[DOI]:10.19685/j.cnki.cn11-2922/n.2021.02.001

论我国数据安全保护法律制度的完善

马忠法,胡　玲

(复旦大学 法学院 上海 200433)

摘　要:《中华人民共和国数据安全法(草案)》第九条明确了国家、企业和个人等参与数据安全协同治理体系构建的重要性。对此,在界定数据安全概念之含义并对其进行分类后,应意识到重要数据和敏感数据之安全应比一般数据安全更需要受到重视。针对数据泄露事件频发使得数据安全受到普遍关注之现象,分析现行数据保护法律制度内容及其不足十分关键。在前述分析论证基础上,结合数据治理主体的多元性等方面,可以在数据安全保护法律制度完善方面做出如下努力:宏观层面,政府应完善政府数据保护法律制度,完善数据安全标准,指导企业构建数据安全体系;微观层面,企业应明确责任并制定系统的数据安全管理制度,而个人应树立对个人信息保护的主动防范意识,提升保护隐私和个人数据维权意识,采取积极有效的数据保护防范措施。

关键词:数据安全;法律保护制度;完善对策

中图分类号:D 912　　**文献标识码:** A　　**文章编号:**2096-9783(2021)02-0001-07

引　言

随着数字化世界的到来,数据成为各国博弈的新领域。随着数据的急剧增长,数据安全风险也随之提高,但是无论是国内法律还是国际规则尚缺乏应对经验和智慧。《中华人民共和国数据安全法(草案)》(以下简称《数据安全法(草案)》)(2020年7月3日发布)既是践行中国一直倡导的网络空间命运共同体理念,也是中国为全球数据治理贡献的中国方案和智慧。《数据安全法(草案)》是构建以《国家安全法》为核心的国家安全法律体系的重要组成部分,国家安全保护是其出台的出发点之一,数据安全是国家安全的组成部分。可以说,二十一世纪是大规模放松管制和私有化的时代,许多国家的关键基础设施(如能源、交通、金融和医药等领域)已交由私营部门掌握,入侵者正不断瞄准这些关键基础设施领域。同时,个人信息安全也时刻牵动着社会各界的神经,已经可用的大量信息使重新识别变得容易。数据安全主要侧重于防止通过入侵或泄漏而对数据进行未经授权的访问,而不管未经授权的一方是谁①。数据安全目前是大数据新时代的主题,在新时代进行科学有效的数据安全治理,确保数字经济的持续健康发展是我国国民经济和社会发展的重要任务。《数据安全法(草案)》第九条明确了国家在建立健全数据安全协同治理体系过程中,有关部门、行业组织、企业和个人等应共同参与数据安全保护工作。下文主要从政府、企业和个人三个层面进一步探析数据安全保护法律制度的完善问题,尤其侧重个人数据和重要数据的安全保护。

一、数据安全的定义、分类及其保护法律制度完善的必要性

(一)数据安全定义及其分类

1.数据安全概念的界定

安全通常是指保护资产(如建筑物、设备、货物、

基金项目:2018年国家社会科学基金重大项目"'人类命运共同体'国际法创新研究"(18ZDA153);2018年国家社会科学基金重点项目"'人类命运共同体'国际法理论与实践研究"(18AFX025);上海市教育委员会人文社科重大项目"创新驱动发展战略下知识产权公共领域问题研究"(2019-01-07—00-07-E00077)

作者简介:马忠法(1966—),男,安徽滁州人,教授,研究方向:国际经济法、国际商法;

胡　玲(1985—),女,江苏溧阳人,博士研究生,研究方向:国际贸易的知识产权法。

① DILLON PHILLIPS, Data Privacy vs. Data Security: What is the Core Difference? DATA SECURITY, JULY 7, 2020.see https://www.tokenex.com/blog/data-privacy-vs-security. 最后访问时间:2020年8月13日。

存货、在某些情况下还包括人员等)不受威胁。数据安全(信息安全)通常是指"保护(数据)信息免受各种威胁以确保业务的连续性、风险最小化以及最大化投资回报和商业机会"[②],以及"组织或机构维护对其运营至关重要的信息的系统、媒体和设施的过程。[③]"本文认为,数据安全通常指数据的机密性、可用性和完整性,即依靠各种流程和措施防止未经授权的个人或组织使用或访问数据。数据安全需要确保数据准确可靠,并且在具有访问权限的人员需要时确保数据可用。实践中,"数据安全"关注如下两个方面:一方面,信息系统,如计算机系统、网络和软件;另一方面,通过信息系统进行记录、存储、处理、共享、传输的数据、消息和信息[④]。

