主题研讨

数据安全范式革新及其立法展开

刘金瑞

内容提要:数字经济时代数据大规模的流动、聚合和分析带来了新的风险与挑战,信息安全和网络安全范式已经不足以应对,维护数据安全亟需范式革新。应该建立以数据风险管控为中心的数据安全范式:除了包括传统数据自身安全的保密性、完整性、可用性,还要确保数据利用安全的可控性和正当性。对于数据安全立法而言,要从国家安全高度进行数据安全法制体系化设计,以风险管控为中心构建数据安全保护制度体系,以重要数据安全为核心管控国家数据安全风险。特别是在制度建构上,应该以重要数据为抓手构建国家数据安全管理制度,包括明确重要数据的识别认定制度、规定重要数据处理者的安全保护义务、将重要数据安全审查纳入网络安全审查以及建立重要数据出境管制制度。

关键词:数据安全范式　数据利用安全　数据安全立法　重要数据　国家安全

刘金瑞,中国法学会法治研究所副研究员。

以科技为动力的现代化发展,使人类社会迈入了风险社会。从现代化进程的自反性角度来看,风险是现代化的副产品。〔1〕现代化风险主要是"人为制造的不确定性"。〔2〕信息化安全风险正是随着信息和通信技术(ICT)发展,而产生的一种人为制造的现代化风险。人类社会信息化历经1.0数字化和2.0网络化两次发展浪潮,已经迈入了3.0智能化阶段。〔3〕目前,"人机物"三元融合,数字化、网络化、智能化融合发展,海量数据正在不断积累、集聚和融合,对经济发展、社会治理、人民生活都产生了重大而深刻的影响,数据安全风险已成为事关各国国家安全与经济社会发展的重大问题。

数字经济时代的数据安全风险,对既有的安全范式和法律制度带来了极大挑战,维护

〔1〕 参见[德]乌尔里希·贝克著:《风险社会:新的现代性之路》,张文杰、何博闻译,译林出版社2018年版,第14页。

〔2〕 参见[德]乌尔里希·贝克:《再谈风险社会:理论、政治与研究计划》,载[英]芭芭拉·亚当等编著《风险社会及其超越:社会理论的关键议题》,赵延东、马缨等译,北京出版社2005年版,第328页;[英]安东尼·吉登斯著:《失控的世界》,周红云译,江西人民出版社2001年版,第22页。

〔3〕 梅宏院士将信息化发展分为数字化、网络化和智能化三个阶段,本文采纳了这一分类。参见梅宏:《十三届全国人大常委会专题讲座第十四讲 大数据:发展现状与未来趋势》,2019年10月30日,中国人大网,http://www.npc.gov.cn/npc/c30834/201910/653fc6300310412f841c90972528be67.shtml,最近访问时间[2020-12-15]。

数据安全亟需范式革新和立法保障。从世界范围来看,各国对此正处于探索之中,尚未出现成型的范式和专门的综合立法。我国目前已经形成了《中华人民共和国数据安全法(草案)》(下称"《草案》"),这是全球数据安全综合立法的首创性探索。本文就是在此背景下,针对新型数据安全风险和威胁,在梳理传统信息安全和网络安全范式的基础上,提出以数据风险管控为中心的数据安全范式,进而提出范式革新下数据安全立法的基本思路和核心制度,以期能够对数字经济时代的数据安全立法提供有益参考。

一 传统信息安全和网络安全范式下的数据安全

从技术发展的阶段来看,人类社会所面临的信息化安全风险从通信过程被窃听的威胁,逐渐演变为计算机被攻击、信息系统被攻击的风险。与此同时,安全观念也在不断演变和发展,从最初关注通信安全,逐渐发展到强调信息系统及其数据的安全。这种安全观念演变直接影响了信息化安全风险规制模式的转变。本文将认识和应对信息化安全风险的不同观念和规制模式称之为"范式"。[4] 归纳目前的规制模式,可以概括为传统信息安全范式和网络安全范式。为深刻认识和应对数字经济时代的数据安全挑战,有必要厘清这两种范式的核心概念和基本要素,并明确其与数据安全的关系。

(一)信息安全范式与数据安全

20 世纪 80 年代,随着个人计算机大规模普及应用,人类社会信息化进入了 1.0 数字化阶段。在这一阶段,从关注计算机安全逐步发展到强调数字化信息的安全,传统信息安全范式随之产生。1998 年 5 月,美国克林顿政府颁布《第 63 号总统决策指令》,[5] 相较于 20 世纪 80 年代美国《计算机安全法》,[6] 该指令将之前侧重的计算机安全扩展到信息安全。2002 年 12 月,美国颁布《联邦信息安全管理法》,将"信息安全"界定为"保护信息和信息系统不受未经授权的获取、使用、披露、破坏、修改或者销毁",以确保信息的完整性、保密性和可用性。[7] 保密性是指"维护信息获取和披露的授权限制,包括保护个人隐私和专有信息的方法";完整性是指"防止不当的信息修改或破坏,包括确保信息的不可否认性和真实性";可用性是指"确保信息的及时以及可靠的获取与使用"。[8] 由该定义可知,信息的可用性可以涵盖信息的可靠性。

可以发现,传统信息安全范式在定义信息安全时主要侧重信息自身安全,包括了三个基本要素:保密性、完整性和可用性。需要指出的是,我国关于信息安全的理解,一直以来既强调信息自身安全,又强调信息内容安全。[9] 信息内容安全是指信息的内容和传播,

---

〔4〕 托马斯·库恩认为,"一个范式就是一个公认的模型或模式(Pattern)"。参见[美]托马斯·库恩著:《科学革命的结构》,金吾伦、胡新和译,北京大学出版社 2003 年版,第 21 页。

〔5〕 *Presidential Decision Directive 63: Critical Infrastructure Protection*, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm,最近访问时间[2020-12-15]。

〔6〕 *Computer Security Act of 1987*, Pub. L. No. 100-235, 101 Stat. 1724.

〔7〕 *Federal Information Security Management Act of 2002*, 44 U.S.C. §3542(b)(1).

〔8〕 FISMA, 44 U.S.C. §3542(b)(1). 参见我国国家标准《GB/T 25069-2010 信息安全技术 术语》的 2.1.1 保密性、2.1.42 完整性、2.1.20 可用性。

〔9〕 参见沈昌祥主编:《信息安全导论》,电子工业出版社 2009 年版,第 11 页。

应该符合一国的价值观、意识形态和法律法规，不得损害国家安全和社会稳定。2015 年 1 月，中国与俄罗斯等国向联合国提交新版《信息安全国际行为准则》，就强调“不利用信息通信技术和信息通信网络干涉他国内政，破坏他国政治、经济和社会稳定”等。[10] 笔者认为可以将信息内容安全的基本要素称为“正当性”。本文将信息自身安全称为“狭义的信息安全”，将信息自身安全与信息内容安全统称为“广义的信息安全”。

在信息技术环境下，“狭义的信息安全”往往与“数据自身安全”不加区分的使用。根据 ISO/IEC 信息技术国际标准的定义，数据是指“为便于交流、解释或处理，对信息的可再解释的形式化表示”，信息是指“关于客体（如事实、事件、事物、过程或思想，包括概念）的知识，在一定场景中具有特定的意义”。[11] 我国国家标准借鉴该国际标准定义，作出了类似的界定。[12] 可以发现，数据本身不强调对于人的意义，但信息则强调可以被人所认知和解读的意义。在信息和网络技术环境下，数据就是比特形式的数字化符号，而这种数字化符号则用于表示信息。此时，数据就是信息的载体，信息就是数据的内涵。因此，狭义的信息安全即信息自身安全，就是指作为信息载体的数据的自身安全。

