新时代数据安全风险的法律治理

付霞[1]　　付才[2]

(1.武昌首义学院 新闻与法学学院,湖北 武汉 430064;2.华中科技大学 计算机学院,湖北 武汉 430074)

摘　要:新形势下数据安全风险防控,要树立适度安全观、动态监控、协同防控的治理理念。从完善数据安全立法、落实数据安全法律法规实施、强化数据安全责任、协同构建数据安全信息共享平台、建立数据安全研究领域财政投入长效机制、提升社会数据安全意识等方面,综合开展数据安全风险的法律治理。

关键词:数据安全;风险;法律治理

分类号:D920　**文献标识码**:A　**文章编号**:1673－1395 (2019)02－0058－04

在数字化、网络化、智能化的今天,数据作为重要的生产要素,犹如工业社会的石油,不仅蕴藏着巨大的经济利益,而且隐含着政治利益、国家利益,成为企业实施商业策略和国家保持国际竞争力的必争之物。数据安全作为网络安全的重要内容,不仅关系到个人利益、企业商业利益,而且直接影响着国家安全。数据治理正在从边缘走向网络社会治理的核心。[1]目前,数据安全形势严峻,恶意程序、木马、流量攻击仍处高发态势。据《2017 年中国互联网网络安全报告》,2017 年,国家信息安全漏洞共享平台(China National Vulnerability Database,简称 CNVD)收集新增漏洞 15955 个,与 2016 年相比,漏洞总数增长 46.4%;移动互联网恶意程序样本数 2533331 个,增长 23.4%;境内被篡改网站数量为 20111 个,增长 20%。[2]

一、数据安全的概念与内涵

与数据安全近似的概念,还有网络安全、信息安全。《中华人民共和国网络安全法》(以下简称"网络安全法")第 76 条规定: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。据此可以得出,数据安全是网络安全的重要组成部分。"信息安全包括信息的完整性、保密性、可用性的保持;计算机通信设施运行的正常;信息内容的合法和受法律保护。"[3]因此,数据安全是信息安全项下的内容,信息安全同时还要求数据承载内容的合法性。

按照我国网络安全法的规定,数据安全是指数据的完整性、保密性、可用性。完整性是指数据保持其生成时的完好状态,在存储和传输过程中不能被篡改、破坏和丢失;保密性是指数据的非普遍公开性,非经授权的用户不能获取该数据,以限制和控制数据的访问主体;可用性是指数据能够满足访问主体的需求,可用性与安全息息相关,因为攻击者会故意使用户无法访问相关数据。

随着电子商务、电子政务的广泛推行,数据不仅记录了人们生活、工作、学习的点点滴滴,而且记载了企业运行、公共服务提供、社会治理的信息,在传统的社会之外,数据同时也构建了数字化社会全貌的副本。因此,只有数据安全,才有个人信息安全,才有企业安全、社会安全和国家安全。

二、数据安全风险的来源

在数据生命周期里,数据收集、存储、传输、分析和使用等过程中,数据安全都面临各种风险。大数据安全威胁渗透在数据生产、流通和消费等大数据

收稿日期:2018－11－10

基金项目:湖北省教育厅人文社科项目"数据交易法律治理研究"(18G119)

第一作者简介:付霞(1980－),女,湖北通城人,讲师,主要从事信息安全法、知识产权法研究。

产业链的各个环节,数据源的提供者、大数据加工平台提供者、大数据分析服务提供者等主体,都是威胁源。[4]笔者试图从网络结构和环境视角来分析数据安全风险来源。

(一)网络和数据设施、设备缺陷

关系到国计民生和公共利益的信息、能源、交通等行业的关键信息基础设施,由于涉及大体量的重要数据,是数据安全风险来源的重点区域。数据一旦被篡改、泄露,可能导致有关行业及其他社会公共服务大面积受到牵连并陷入紊乱,对社会秩序和稳定造成极大的破坏和威胁。我国信息网络基础设施还远远不能满足自主可控、安全可信的要求[5],并且在万物互联的形势下,关键信息基础设施面临的风险增大,大规模的互联互通为攻击者提供了更多的攻击路径。普通个人电脑、手机、传感器、路由器、移动存储器等都可以成为数据收集、流通、使用的介质,也因此会成为数据安全问题的窗口。目前,我国网络和计算机产品,如服务器、数据库等产品国产化率低。如果被预先植入后门,很难发现,一旦发生数据安全事故,造成的损失将无法估量。