2.数据安全分类

(1)按数据安全级别划分:特别数据安全和一般数据安全

特别数据安全的保护适用于重要数据和敏感数据。重要数据是指与国家安全、经济发展,以及社会公共利益密切相关的数据,具体包括"未公开的政府信息、大面积人口、基因健康、地理、矿产资源等"[⑤]。重要数据一旦泄露可能会直接影响国家安全、经济安全、社会稳定、公共健康和安全。敏感数据是个人数据中需要特别关注的一种类型,一般是指"一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇的个人信息[⑥]。就本文而言,敏感数据主要指:种族或民族血统、政治意见、宗教信仰或其他类似性质的信仰、身体或精神健康或状况(或任何遗传数据)、性取向和其他相关活动、有关司法程序的任何信息、任何个人财务数据。一般数据安全保护适用于除重要数据和敏感数据以外的普通数据。

(2)按数据安全主体划分:政府的数据安全、企业的数据安全及个人的数据安全

实践中,数据治理主体呈现多元性,政府、企业和个人是数据安全治理的直接参与者和主要利益相关方。政府数据安全保护涉及:管理自身政务数据、建立数据安全标准、为社会组织合法合理收集、使用数据提供规范指引及加强个人数据保护公共宣传。企业数据保护范围包含其经营过程中涉及的一切数据,其中个人数据和重要数据需要额外关注。个人是当今互联网的主要用户,尽管侵犯隐私报道连篇累牍,绝大多数用户依然心存侥幸或选择漠视,但是只要互联网存在一天,个人就应加强自我防范意识,保护自身信息不被泄露和滥用。

(3)按数据生命周期的安全管理划分:静态的数据安全、传输中的数据安全、正在使用的数据安全

数据安全管理应贯穿整个数据生命周期,即处在静态中的数据、传输中的数据和使用中的数据。静态数据是指以任何数字形式存储的非活动数据,静态数据可能位于硬盘驱动器或数据库、云存储或其它位置,由于数据存储的聚合性,静态数据常常成为攻击者的主要目标。传输中的数据是指数据从一存储地向另一存储地进行移动,此种数据也很容易受到攻击,无论是通过专用网络、本地设备、还是公共/不可信空间。使用中的数据保护最容易被忽略,在对使用中的数据进行保护时,除了访问控制和用户身份验证,还应采用同态加密等安全技术。总之,数据保护方案必须贯穿数据生命周期中的各个环节。

(二)数据泄露事件频发对数据安全保护法律制度的完善提出了迫切要求

现在的大型数据泄露事件,几乎到了每天都会曝光一次的频率。根据国际数据公司(IDC)预测,至2020年,全球四分之一的人口将受到数据泄露的影

② ISO/IEC 27002:2005, Information Technology-Security Techniques-Code of Practice for Information Security Management (June. 2005)。

③ FFIEC, IT Examinations Handbook - Information Security (July 2006) at p. 1, see https://ithandbook.ffiec.gov/media/222209/ffiec_itbooklet_informationsecurity-2006.pdf. 最后访问时间:2020年8月6日。

④ 此处要保护的数据、消息和信息包括了以下各种数据:有关员工、客户、潜在客户和其它个人的个人身份信息;公司财务信息即有关公司交易的信息、商业秘密和其它与公司通讯有关的信息(包括电子邮件)以及各种其它类型的公司数据。数据形式多样,包括:信息、文档、录音、图像、视频、软件以及其它电子和纸质形式的内容。

⑤ 参见《数据安全管理办法(征求意见稿)第三十八条(五)。

⑥ 何渊主编,《数据法学》,北京大学出版社,2020年7月,第7页。

响，在这个高度连接的世界中，这些数据泄露行为对许多组织及其领导人来说都是迫在眉睫的威胁⑦。纵观国际商业机器公司（IBM）发布的《2020数据泄露成本报告》⑧，我们可以看到，恶意攻击、系统故障、人为错误这三类是导致数据泄露事件发生的根本原因，其中系统故障是导致政府等公共部门数据泄露的主要原因。我国也发生过不少大型数据泄露事件，对个人和企业造成了很大损害⑨。在数据的作用与地位日渐重要的今天，数据安全关乎国家安全，关乎市场组织数字化发展和未来的商业模式及竞争力，任何数据泄露事件将对市场组织的正常运营、收入和声誉造成重大影响，同时，数据安全也关乎着个人信息隐私保护。