（二）网络安全范式与数据安全

20 世纪 90 年代中期，计算机和信息系统网络化发展迅速，人类社会信息化进入了 2.0网络化阶段。在这一阶段，金融、交通、电信等基础设施运营日益依靠网络信息系统。然而网络信息系统及其数据可能遭受攻击和破坏，从而引发了网络安全问题。

对于网络安全风险而言，只关注信息自身安全的传统信息安全范式已经不足以应对，随之出现了以网络信息系统安全为中心的网络安全范式。20 世纪 90 年代后期以来，美国出台了一系列关于“关键基础设施”“网络安全”的政策和立法。[13] 欧盟从 2001 年开始制定专门立法以确保“网络和信息安全（NIS）”，其是指“网络或信息系统在一定的可信度下抵御突发事件、非法或恶意行为的能力，这些行为会危害该系统存储或传输的数据的可用性、真实性、完整性和保密性，危害依靠该网络或系统提供或获得的有关服务”。[14] 2016 年 7 月，欧盟通过的《促进欧盟共同高水平网络与信息系统安全的措施之指令》（下称“网络与信息系统安全指令”）也基本沿用了这一定义。[15] 我国《网络安全法》规定：“网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以

---

〔10〕《信息安全国际行为准则》，2015 年 3 月 5 日，外交部官网，http://infogate.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t858317.shtml，最近访问时间[2020－12－15]。

〔11〕ISO & IEC, *Information technology-Vocabulary*, ISO/IEC 2382:2015, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en，最近访问时间[2020－12－15]。该标准除了从信息处理角度对信息作上述界定外，还从信息论角度界定了信息：“可以减少或消除一组给定可能事件中某一特定事件发生的不确定性的知识”。

〔12〕中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会：《GB/T 17532-2005 术语工作 计算机应用 词汇》，中国标准出版社 2005 年版，第 1 页。

〔13〕参见刘金瑞：《美国网络安全的政策战略演进及当前立法重点》，《北航法律评论》2013 年第 1 辑，第 205－227 页。

〔14〕Commission of the European Communities, *Network and Information Security: Proposal for A European Policy Approach*, COM (2001) 298 final, 6.6.2001, p.9; *Regulation No* 460/2004 *of the European Parliament and of the Council of* 10 *March* 2004 *Establishing the European Network and Information Security Agency*, Art.4(c), OJ L 77, 13.3.2004, p.5.

〔15〕*Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (NIS Directive)*, Art.4 (2), OJ L 194, 19.7.2016, p.13.

及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力”。由此可以看出,网络安全就是要确保网络信息系统及其数据的安全。

对于网络信息系统中的数据而言,传统信息自身安全的“完整性、保密性、可用性”三要素仍然适用,“网络数据安全”就是网络空间的狭义信息安全。在网络空间,网络信息安全除了网络数据自身安全之外,也包括网络数据所承载信息的内容安全,仍然适用前述信息内容安全的“正当性”要素。网络信息安全就是网络环境下的广义信息安全。但对于“网络信息系统”而言,传统信息安全三要素不足以适应其安全性要求。有学者将网络空间安全分为设备层安全、系统层安全、数据层安全、应用层安全。[16] 本文将设备层安全和系统层安全统称为网络系统安全。对于网络系统安全,虽然保密性和完整性要求仍然适用,但从目前立法来看,更加强调“稳定可靠运行”和“持续提供服务”。

笔者认为可以将这些安全要求概括为“可靠性”和“坚韧性”。可靠性(Reliability)是指“预期行为和结果保持一致的特性”,[17] 强调特定系统、产品或元件在一定条件下执行指定功能的能力或可能性,是传统信息安全“可用性”要素中“可靠使用”内涵在网络环境下的凸显。可靠性要素要求确保构成系统的硬件和软件的供应链安全。坚韧性(Resilience)是指“在面对影响网络正常运行的多样挑战时,该网络提供或者维持一种可接受水平的服务的能力”。[18] 这就要求网络系统足以应对黑客攻击、洪水、火灾等意外事件,即使被攻击也能及时恢复正常运行。“坚韧性”这个要素很少见于传统信息安全领域,一般只用于网络系统安全,尤其是关键信息基础设施保护领域[19]。

综上,网络安全包括网络信息安全与网络系统安全,前者的基本要素是保密性、完整性、可用性和正当性;后者的基本要素是保密性、完整性、可靠性和坚韧性。鉴于传统信息安全范式立法对数据和信息系统有了一定的保护,网络安全范式立法从世界范围来看,无论是美国的“关键基础设施”,欧盟的“基本服务运营者”,还是我国的“关键信息基础设施”,核心都是保护事关国家安全、公共安全的关键信息基础设施安全。[20]

二 数字经济时代下的数据安全风险与范式革新

进入 21 世纪以来,随着云计算、大数据、物联网和人工智能等新技术迅速发展和应用,人类社会信息化进入了 3.0 智能化阶段。在这一阶段,信息技术与人类生产生活深度

〔16〕 参见方滨兴:《定义网络空间安全》,《网络与信息安全学报》2018 年第 1 期,第 3 - 4 页。

〔17〕 参见我国国家标准《GB/T 25069-2010 信息安全技术 术语》的 2.1.19 可靠性。

〔18〕 European Network and Information Security Agency [ENISA], *Guidelines for Enhancing the Resilience of Communication Networks: Providers' Measures*, December 2009, p. 11, https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Guidelines%20for%20Enhancing%20the%20Resilience%20of%20Communication%20Networks%20-%20Providers%20Measures.pdf,最近访问时间[2020-12-15]。

〔19〕 Commission of the European Communities, *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM (2009) 149 final, 30.3.2009; White House, *Cyberspace Policy Review: Assuring A Trusted and Resilient Information and Communications Infrastructure*, May 2009, https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf,最近访问时间[2020-12-15]。

〔20〕 参见刘金瑞:《我国网络关键基础设施立法的基本思路和制度建构》,《环球法律评论》2016 年第 5 期,第 117 页。

交汇融合,数据呈现爆发式增长并且海量集聚。这股强大的数据流催生了数字经济,数据成为推动经济发展的关键生产要素,人类社会迈入了数字经济时代。

(一)数字经济下数据的价值创生与安全风险

在数字经济时代,数据驱动创新和发展的关键在于发掘和释放数据资源的价值。数据价值产生和创造的机理,可以结合"数据—信息—知识—智慧层次模型"和"数据价值周期"来理解。前者由拉塞尔·阿克夫(Russell Ackoff)提出。他认为数据是观察的产物,本身不具有价值,除非被处理成可用形式的信息;知识是对信息的进一步提炼,是将信息转化成行为指南;智慧是感知和评估任何行为长期后果的能力;"数据—信息—知识—智慧"形成了从下到上的金字塔式层次模型。[21] 后者由经济合作与发展组织(OECD)提出,描述了数据价值的产生过程,包括数据化和数据收集、大数据、数据分析、知识库、数据驱动决策等一系列阶段,数据价值产生于数据被转化为知识以及被用于决策这两个环节。[22]

