们还须注意国际上的另一种声音。近期，针对《情报法》第 7 条第 1 款“任何组织和公民都应当依法支持、协助和配合国家情报工作，保守所知悉的国家情报工作秘密”，一种强烈的质疑情绪在西方发酵，给我国国际正常交往和商业活动蒙上了阴影。从文义解释看，第 7 条第 1 款并未要求组织和公民对国家情报工作“无条件地”支持、协助和配合，相反，所谓“支持、协助和配合”必须“依法”开展。需要指出：这里的“依法”并非依照《情报法》，而是依据《情报法》以外的法律法规，否则，这里的表述应当是“依据本法”。在依法行政的“法律保留”原则下，公安机关、国家安全机关不能在法律法规未授权时，强制任何组织和公民提供协助。同时，基于体系解释，第 7 条位于第一章“总则”部分，而总则部分所规定的一般是立法的目的和原则，而非具体的法律规范，《情报法》第四章“法律责任”中，并没有规定组织和公民不履行“支持、协助和配合”的责任。违法后果陈述的欠缺，使得第 7 条只是一个不完全法条，一个无法被执法机构直接援引适用的倡导性规定。

尽管西方曲解了《情报法》第 7 条，可它却给我们敲响了警钟。在中国企业走出去的背景下，《数据安全法》亟待摒弃“宜粗不宜细”的立法风格，尽量使用明确、清晰的立法语言，将企业向政府机关报送的数据限于“重要数据”之内，确立报送数据的合法性原则、比例原则、保密性原则、正当程序原则以及相关法定程序，明确政府相关部门的数据保护义务与责任，以避免引发无谓的争议。

（四）数据泄露通知制度

安全情报提供商 Risk Based Security(RBS)报告显示：2018 年全球公开披露数据泄露事件超过 6 500 起，有 12 起数据泄露事件涉及人数超过 1 亿。在“相对安全”架构下，《数据安全法》与其说是杜绝数据泄露，毋宁说是尽量降低其带来的损失。就此而言，旨在防止损失扩大的数据泄露通知的作用就非同寻常。而从风险规制理论观察，泄露通知是风险交流的基础，其有助于政府机

关和受害方识别和评估风险，并作出恰当的回应。[41]

数据泄露通知制度首创于美国，近年来被各国广泛采纳。[42] 2003 年，第一部数据泄露通知法案——《加州数据安全泄露通知法案》（California Data Security Breach Notification Law）出台。在该法的影响下，欧盟 2011 年修订《电子通信行业隐私保护指令》时引入数据泄露通知，GDPR 进一步将该制度扩展到所有数据控制者。2018 年 11 月，欧洲数据保护专员公署（European Data Protection Supervisor，EDPS）发布《个人数据泄露报告指南》（Guidelines on Personal Data Breach Notification For the European Union Institutions and Bodies），以保证欧盟机构有效应对相关事件的发生。我国《网络安全法》第 42 条第 2 款也规定了数据泄露通知，但仅限于个人信息泄露，且缺乏必要的程序细则，亟待《数据安全法》补足。基于比较法经验，数据泄露通知制度应具备如下内容。（1）数据泄露通知的主体。与 GDPR 项下的数据控制者承担通知义务不同，我国《网络安全法》的对象是包括“网络所有者、管理者和网络服务提供者”在内的网络运营者。该等宽泛规定在实践中不但可能出现“三个和尚没水喝”的窘境，还会令客观上无力履行义务的主体面临不能承受之重。《数据安全法》有必要改弦更张，从数据而非网络出发，借鉴数据控制者/数据处理者的二分法，重新设定新的法律主体。（2）触发数据泄露通知的条件。首先，泄露应作广义解释，包括可能危害数据“自身安全”“自主可控”和“宏观安全”的各种情形；其次，基于效果管辖原则，在中国境外发生但对中国公民或企业造成实质影响的数据泄露事件，相关数据控制者亦负通知义务。（3）数据泄露通知的对象。由于数据泄露关乎国家安全，政府机关首当其冲。考虑到通知效率，《数据安全法》可以规定网信部门作为第一通知接收人。此外，如个人可能因之受损，应有权获得通知。（4）数据泄露通知的程序。事件发生后，数据控制者应毫不迟延地向网信部门发出通知，通知内容包括事件基本情况、可能造成的后果、及时补救措施、联络方式等。在向个人发出通知的场合，通知应在合理期限内作出。

四、结语

从 2018 年初，Facebook 的 8 700 万名用户数据被不法用于政治目的，到年末万豪酒店喜达屋系统中高达 5 亿个人数据被窃，从美国《海外数据使用权明确法》到欧盟的 GDPR，再到华为公司 5G 战略因数据安全屡屡受挫，可见数据的安全风险和政治挑战屡见不鲜。恰恰在此背景下，我国《数据安全法》才有了特别的意义。立法充满挑战，任重而道远，但我们相信，凭借科学的规则设计和有效的国际对话，一个国内安全有序、国际公正合理的数据新秩序终将建立。

〔41〕［美］凯斯·R. 桑斯坦：《权利革命之后：重塑规制国》，钟瑞华译，中国人民大学出版社 2008 年版，第 322-327 页。

〔42〕 何波：《数据泄露通知法律制度研究》，《中国信息安全》2017 年第 12 期，第 40-41 页。

Data Security Law: Location, Position and Institution Construction

XU Ke

Abstract: The enactment of the Data Security Law is very urgent and pressing, but the related basic theoretical research is still weak. In the context of the transformation from single security to overall security and the separation between data and information, the Data Security Law, Cybersecurity Law, Personal Information Protection Law and other laws or regulations remain compatible and mutually supportive. Based on the data sovereignty of both offensive and defensive and the balance of data security and data utilization , the Data Security Law is able to classify data into categories, with 'important data' as the focus of regulation, including various system designs such as the identification, reporting and leak notification of important data，thus laying the foundation for a new data order that is internally secure and orderly and internationally fair and reasonable.

Keywords: Data Security; Personal Information; Cyber Security

（责任编辑：王乐兵）