(二)系统漏洞和恶意攻击

上海社科院互联网研究中心发布的《大数据安全风险与对策研究报告》遴选了近年来十大国内外典型数据安全事件,有七件是因为系统有漏洞而遭到攻击,如 2017 年全球范围爆发的勒索软件(WannaCry)感染事件,该勒索软件利用 WindowsSMB 服务漏洞进行攻击,全球 100 多个国家数十万用户中招,我国多个行业也遭受不同程度的影响。[4]

国家互联网应急中心发布的《2017 年我国互联网网络安全态势报告》显示,网络安全风险来源主要是恶意程序、安全漏洞、拒绝服务攻击;通过篡改、窃取数据或攻击服务器,对数据安全造成极大威胁,严重危害人民群众的个人信息安全和财产安全。[2]由于系统漏洞客观上一直存在,因此也为非法之徒提供了可乘之机,蓄意攻击防不胜防。

(三)内部工作人员道德风险

上述十大数据安全事件中,有两件是内部工作人员所为,内部人员利用工作之便泄漏大量用户数据,这反映了数据控制的企事业单位在数据内部管理上的失序。“未采取有效的数据访问权限管理、身份认证管理、数据利用控制等措施,是大多数企业内部人员数据盗窃的主要原因。”[4]

(四)数据安全管理薄弱

数据安全法律保障不完善。目前,在国家层面上已建立以《网络安全法》为基础的数据安全法律保障体制,中央网信办已经印发《国家网络安全事件应急预案》。国家网信办、工信部、公安部、广电总局、其他行业主管部门等均已出台有关数据安全保障的具体办法和规定,数据安全风险治理的法律制度框架已基本形成,但对数据这一基础性战略资源缺少专门的体系化的法律保护制度。对个人信息的保护、关键信息基础设施保护、网络安全等级保护、网络安全信息共享、网络安全监测预警和信息通报、网络安全应急处置、网络安全风险评估等做了制度安排,但缺少可操作性的配套措施。同时,《网络安全法》第 8 条规定:“国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关……负责网络安全保护和监督管理工作。”可以看出,国家网信部门是网络安全统筹协调机关。涉及刑事犯罪,由公安部门负责;涉及电信、互联网用户信息安全,则由电信主管部门及其他有关机关在各自职责范围内负责监督管理工作。这种“1+X”的监管方式符合目前数据利用的管理现状,但从数据安全的长效保障来看,不利于数据安全统一保障机制的形成。

网络运营单位缺乏数据安全的系统管理。许多网络运营单位高层对数据资产所面临的安全风险的严重性认识不足,或者对数据安全管理认识局限于信息安全技术,没有形成一套合理的数据安全规章制度来预测、防范、化解数据安全风险,对员工缺少必要的数据安全法律法规和风险防范教育与培训,缺乏相应的数据管理责任制度。

数据安全管理的意识还停留在传统的“出事后补救”阶段,这显然已不适应新时代数据技术高速发展的形势。数据不断地被抓取、流通、利用,处于变化之中,因此,数据安全风险具有动态特征。如果等风险发生后再采取措施,后果将不可控制。

三、新时代数据安全风险的治理理念

适度安全观。适度安全是指在进行数据安全制度设计时,协调安全和自由、效益等价值之间的关系,不能为了保障安全而牺牲网络用户的自由、数据技术的创新发展。我们同时也要看到,数据技术的发展为数据安全技术发展提供了更多的机会和可能。习总书记指出:安全和发展是一体之两翼、驱动之双轮,安全是发展的前提,发展是安全的保障;要处理好两者的关系,做到协调一致、齐头并进。“在现今的工业国家现代化发展进程中,社会的安全阀

随着现代化程度的不断提升而不断地脆化。”[6]社会在不断发展的进程中,也在不断产生各种风险,安全风险也不可避免地存在。“绝对安全不具有技术上的可能性,抑或是要支付巨额成本。”[7]

动态风控。静态数据价值有限,数据只有在流通、使用过程中,其价值才会被发现、被挖掘出来。数据安全风险治理理念要从以保护静态的资产为核心变成数据流动优先的动态风险监测与控制,对于已知风险可以监控,对于未知风险可以感知和关联,能够全天候、全方位感知安全态势。“如果收益远大于风险损失,小的风险就可以接受以流动增值优先,但需要防范系统性的风险,同时要对风险具备感知能力,在风险变大时及时感知出来并进行处置。”[8]