总结来看,数据本身不具有价值,但依靠技术手段对数据进行分析和挖掘可以获得信息和知识,这些信息和知识可以用于决策和指导实践,这就是数据的社会和经济价值所在。从数据价值的创生来看,数据价值依赖于大量多样性数字化数据的汇聚、流动、处理和分析活动。这种流动性的数据密集型活动以分布式处理为主,参与主体更加多元,业务生态更加复杂,传统的系统和业务边界更加模糊。[23] 数据密集型活动的流动性和复杂性既使得传统的数据安全风险大大增加,也引发了新型的数据安全风险和挑战。

所谓传统的数据安全风险,就是指数据自身安全层面的风险,主要表现为利用数字环境的漏洞来侵害数据的保密性、完整性和可用性。从表现形态看,数字经济时代数据自身安全是动态的,贯穿于数据流动的全过程。这使得数据自身安全面临更大的风险,一旦遭受攻击也容易造成更严重的后果。比如,如果在人工智能的训练数据中加入恶意数据进行"数据投毒",就会导致训练的算法模型出现决策偏差,有研究就指出用数据污染脸部检测算法可以将攻击者的脸识别成获授权者的脸。[24]

所谓新型的数据安全风险主要是多源大量数据聚合和分析可能带来的安全风险。也就是说数据聚合分析是把"双刃剑",数据聚合分析得到的信息和知识,不一定对社会和经济有价值,反而可能带来安全风险。这主要表现为两个方面:一是数据分析挖掘得到的信息和知识,本身就具有安全风险。例如,2018 年 1 月,健身应用 Strava 发布了基于 2700 万用户运动轨迹数据的"全球热力地图",由于许多美军士兵是该程序的用户,据此可以分析出美军在阿富汗等地的军事基地位置。[25] 可见,数据聚合分析通过对积累汇聚的数

〔21〕 Jay H. Bernstein, The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis, https://journals.lib.washington.edu/index.php/nasko/article/viewFile/12806/11288,最近访问时间[2020-12-15]。Russell L. Ackoff, *Re-Creating the Corporation: A Design of Organizations for the 21st Century*, Oxford University Press, 1999, pp. 159-164.

〔22〕 Org. for Econ. Co-operation & Dev. [OECD], *Data-Driven Innovation: Big Data for Growth and Well-Being*, October 2015, pp. 32-33, https://doi.org/10.1787/9789264229358-en,最近访问时间[2020-12-15]。

〔23〕 参见中国信息通信研究院安全研究所:《大数据安全白皮书(2018 年)》,第 3 页,http://www.caict.ac.cn/kxyj/qwfb/bps/201807/P020180712523226672500.pdf,最近访问时间[2020-12-15]。

〔24〕 参见梅宏主编:《数据治理之论》,中国人民大学出版社 2020 年版,第 264 页。

〔25〕 参见《跑步 APP 泄露美军事基地位置?五角大楼着手调查》,2018 年 1 月 31 日,新华网,http://www.xinhuanet.com/world/2018-01/31/c_129802139.htm,最近访问时间[2020-12-15]。

据进行搜索、比对、关联等分析,可能挖掘出数据集背后隐藏的安全情报甚至涉密信息。这说明某些之前认为无关紧要的数据在聚合分析技术条件下也会成为高风险敏感数据,判断数据重要性和敏感性要充分考虑数据的集聚效果和潜在使用方式。

二是滥用数据分析所得的信息和知识,作出决策和行动而引发安全风险。滥用数据分析结果不仅可能造成“大数据杀熟”“歧视”等个人权益侵害行为,更有可能对公共安全和国家安全造成严重威胁。例如,有报告指出,通过分析公开发表的科技论文和公共数据库的基因信息,可以分析出某种病毒的易感宿主基因,利用这些信息可以制造感染特定人群的病毒。〔26〕 这无疑会造成严重的生物安全风险。再如,2018 年 Facebook 约 8700 万用户数据被剑桥分析公司用于分析用户偏好并投放定向政治广告,从而影响了美国总统大选和政治安全。〔27〕 该事件也说明,数据分析结果本身可能无关信息内容安全,但如果滥用数据分析结果来干预信息传播秩序和内容,也可能危害信息内容安全。原因在于网络信息传播存在“过滤泡”〔28〕效应和“信息茧房”〔29〕效应,基于数据分析的个性化内容推荐,如果被滥用于推送违法和不良信息尤其是虚假信息,就可能会扰乱信息传播秩序,破坏信息内容生态,造成受众观念极化,甚至会操纵用户的观念和行为。

(二)以数据风险管控为中心的数据安全范式

数字经济时代的数据安全,就是既要确保数据密集流动中数据的保密性、完整性和可用性,也要防范数据大规模聚合和分析引发的安全风险。本文将前者称为数据自身安全也即“狭义的数据安全”,后者称为数据利用安全,二者统称为“广义的数据安全”。下文如无特别说明,“数据安全”都是指“广义的数据安全”。由此,结合前文所述,可以得出数据安全与信息安全、网络安全之间的概念关系:数据安全与信息安全的交集,在于数据形式信息的自身安全和数据聚合分析导致的信息内容安全;数据安全与网络安全的交集,在于网络数据的自身安全;网络安全和信息安全的交集在于网络数据的自身安全以及网络信息内容安全;网络数据安全也是三者的交集所在。

虽然传统信息安全范式的“保密性、完整性、可用性”三要素对于数据价值周期某一节点的数据自身安全仍然适用,但对于流动性数据的利用安全而言,传统信息安全范式和网络安全范式下静态的安全边界防护方法已经难以满足安全需求。应该发展一种动态的以数据为中心的新的数据安全范式。目前从全球来看,这种新范式尚处在探索之中。例如,经济合作与发展组织(OECD)于 2015 年 9 月发布了《理事会关于为了经济和社会繁荣的数字安全风险管理的建议》,认为:数字安全风险是“在任何活动过程中与数字环境

〔26〕 American Association for the Advancement of Science, Federal Bureau of Investigation, United Nations Interregional Crime and Justice Research Institute, *National and Transnational Security Implications of Big Data in the Life Sciences*, 2014, p. 38, http://www. aaas. org/sites/default/files/AAAS – FBI – UNICRI_Big_Data_Report_111014. pdf,最近访问时间[2020 – 12 – 15]。

〔27〕 参见孙宝云、李艳、齐巍:《网络安全影响政治安全的微观分析——以“剑桥分析”事件为例》,《保密科学技术》2020 年第 4 期,第 27 – 34 页。

〔28〕 伊莱·帕里泽认为,个性化推荐新闻和其他内容的做法,会缩小展现给某个人的观点范围。See Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, The Penguin Press, 2011, pp. 54 – 55.

〔29〕 凯斯·桑斯坦认为,人们如果只关注与自己信念和观点一致的信息,就如同桎梏于“茧房”之中。参见[美]凯斯·R. 桑斯坦著:《信息乌托邦:众人如何生产知识》,毕竞悦译,法律出版社 2008 年版,第 206、237 页。

的使用、开发和管理相关的一类风险”;通过妨碍活动和/或环境的保密性、完整性和可用性,可以危害经济或社会目标的达成。[30] 可以看出,OECD 还是侧重基于网络信息系统的数字环境的安全,沿用了传统的保密性、完整性、可用性三要素。

本文认为,以数据为中心的数据安全范式革新,核心是要管控好数据大规模流动、聚合和分析所致风险即大数据安全风险,在充分释放数字经济数据价值的同时,将不确定性的潜在不利影响降至最低。本文将这一新的安全要求概括为“可控性”(Controllability),并界定为“在数据大规模流动、聚合和分析的过程中,将安全风险维持在一种可接受水平的能力”。此外由前所述,滥用数据分析有可能造成危害信息内容安全等后果,那么管控数据安全风险还应该要求数据利用合乎“正当性”。

表 1　数据安全范式、信息安全范式、网络安全范式对比

发展阶段	范式	安全层面	安全要素
信息化 1.0 数字化	信息安全范式	信息自身安全	保密性、完整性、可用性
		信息内容安全	正当性
信息化 2.0 网络化	网络安全范式	网络系统安全	保密性、完整性、可靠性、坚韧性
		网络信息安全	保密性、完整性、可用性、正当性
信息化 3.0 智能化	数据安全范式	数据自身安全	保密性、完整性、可用性
		数据利用安全	可控性、正当性

综上,数字经济时代的数据安全包括数据自身安全与数据利用安全,前者的基本要素仍然是保密性、完整性和可用性,后者的基本要素是可控性和正当性。数据安全范式与信息安全范式、网络安全范式的对比,如表 1 所示。数据安全范式的新要素是可控性,可控性的关键是将数据大规模流动、聚合和分析纳入风险管控的过程之中。风险管控的思路其实一直蕴含在信息和通信技术风险的应对之中,只不过在信息安全和网络安全范式下,风险管控聚焦到信息和系统的静态的安全边界防护上,表现为信息自身安全三要素和网络系统安全的可靠性、坚韧性,而数字经济时代数据突破边界的动态流动,使数据成为安全焦点,数据风险的可控性要求更加凸显和必要。

三　域外数据安全风险管控制度的探索——以美国为例

目前来看,对于如何管控数字经济时代的数据安全风险,世界各国正处于探索之中,尚未出现专门的系统性制度设计。美国作为全球网络信息技术最发达的国家,较早认识到传统安全范式的不足,开始在部分领域探索以数据为中心的风险管控制度。

(一)联邦政府的受控非密信息管理

在很长一段时间里,美国政府不同部门对敏感信息的管理各自为政、比较混乱,包括

〔30〕 OECD, *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*, October 2015, https://doi.org/10.1787/9789264245471-1-en,最近访问时间[2020-12-15]。

敏感但非密信息、仅限官方使用信息、敏感安全信息等。2010 年 11 月,奥巴马政府颁布《第 13556 号行政命令》,在“受控非密信息”(CUI)概念下建立了联邦政府公开和统一的管理框架。[31] 受控非密信息是指“按照和遵从法律、法规和联邦政府政策,需要进行保护和控制传播的信息”,但不包括涉密信息。美国国家档案和文件管理局(NARA)被指定为行政命令的执行部门。2016 年 9 月,该局发布了实施细则,规定了受控非密信息的登记、分类、安全保护、获取和传播、控制解除、标识、应用限制等。[32]

1. 登记、分类和标识

执行部门负责建立公开的受控非密信息登记系统,公布所有被批准的受控非密信息的分类、标识、控制解除以及法定依据。[33] 美国受控非密信息目前共分为 20 个类别、125 个子类,20 个类别是:关键基础设施、国防、出口管制、金融、移民、情报、国际协议、执法、法律、自然和文化资源、北约、核、专利、隐私、采购和收购、专有商业信息、临时信息、统计、税收和交通。[34] 政府机构只能按照上述分类来认定受控非密信息。[35]

受控非密信息应该加注标识,标识内容用双斜杠分隔为三个部分:“CONTROLLED”或“CUI”标识;受控非密信息类型或子类标识,如果应遵守特别管控规定,还要在分类前加注“SP-”;传播限制标识,目前有 10 种,如禁止国外传播(NOFORN)、仅限联邦雇员使用(FED ONLY)等。[36] 当因信息的数量或性质逐一标注受控非密信息不切实际或已获得标记豁免时,授权持有者必须以获取协议、系统弹屏、储存区标记等方式表明该信息属于受控非密信息。[37] 政府机构不得通过把信息标注为受控非密信息的方式来掩盖违法、过失、不称职或者其他令官员、政府机构、联邦政府及其合作伙伴尴尬的不光彩情况,也不得在法定授权之外将信息标注为受控非密信息。[38] 各政府机构应该建立报告和调查滥用受控非密信息的程序和标准,政府机构应该根据有关规定对滥用受控非密信息行为予以惩处。[39]

2. 安全保护

执行部门通过发布受控非密信息安全保护标准来要求政府机构在允许授权持有者及时获取受控非密信息的同时,能够最小化未经授权披露的风险。安全保护标准分为基本保护和特别保护两类,无特别规定则默认采用基本保护。授权持有者应当采取合理措施防范受控非密信息泄露,包括:建立可控的安全环境;确保未经授权的人不能获取、观察或

〔31〕 Executive Order 13556: Controlled Unclassified Information, *Federal Register*, Vol. 75, No. 216, November 9, 2010, pp. 68675 – 68677.

〔32〕 *Controlled Unclassified Information* (*CUI*), 32 C. F. R. Part 2002.

〔33〕 32 C. F. R. § 2002. 10.

〔34〕 CUI Categories, https://www. archives. gov/cui/registry/category – list, U. S. National Archives and Records Administration,最近访问时间[2020 – 12 – 15]。

〔35〕 32 C. F. R. § 2002. 12.

〔36〕 32 C. F. R. § 2002. 20 (b). CUI Marking Handbook, Version 1. 1, December 6, 2016, https://www. archives. gov/files/cui/documents/20161206 – cui – marking – handbook – v1 – 1 – 20190524. pdf,最近访问时间[2020 – 12 – 15]。

〔37〕 32 C. F. R. § 2002. 20 (a) (8).

〔38〕 32 C. F. R. § 2002. 20 (a) (6).

〔39〕 32 C. F. R. § 2002. 54, § 2002. 56.