协同防控。协同论的主要观点为:“不同属性的、千差万别的系统存在于整个环境中,各个系统间存在着相互影响又相互合作的关系。”[9]协同论现在被引入社会科学领域,与治理理论相结合,形成协同治理理论。由于数据安全风险来源的专业性、影响的普遍性,完全依靠政府的管制难以有效防控风险的发生。在数据安全风险防控上,网民、社会组织、企事业单位、政府很容易达成协同防控数据风险的共识。因此,只有多元主体有效参与、共管共治的协同防控,才能顺应新时代安全风险防控的形势。

四、新时代数据安全风险的法律治理

(一)完善数据安全立法

建立专门的数据保护法。《国民经济和社会发展第十三个五年规划纲要》中提到“把大数据作为基础性战略资源……助力产业转型升级和社会治理创新。”基于国家安全的至高利益,应建立专门的数据保护法,将数据从网络、信息系统的保护中分离,作为独立的保护对象;对大数据的分析、挖掘进行法律上的引导,防止有关敏感数据的使用威胁国家安全。

完善数据权属制度。目前,数据安全立法多采用义务性和禁止性规范,网络运营者负担了诸多的数据安全责任,用户和网络运营者变成了数据权利的对立方,用户为权利人,而网络运营者为义务人,二者并非利益共同体,导致数据保护上权利义务的失衡。赋予网络运营主体数据权利,便是把外在安全要求转化为内在发展需要[10],这样,他们不仅有外在的法律责任要求,也有内在的利益驱动去保护数据安全,企业高层会自觉自愿地推动构建数据安全管理制度。物权法上有句谚语,“有恒产者有恒心”,用在数据安全保护上再恰当不过。当然,如何平衡网络运营者和用户之间对于数据的权利,是制度设计者要慎重考虑的。

构建数据安全责任保险制度。数据安全事故给网民带来极大的经济损失,随着网民数据权利意识的逐步成熟,一旦发生数据安全风险,网络运营者可能面临群体性诉讼及其带来的不可预估的赔偿责任。因此,数据安全责任保险制度对网络运营者来说,不失为化解数据安全风险责任的制度选择。责任保险是保险制度体系中已经比较成熟的险种,并且在实践中被证明是有效化解风险的法律策略。数据安全责任保险可以以此为经验,构建以数据风险为保险标的的制度。美国、英国、德国、印度等国家的保险企业早已开始了网络安全保险,对网络入侵、计算机病毒、网络攻击等造成的客户损失进行赔偿;他们对数据安全风险的预估和计算以及保险责任范围的实践经验,值得我们学习和借鉴。我国于 2016 年首次推出数据安全险,是专门针对黑客盗取云计算数据、保障企业云上数据安全的保险。

建立统一的数据安全监管机构。统一的监管机构及监管执法,有利于确保数据安全法律实施的效率,有利于克服行业之间利益割据而形成统一的数据安全防控形势。

(二)落实数据安全法律法规的实施

网信机构会同相关行业主管机构经常性开展数据安全专项检查,将关键信息基础设施安全检查作为检查工作的重点。按照数据安全法律法规和国家强制性标准制定具体检查办法,明确检查对象和程序,依法开展工作。根据检查情况,制定数据安全“白名单”和“黑名单”,将数据安全保障机制完善的单位列入“白名单”;对不符合法律规定的企业,按照法律规定责令改正,或依法责成其承担行政责任;对构成刑事责任的,移交有关司法机关;违法情节严重者,列入“黑名单”。对“白名单”单位给予奖励或政策扶持,对“黑名单”单位予以经常性监督和检查。

网络安全风险评估也是一项常规性、强制性工作。《网络安全法》第 38 条规定:“关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次监测评估……”第 53 条规定:“国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制,制定网络安全事件应急预案,并定期组织演练。”目前尚没有统一的风险评估标准和方法,网信机构可以在听取行业协会、企业、科研机构等单位意见的基础上,出台试行办法。同时,监督检查关键信息基