听说受控非密信息;确保受控非密信息在离开可控环境后始终处于授权持有者的直接控制下,或者至少有一种物理保护屏障;使用联邦信息系统处理、存储或传输受控非密信息时,要按照《联邦信息及信息系统安全分类标准》(FIPS PUB 199)、《联邦信息及信息系统最低安全要求》(FIPS PUB 200)、《联邦信息系统和组织的安全及隐私控制》(NIST SP 800-53)的要求来保护受控非密信息的保密性。[40]《联邦信息及信息系统最低安全要求》规定了17类安全控制,包括:访问控制,意识和培训,审计和可追溯性,认证、认可和安全评估,配置管理,持续规划,识别和鉴别,事件响应,维护,介质保护,物理和环境保护,规划,人员安全,风险评估,系统和服务采购,系统和通信保护,系统和信息完整性。如果非联邦主体在非联邦信息系统中处理、存储或传输受控非密信息,则要按照《保护非联邦系统和组织的受控非密信息》(NIST SP 800-171)的要求来保护受控非密信息。[41]

3. 获取传播和控制解除

只要满足下列条件,政府机构就应当允许获取或传播受控非密信息:遵守法定的受控非密信息分类;促进合法的政府目的;未被限制传播控制所限制;也没有被其他法律禁止。政府机构实施受控非密信息传播控制只能限于法定的必要限制,这些控制必须经过执行部门批准并公布于登记系统。授权持有者将受控非密信息共享给非行政主体,除有豁免外应该与该主体签订正式协议,协议至少应当包括下列内容:该主体必须遵守法定要求处理受控非密信息;滥用受控非密信息将依法受到惩罚;出现不符合处理要求的情况要报告。政府机构与外国实体共享受控非密信息,也应该签订协议或安排,政府机构应该鼓励外国实体根据美国的法定要求来保护受控非密信息。[42]

对受控非密信息解除控制的情形包括:一是根据有关规定不再需要控制;二是指定受控非密信息的政府机构决定公开;三是政府机构根据《信息自由法》《隐私法》等将受控非密信息予以公开;四是预先设定的事件或日期到来。此外,受控非密信息指定机构也可以根据授权持有者请求或者解密行动对受控非密信息解除控制。对于解除控制的受控非密信息,授权持有者在复述、改写、再利用、向公众发布或捐赠给私人机构时必须明确说明不再受控,除此之外不必采取标记、审查或其他行动来表明受控非密信息不再受控,解除控制后的信息要去掉保护标识。[43]

(二)敏感个人数据风险纳入外资安全审查

2018年8月,美国总统特朗普签署《2018年外国投资风险审查现代化法》(FIRRMA),[44]授权美国外国投资委员会(CFIUS)应对敏感个人数据对国家安全的威胁。

1. 审查涉及敏感个人数据的非控制性投资

FIRRMA授权美国总统和CFIUS可以审查某些针对特定领域美国商业的外国非控

---

〔40〕 32 C. F. R. §2002.14 (a) (b) (c).

〔41〕 32 C. F. R. §2002.14 (h).

〔42〕 32 C. F. R. §2002.16 (a).

〔43〕 32 C. F. R. §2002.18 (b) (c) (f).

〔44〕 *Foreign Investment Risk Review Modernization Act of 2018* (FIRRMA), Pub. L. No. 115 – 232, 132 Stat. 2173.

制性投资,[45]而在这之前 CFIUS 的管辖范围仅包括可能导致外国主体控制美国商业的交易。[46] 根据 FIRRMA 和美国财政部颁行的该法实施细则,[47]“美国商业”是指不论控制人的国籍如何,任何在美国从事跨州商务的实体;这些特定领域美国商业是指涉及关键技术、关键基础设施和敏感个人数据(TID)的商业(下称“美国 TID 商业”)。[48]

只要对美国 TID 商业的非控制性投资使得外国主体取得了以下权利,该投资就属于审查范围:取得美国 TID 商业重大非公开技术信息的访问权限;取得美国 TID 商业董事会或同等管理机构的成员或观察员权利,或者有权指定他人进入董事会或同等管理机构任职;除了股份投票权外,取得美国 TID 商业有关 TID 业务实质性决策的参与权,这里的 TID 业务包括了决定使用、开发、获取、保管或发布其持有或收集的美国公民的敏感个人数据。[49] 由此,如果外国主体针对持有或收集美国公民敏感个人数据的美国商业投资,并且能够取得上述权利,该投资就属于 CFIUS 的审查范围。

2. 界定影响国家安全的敏感个人数据

FIRRMA 明确将敏感个人数据列为外国投资安全审查时评估国家安全风险的要素之一,原因在于“这些信息可能被外国政府或外国主体获取,并以威胁美国国家安全的方式利用”。[50] 比如,通过数据聚合分析,可以发现某些关键岗位人员的财务或健康状况,以此威胁、利诱这些人员实施危害国家安全行为。由此,“敏感个人数据”的“敏感”并不是强调个人权益的保护,而是强调对国家安全的威胁。FIRRMA 实施细则从两方面界定了影响国家安全的敏感个人数据:

一是界定了可识别数据,是指“可用于区分或追踪个人身份的数据,包括个人身份标识符”。如果交易方具备使聚合数据分解、匿名数据去匿名化的能力,那么聚合数据和匿名数据也是可识别的。[51] 实施细则列明了 11 类个人可识别数据,包括:个人财务状况数据,消费者信用报告数据,保险申请相关数据,个人身体、精神或心理健康状况数据,非公开的电子通信数据,地理位置数据,生物识别数据,州或联邦的个人身份证数据,政府工作人员安全审查状况相关数据,政府工作人员安全审查申请或公众信任职位申请;此外,个人的基因检测结果包括基因测序数据,也构成可识别数据。[52]

二是界定了本文所称的“国家安全敏感性”。这要求被投资的美国商业具备下列情形之一:目标或定制产品或服务是针对负有情报、国家安全或国土安全职责的美国行政机构或军事部门,或者针对这些机构或部门的工作人员和承包商;在交易完成或者提交书面通知或申报之前 12 个月内的任一时间节点,曾经持有或者收集超过 100 万人的可识别数据;其已证明的商业目标,是去持有或者收集超过 100 万人的可识别数据,且这些数据属

〔45〕 FIRRMA, § 1703 (a) (4).

〔46〕 *Foreign Investment and National Security Act of 2007* (FINSA), Pub. L. No. 110 – 49, § 2 (a) (3), 121 Stat. 246.

〔47〕 *Provisions Pertaining to Certain Investments in the United States By Foreign Persons*, 31 C. F. R. Part 800.

〔48〕 Critical Technologies, Critical Infrastructure, Sensitive Personal Data, 31 C. F. R. § 800. 248.

〔49〕 FIRRMA, § 1703 (a) (4) (D); 31 C. F. R. § 800. 211.

〔50〕 FIRRMA, § 1702 (c) (5).

〔51〕 31 C. F. R. § 800. 226.

〔52〕 31 C. F. R. § 800. 241 (a) (1) (ii), (a) (2).

于所投美国商业的主营产品或服务不可分割的一部分。[53] 由此可知，只有所投资的美国商业持有或收集的个人可识别数据不是来自上述美国政府部门或人员，并且数据量没有达到100万人的门槛，该笔非控制性投资才不属于美国外资安全审查的范围。

当然，如果外国主体对持有或收集个人可识别数据的美国商业的投资达到了“控制”程度，即获得“确定、指导或决定受影响主体重要事项的直接或间接的权力”，[54] 即使这些数据不涉及上述有关国家安全的部门和人员，也有可能会纳入CFIUS国家安全审查范围。2020年3月，美国总统特朗普基于CFIUS审查发布行政命令，要求北京石基公司剥离其收购的美国酒店管理软件公司StayNTouch的100%股权。从该行政命令中“可能损害美国国家安全”以及要求石基公司完成撤资前“不得访问酒店客人数据”的表述来看，大量个人可识别数据对国家安全的威胁是禁止该交易的主要考虑。[55]

（三）域外观察小结

总结来看，美国近期管控数据安全风险的制度探索包括两个方面：一是完善了联邦受控非密信息管理制度，二是将敏感个人数据的国家安全风险纳入了外资安全审查范围。二者出台都是为了应对数据安全挑战，都在一定程度上考虑了数据流动、聚合和分析带来的风险，只不过前者侧重管控敏感数据流转的风险，后者侧重防范敏感数据聚合分析带来的威胁。二者在制度设计上都贯彻了风险管理的思想，只不过风险管控重点和策略有所不同，前者侧重避免政府所持数据泄露给政府部门和相关主体带来损害，策略是数据处理、存储和传输过程中的风险控制；后者强调防范敏感个人数据的国家安全风险，策略是以暂停或禁止涉及敏感个人数据部分的交易来实现风险避免。这些制度设计虽然限于局部领域，但为我们思考数据安全综合性立法提供了一定的启发和参考。

四　范式革新下数据安全立法的基本思路和核心制度

针对信息化3.0阶段的安全风险，本文提出了以数据风险管控为中心的数据安全范式。基于该范式，就数据安全立法的基本思路和制度设计提出以下建议。

（一）范式革新下数据安全立法的基本思路

数据安全立法需要加强顶层设计和系统规划。

1. 从国家安全高度进行数据安全立法体系化设计

从数据的特性来看，数据是信息的载体，在网络环境下表现为比特形式的数字符号，可以承载多种多样内涵的信息，数据安全与信息安全、网络安全必然存在交集。这也使得作为非传统安全的数据安全，无论是数据密集流动的自身安全还是数据聚合分析的利用安全，都与政治安全、经济安全、文化安全、社会安全、军事安全等领域问题交织在一起，和

〔53〕 31 C. F. R. §800.241 (a) (1) (i).

〔54〕 FIRRMA, §1703 (a) (3). 需要指出的是，这种控制包括但并不限于取得多数股权。

〔55〕 Order Regarding the Acquisition of Stay NTouch, Inc. by Beijing Shiji Information Technology Co., Ltd., *Federal Register*, Vol. 85, No. 47, March 10, 2020, pp. 13719 – 13721.

网络安全一样具有牵一发而动全身的全局效应。前文所述滥用数据分析制造感染特定人群的病毒而引发生物安全风险、滥用个性化推荐危害信息内容安全就是例证。乌尔里希·贝克(Ulrich Beck)就曾指出:“在风险社会中,风险一般都会从技术风险自我转换为经济风险、市场风险、健康风险、政治风险等等。”〔56〕从这个意义上讲,我国总体国家安全观辩证、全面、系统的理念,恰恰能为数据安全立法的布局和设计提供明确指引。

数据安全立法的目标应该是在维护国家安全定位下形成专门性规定重点突出、各领域各层次规范相互配合的数据安全法制体系。这里的规范既包括法律、行政法规和规章,也包括国家标准。对于与信息安全、网络安全存在交集的数据自身安全而言,传统信息安全范式和网络安全范式的一系列相关立法,依然是控制数据安全风险的重要依据。以我国为例,这包括《网络安全法》《刑法》《密码法》等,涉及网络安全等级保护、关键信息基础设施保护等制度。数据安全立法并不是否认传统信息安全和网络安全范式立法,而是要补足之前既有范式下静态安全边界防护制度应对数据安全风险的短板。

这就要求专门的数据安全综合立法,应该着重解决其他法律法规尚未规定的新型数据利用安全问题,尤其是事关国家安全、公共安全的突出问题,尽量避免对数据自身安全进行重复立法。从我国目前的数据安全立法制度设计来看,《草案》不少规定还是侧重数据的自身安全,这造成了与《网络安全法》相关规定的某些重复与交叉。建议专门的数据安全立法应该聚焦数据利用安全,就数据自身安全可以只规定与其他法律的衔接条款。对于数据利用安全,要按照可控性和正当性要求来设计风险应对和管控制度。

2. 以风险管控为中心构建数据安全保护制度体系

数据安全范式的核心新要素是风险的可控性,管控数据安全风险立法的总体思考可以根据风险管控的策略展开。一般认为风险管控包括四种策略:接受风险、避免风险、控制或减少风险以及转移风险。〔57〕鉴于绝对安全是不可能的,应该接受一定残留风险〔58〕的存在,平衡安全与发展的关系。另外当避免某些风险的成本过高时,接受一定风险也是合理的策略。从这个意义上讲,近期美国将敏感个人数据交易纳入外资安全审查范围,动辄在没有充分证据的情况下就以国家安全为名禁止交易以求避免风险,〔59〕这实际上是在追求一种绝对安全,忽视了风险防范与自由贸易的平衡,使得安全审查沦为一种政策工具和贸易壁垒。就不可接受风险而言,避免风险和转移风险是强调事前和事后的应对,对于

〔56〕 参见[德]乌尔里希·贝克:《再谈风险社会:理论、政治与研究计划》,载[英]芭芭拉·亚当等编著《风险社会及其超越:社会理论的关键议题》,赵延东、马缨等译,北京出版社 2005 年版,第 334 页。

〔57〕 U. S. Department of Homeland Security, *Risk Management Fundamentals*, April 2011, p. 23, https://www. dhs. gov/sites/default/files/publications/rma - risk - management - fundamentals. pdf,最近访问时间[2020 - 12 - 25]。

〔58〕 我国国家标准《GB/T 25069-2010 信息安全技术 术语》的 2. 3. 26 将“残留风险”界定为“在实现防护措施之后仍然存在的风险”。

〔59〕 除了前述对北京石基公司的行政命令,2020 年 8 月,美国总统特朗普发布行政命令,禁止任何主体与 WeChat 和 TikTok 进行交易,理由之一在于 WeChat 和 TikTok 有可能让美国人的个人和专有信息泄露等,影响美国的国家安全。Executive Order 13943: Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, Executive Order 13942: Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, *Federal Register*, Vol. 85, No. 155, pp. 48637 - 48643.

数据的流动、聚合和分析来说，事中的控制风险才是关键。

控制风险应该从风险的产生入手，数据安全风险主要来自于数据大规模流动、聚合和分析，既有数据自身安全风险，也有数据利用安全风险。对前者如前所述既有制度已有规定，立法重点是管控数据利用安全风险。从阻断风险产生来看，制度建构思路包括两点：一是在数据分类分级的基础上，对高风险数据的流动和聚合进行重点管控，避免这些数据被不当披露和聚合分析，符合可控性要求；二是对数据分析及分析结果的再利用进行规制，避免数据分析滥用带来的危害，符合正当性要求。从目前各国立法来看，前者主要表现在个人信息和商业秘密保护等方面，后者主要表现在为避免个人歧视等对自动化决策〔60〕和算法〔61〕进行规制，现阶段还都只是聚焦在个人权益保护层面。对于事关国家安全和公共安全的重要数据保护以及数据分析规制，尚处于探索之中。笔者认为，规制数据分析滥用应该以规定负面清单为主，比如禁止将数据分析及其结果用于政治广告等。