础设施的运营者对安全风险的年度自查;健全网络安全事件应急工作机制,定期演练应急预案。“争取做到尽早发现风险,隔离风险,减少损失和应急恢复,尽最大可能保障关键基础设施的持续运转。”[11]及时总结数据安全风险防范的经验,做到风险发生前能预防,风险发生时能控制,风险发生后要问责。

(三)强化数据安全责任

合理界定数据安全监管机关的职能范围,明确监管责任,遵循权责一致的原则,强调法治精神,在法定范围内监管。主管领导要提高数据安全意识。行业主管机构要依法对本行业进行指导、检查,督促其落实数据安全防控措施。对渎职、玩忽职守的工作人员实行问责,情节严重者,追究其法律责任。

落实关键信息基础设施防护责任。行业、企业作为关键信息基础设施运营者,承担防护责任。关键信息基础设施运营者应设置专门的安全管理机构和负责人,定期对从业人员进行网络安全教育、技术培训和技能考核,对数据进行容灾备份,制定网络应急预案并定期进行演练。其他网络运营者也要确定数据安全责任人,对数据安全人员进行数据安全责任、网络安全管理制度、操作规程的培训,切实落实数据安全保护责任。

(四)协同构建数据安全信息共享平台

协同社会组织、企业建立数据安全信息共享平台,通过及时的安全信息交换,实现数据安全风险识别、评估、预防、控制的技术和资源的共享。共享的信息主要指技术漏洞、恶意攻击、网络入侵、计算机病毒以及应对技术和措施。《网络安全法》第 29 条、第 39 条规定了国家支持网络运营者之间以及行业组织成员之间建立安全保障协作机制,网信部门参与安全信息共享机制的构建。按照法律法规,根据自愿原则,鼓励企事业单位参与信息共享平台,完善共享工作机制和程序,利用大数据挖掘分析数据安全信息。

(五)建立数据安全研究领域财政投入长效机制

互联网核心技术是网络安全的命门。习近平总书记在中国科学院第十九次院士大会、中国工程院第十四次院士大会上指出:“关键核心技术是要不来、买不来、讨不来的”,一定要发展互联网核心技术。信息安全技术属于前沿、高精技术,需要足够的财政保证。因此,要建立数据安全领域财政投入长效机制,制定相应的法律和政策措施,建立数据安全科研资助专项基金,同时鼓励各级地方政府、企事业单位加大对数据安全技术的投入,尽早实现对网络核心技术的突破,构筑坚实的数据安全技术防线。

(六)提升数据安全意识

通过各种媒体、宣传阵地,宣传数据安全的重要性及风险的来源,告知社会保护好个人数据及隐私,以防止人身及财产安全受损,不要轻易允许个人数据被收集和使用。开展各项数据安全的竞赛及讲座活动,让数据安全的法律法规及数据安全意识更加深入人心,让数据安全意识成为老百姓日常安全意识的一部分。

参考文献:

[1]马民虎.新时代网络社会治理创新的法制议题[J].信息安全研究,2017(12).

[2]国家计算机网络应急技术处理协调中心.2017 年中国互联网网络安全报告[R].北京:人民邮电出版社,2018.

[3]马民虎.网络安全法适用指南[M].北京:中国民主法制出版社,2018.

[4]张衡.大数据安全风险与对策研究——近年来大数据安全典型事件分析[J].信息安全与通信保密,2017(6).

[5]倪光南.eID 是保障网络主权、安全和发展的需要[J].国家治理,2015(Z1).

[6]薛晓源,刘国良.法制时代的危险、风险与和谐——德国著名法学家、波恩大学法学院院长乌·金德霍伊泽尔教授访谈录[J].马克思主义与现实,2005(3).

[7]崔聪聪.中国信息安全立法的宏观分析与制度设计探究[J].苏州大学学报(哲学社会科学版),2014(1).

[8]信息安全焦点人物专访[EB/OL].https://baijiahao.baidu.com,2018-07-25.

[9](德)H·哈肯.协同学——自然成果的奥秘[M].戴鸣钟,译.上海:上海世纪出版集团,2005.

[10]周汉华.建立激励相容机制保护数据安全[J].当代贵州,2018(21).

[11]王玥,马民虎.“互联网+”时代关键基础设施信息安全法律保护研究[J].西北大学学报(哲学社会科学版),2016(5).

责任编辑 叶利荣　E-mail:yelirong@126.com