3. 以重要数据安全为核心管控国家数据安全风险

由于数据分析只有依靠敏感的高风险数据即我国所称的“重要数据”才可能挖掘出危害安全的信息，如果能够实现这些数据的流转限于有权主体之间并处于一定的控制之下，避免这些数据被任意披露和整合，那么就能大大减少数据聚合分析带来的风险，因此上述制度建构思路的第二点在很大程度上要依靠第一点来实现。这说明数据安全立法的关键在于重要数据保护和管控制度。这种重要数据是介于国家秘密和公开信息之间的一类应该被管控风险的数据。对于管控这类数据的理由，可能会有国家安全、产业利益和个人权益等多重考虑，如美国受控非密信息管理除了保护政府部门敏感数据外，还保护个人隐私和企业的专有商业信息。但考虑到前述目前一般已有专门制度防范私主体敏感数据的安全风险，但在防范数据利用导致的国家安全和公共安全风险上存在短板，从实践需求的紧迫性和制度规范的体系性出发，应该将专门性数据安全立法管控重要数据的理由设定为可能严重危害国家安全或公共安全。由此，参考我国相关的法律、立法草案和国家标准，〔62〕本文将“重要数据”界定为“金融、交通、能源、医疗健康、电子政务等领域收集和产生的不涉及国家秘密，但一旦泄露或者聚合、分析后，可能严重危害国家安全、经济安全、社会稳定、公共健康和安全的数据”。

总之，数据安全立法的核心就是确保重要数据安全可控。所谓重要数据的“重要”就是指事关国家安全、公共安全。如此，既可以突出立法重点，也可以避免对数据正常流动和利用造成不当干预，确保数字经济时代数据价值的充分释放。

（二）以重要数据为抓手构建国家数据安全管理制度

应该以重要数据为制度抓手，切实维护国家数据安全。近年来我国通过法律法规和

---

〔60〕 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*, Art. 22, OJ L 119, 4.5.2016, p. 46.

〔61〕 参见梅宏主编：《数据治理之论》，中国人民大学出版社 2020 年版，第 199－205 页。

〔62〕 参见《网络安全法》第 37 条、《个人信息和重要数据出境安全评估办法（征求意见稿）》第 70 条、国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》的 3.5 及附录《重要数据识别指南》、国家标准《GB/T 35274-2017 信息安全技术 大数据服务安全能力要求》的 3.13、《数据安全管理办法（征求意见稿）》第 38 条。

行业标准已经对地理信息数据、科学数据、健康医疗数据、金融数据、工业数据等重要领域数据的保护进行了规范。[63] 借鉴美国的制度经验，应该对不同领域的重要数据建立统一的制度架构。从国内外制度探索来看，重要数据管控的关键环节在于数据的识别认定、安全保护和受控流转，从尽可能不影响数据利用来看，数据流转管控主要是基于数据安全风险评估的安全审查和出境管制。由此，重要数据保护制度主要包括以下方面：

1. 明确重要数据的识别认定制度

虽然立法不可能列举出重要数据的具体范围，但可以规定重要数据识别认定的所涉领域、标准依据、负责部门和相应程序，构建统一的重要数据管控制度架构。

首先，以“抽象概括 + 具体列举”的方式规定重要数据所涉及的重要行业领域，抽象标准可以概括为数据一旦泄露或者聚合分析等，“可能严重危害国家安全、经济安全、社会稳定、公共健康和安全”；在这一标准下可以列举出所涉及的重要行业领域，如金融、交通、能源、医疗健康、电子政务等。需要指出的是，认定某些因聚合分析而影响国家安全、公共安全和重大社会公共利益的重要数据，应采取定性与定量相结合的方式。

以个人信息为例，个人信息一般仅涉及个人权益，不会影响国家安全、公共安全，但达到一定数据量后通过搜索、比对、关联等分析，可能挖掘出数据集背后隐藏的安全信息甚至国家秘密，这种个人数据集合应该纳入重要数据范围。2017 年国家网信办公布的《个人信息和重要数据出境安全评估办法（征求意见稿）》曾规定，“含有或累计含有 50 万人以上的个人信息”“数据量超过 1000GB”等情形的数据出境需要经过安全评估，就是考虑了数据集合的风险。但这种仅规定数据量的方式不足以充分界定数据的风险性，建议借鉴美国外资安全审查关于敏感个人数据的界定，对于纳入重要数据的个人信息集合等，在数据量要素之外，同时界定数据集合的高风险性，比如涉及医疗健康、生物识别等特定种类个人敏感信息，或者涉及关系国家安全、公共安全的特定岗位人员。

其次，明确重要数据认定的负责部门和相应程序。考虑到不同领域数据存在特殊性，将重要数据认定的负责部门设定为各领域各行业的主管部门较为妥当。具体规定可以采用逐一列举方式，按不同领域列明重要数据认定所对应的主管部门，例如规定“医疗健康领域的重要数据保护目录由国家卫生健康委员会认定”。具体程序上建议以重要数据持有者根据相关标准先自主申报、主管部门再予以审核认定的方式为主，辅以主管部门对于重要主体的重要数据可依职权主动认定，对于应申报而未申报的主体应该规定相应的法律责任。鉴于纳入重要数据保护范围的数据处理者会承担法律强制性义务和责任，在重要数据认定程序中应当规定处理者不认可主管部门行政认定时的复议等救济程序。

2. 规定重要数据处理者的安全保护义务

对重要数据匹配特别的保护要求和措施，是切实维护国家数据安全的关键所在。首先，明确重要数据处理者范围以及重要数据安全保护原则。借鉴欧盟《一般数据保护条

〔63〕 部分相关规定包括：《测绘成果管理条例》（2006 年）、《科学数据管理办法》（2018 年）、《国家健康医疗大数据标准、安全和服务管理办法（试行）》（2018 年）、《证券期货业数据分类分级指引》（2018 年）、《工业数据分类分级指南（试行）》（2020 年）、《金融数据安全 数据安全分级指南》（2020 年）。

例》和我国《民法典》关于个人数据/信息处理的定义,〔64〕建议将“重要数据的处理”界定为“包括重要数据的收集、存储、使用、加工、传输、提供、公开等”。这样就能将重要数据保护要求贯穿重要数据的整个生命周期。鉴于数字经济数据安全风险的动态性,应该规定重要数据安全保护原则,作为处理者是否尽到安全保护义务的衡量基线。一是规定最小化数据风险原则,根据数据利用场景在确保正常利用情况下应该最小化数据泄露风险;二是规定保护措施成比例原则,借鉴欧盟《网络与信息系统安全指令》和《一般数据保护条例》的相关规定,〔65〕明确应当采取适当的和成比例的技术和组织措施来管理数据安全风险,这些措施应当确保一定程度的安全并且对于所面临的风险是适当的。

其次,制定与重要数据处理者安全保护义务相配套的、具有可操作性的国家标准。建议结合数据分类分级标准,根据安全风险的等级,制定贯穿数据生命周期不同阶段的具体安全措施,数据处理者可以根据自身情况作出相应选择。制定专门的数据安全风险管理指南,对识别潜在风险、评估分析风险、发展替代方案、决定和执行、监测监督以及风险交流等予以指引。在标准实施方面,要注意区分政府部门和私营部门,对于政府部门要以强制性要求为主,对于私营部门要允许一定的自主性,比如应该统一政府部门重要数据分类分级标准,而私营部门在保证保护水平下可以对数据分类有一定自主空间,当然政府部门可以通过合同机制等将某些标准扩展适用到私营部门。

再次,规定重要数据处理者定期风险评估制度。风险评估是风险管控的基础和关键,是处理者安全保护义务的重要内容。应该明确处理者开展重要数据风险评估的年度频次、实施主体、费用承担、结果处理。如果评估工作由安全测评服务机构承担,考虑到重要数据事关国家安全、公共安全,还应该规定测评服务机构许可准入制度,规范这些服务机构的资质条件、评估流程、评估标准、保密义务、评估结果运用等。为了减少相关企业负担,重要数据风险评估应该与相关评估制度相衔接,避免重复评测。

3. 将重要数据安全审查纳入网络安全审查

对高风险数据利用活动进行国家安全审查和处置,是管控国家数据安全风险的必要手段。这种安全审查不是针对所有数据,而是针对关系国家安全、公共安全的高风险重要数据。数据安全审查的重点应该是重要数据处理环境的安全性和数据聚合分析的可控性,这两方面都以信息技术为基础,可以制定可验证性的技术标准,有建立较高透明度审查的需要和可能。从世界范围看,各国涉及信息和通信技术领域的国家安全审查,包括两种制度设计:一是外商投资国家安全审查;二是专门针对网络信息技术产品和服务的国家安全审查。〔66〕 我国将后者称之为“网络安全审查”。

从近期美国外国投资安全审查制度改革和我国《草案》第 22 条规定来看,目前有将敏感数据纳入外商投资安全审查评估要素的倾向。笔者认为,数据处理活动不能类比为“外商投资”,关切国家经济安全的外商投资安全审查制度也无法满足重要数据安全风险

〔64〕 *General Data Protection Regulation*, Art. 4;我国《民法典》第 1035 条。

〔65〕 *NIS Directive*, Art. 14; *General Data Protection Regulation*, Art. 24.

〔66〕 参见马宁:《国家安全审查制度的保障功能及其实现路径》,《环球法律评论》2016 年第 5 期,第 139 – 141 页。

审查的需要。首先,外商投资是指外国投资者直接或者间接在一国境内进行的投资活动,外资从境外流入境内是单向的,而数据处理活动包括了数据的收集、存储、使用、加工、传输、提供、公开等,数据既会从境外流入境内也会从境内流向境外,远比外商投资活动要频繁和复杂。其次,外商投资安全审查的初衷是维护国家经济安全,审查重点是外国资本控制本国企业的国家安全风险,审查标准较为模糊、透明度较低,这种仅侧重外国投资控制性的审查显然无法涵盖侧重数字环境和数据利用安全性的数据安全审查。从近期美国将敏感个人数据交易纳入外资安全审查的实践来看,仅从外国投资控制性出发考虑数据安全审查,不仅审查标准和程序不透明,还容易导致以安全之名干涉正常贸易和打压他国企业,使安全审查异化成政策工具。因此,应该呼吁建立一种基于技术标准、具有较高透明度的审查制度,避免数据安全审查成为国际贸易壁垒。

从网络安全审查制度来看,其审查重点是信息技术产品和服务的安全性和可控性,而重要数据安全审查关注数字环境的安全性和数据利用的可控性,二者在价值定位和审查重点上有类似性,且前者以可验证性技术标准为基础也能满足后者的透明度要求,这说明前者对于后者具有较大的制度相容性。考虑到提高透明度、避免重复监管、降低合规成本等,应该将重要数据安全审查纳入网络安全审查制度。我国近期施行的《网络安全审查办法》,定位聚焦维护国家安全、审查标准突出供应链安全、审查程序透明合理,[67]平衡了维护安全与自由贸易的关系,明确将“重要数据被窃取、泄露、毁损的风险”列为关键信息基础设施供应链国家安全风险评估的考虑因素,已经在一定程度涉及了重要数据安全评估,为将重要数据安全审查纳入网络安全审查提供了良好的制度基础。

4. 建立重要数据出境管制制度

对于数据跨境流动管制方式,经济合作与发展组织(OECD)概括为 4 种基本类型:不设管制、事后问责、以安全保护为条件的流动、以专门授权为条件的流动。[68] 从重要数据事关国家安全、公共安全来看,此种数据一旦出境可能会大大增加国家安全风险,应当以上述第 4 种方式严格加以管控,原则上应该禁止重要数据出境,例外流出需要“专门授权”。建立重要数据出境管制制度,目前有两种思路:一是将重要数据纳入出口管制制度,例如《草案》第 23 条规定“国家对与履行国际义务和维护国家安全相关的属于管制物项的数据依法实施出口管制”;二是建立重要数据出境安全评估批准制度,例如我国《网络安全法》第 37 条规定,关键信息基础设施在境内收集和产生的重要数据应当在境内存储,确需向境外提供的应当进行安全评估。

试图建立“数据出口管制制度”不可行。理由在于:首先,出口管制制度依赖于管制物项出口许可证以及海关对出境货物的监管,而数据的出境通过互联网传输至境外即可实现,并不存在所谓的数据“海关”和许可制度。其次,出口管制侧重对物项本身安全风险的评估,并不能防范大量数据出境后聚合分析引发的安全风险。我国《出口管制法》目

〔67〕 参见刘金瑞:《中美网络安全审查立法比较评析》,《中国社会科学报》2020 年 8 月 19 日第 4 版。

〔68〕 OECD, *Trade and Cross-Border Data Flows*, January 2019, pp. 16 – 21, https://doi.org/10.1787/b2023a47 – en,最近访问时间[2020 – 12 – 25]。

前也只是将管制物项“相关的技术资料等数据”纳入管制范围,规定“向境外提供出口管制相关信息,应当依法进行;可能危害国家安全和利益的,不得提供”。[69]

上述思路二较为稳妥,但应该明确规定重要数据出境评估的启动方式、评估主体、评估范围、评估标准和结果处理等。鉴于重要数据事关国家安全,重要数据认定及其出境评估应由行业主管部门负责。国家网信办2019年5月发布的《数据安全管理办法(征求意见稿)》规定,网络运营者向境外提供重要数据,应当评估安全风险并报主管部门批准,从文义上看这种评估是运营者自评估,但这种自评估不能代替主管部门的评估。而且,为了维护国家安全的重要数据出境管制制度并不同于域外一般探讨的旨在维护个人尊严的“个人数据跨境流动规制”制度,[70]后者的目的是为了维护个人的人格尊严,应该规定在我国未来的《个人信息保护法》之中。当然,如果大量个人数据集合构成了影响国家安全的重要数据,那么这些数据集合也应该适用重要数据出境管制制度。

[本文为作者参加的2018年度国家社会科学基金重大项目“互联网经济的法治保障研究”(18ZDA149)的研究成果。]

[**Abstract**] The large-scale flow, aggregation and analysis of data in the era of digital economy have posed new risks and challenges that can no longer be addressed by traditional paradigms of information security and cyber-security and, as a result, a new paradigm is urgently needed to ensure data security. This article proposes a new data security paradigm centered on data security risk management: apart from confidentiality, integrity and availability of data security *per se*, this paradigm also tries to ensure the controllability and legitimacy of the security of data utilization. With respect to legislation on data security, China should carry out systematic design of data security legal system from the perspective of national security, construct the data security safeguard system by focusing on data security risk management, and control national security risk by taking important data protection as the core. In particular, the national data security management system should take important data as the key link, establish important data identification system, provide for data security protection obligations of important data processors, incorporate important data security review into the cyber-security review system, and establish the regulatory system for the trans fer of important data out of the country.

(责任编辑:支振锋)

〔69〕 我国《出口管制法》第2条、第32条。

〔70〕 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》,《信息安全与通信保密》2017年第6期,第74-75页。