二、我国现行数据安全保护法律制度及其不足

数字经济的发展离不开技术研发和法制保障，在某种意义上，法制建设和完善起着基础性作用，因为良好的法律制度能激发市场主体的积极性、创造性。

（一）我国现行数据安全保护法律制度的现状

1. 基础性法律规范

事实上，我国正在不断完善数据安全相关制度和规则，保障个人数据和重要数据安全的同时充分发挥数据的经济价值，并不断推动数据安全协同治理机制的形成。2016年《网络安全法》首次提出了重要数据的概念，并在第三十七条规定了关键信息基础设施运营者掌握的重要数据境内存储及出境应进行安全评估⑩。《数据安全法（草案）》在第三章“数据安全制度”和第四章“数据安全保护义务”中，从国家需要建立的保护制度和重要数据的处理者应承担的保护义务两方面，对重要数据保护做出了规定。为降低人们在使用那些必需采集个人信息的平台或软件时发生信息泄露风险，《网络安全法》第四十一条明确规定，网络运营者收集、使用个人信息，应当遵循安全、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的方式和范围，并经被收集者同意⑪。《民法典》第一千零三十四条明确了个人信息的保护范围，其中“电子邮箱”和“行踪信息”首次被明确纳入了个人信息范畴，进一步加强了对个人信息的保护；第一千零三十五条从个人信息的处理原则和条件方面进行了规定⑫。《个人信息保护法》（草案）已正式全文对外发布，全文共八章七十条，在总则、个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人处理者的义务、履行个人信息保护职责的部门、法律责任和附则等多个层面设计和建构个人信息保护的立法框架。草案整体上对个人信息提供了高标准的保护⑬。

随着信息技术的高速发展，大数据正在成为一种

⑦ Maddie Davis, Damaging After-Effects of a Data Breach, July 25, 2019. see: https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach/. 最后访问时间：2020年8月16日。

⑧ Cost of a Data Breach Report, IBM Security, 2020. see: https://www.ibm.com/security/digital-assets/cost-data-breach-report/Cost%20of%20a%20Data%20Breach%20Report%202020.pdf. 最后访问时间：2020年8月6日。

⑨ 2016年8月26日，顺丰速递湖南分公司宋某被控“侵犯公民个人信息罪”在深圳南山区人民法院受审，由于对内部人员数据安全管理存在缺陷，顺丰出现过多次内部人员泄露客户信息事件。2012年1号店内部员工与离职、外部人员内外勾结，泄露90万用户数据。见：http://world.people.com.cn/n1/2017/0519/c1002-29287418-5.html. 最后访问时间：2020年8月16日。

⑩《网络安全法》第37条，见 https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html?keyword=网络安全法. 最后访问时间：2020年12月10日。

⑪《中华人民共和国网络安全法》，见 https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html?keyword=网络安全法. 最后访问时间：2020年12月10日。

⑫《中华人民共和国民法典》，见 http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml. 最后访问时间：2020年12月10日。

⑬《中华人民共和国个人信息保护法（草案）》，见 https://www.baidu.com/link?url=vEQpo-7-t3yl_xsw83-J-rPO2stQdleUMkle81SsfGVDX0EFU7d1JGgKYQptWPG9R1wEfKZZ9sFlwe9A3LHk51kYNybp_fWPT-I1ym1JQgOymZ9J5ku5aiwWDGsmxKK&wd=& eqid=f5a3dcab0006b08d000000065fd22026. 最后访问时间：2020年12月10日。

全新的国家实力要素⑭。数据的安全直接关涉国家经济和社会发展,上述数据安全法律制度为相关数字实践提供了重要制度基础。

2.中央和地方性法规及规章

(1)政府数据管理。政府数据包括广义及狭义两个层面,狭义的政府数据主要是政府所拥有和管理的数据,如气象、教育、医疗、金融等不同领域的各种数据;广义的政府数据则与政府部门的工作内容相联系,涉及政府在履行职能而需要收集的外部大数据,具体包括政府及其相关机构在履职过程中形成和掌握的各类统计数据,如国内生产总值、财政及国际收支、物价指数及税收、国土资源、人口就业、交通治安等各类数据,在此之中还涵盖互联网舆论数据。我国保障数据安全的工作随着政务数据开放才逐渐重视起来,2015年,国务院发布《关于促进大数据发展行动纲要》,提出了对涉及国家利益、公共安全、商业秘密、个人隐私、军工科研生产等数据保护,之后,各地也陆续出台了大数据或政务数据安全方面的条例、办法和细则等文件。2019年1月1日,天津市开始实施《天津市促进大数据发展应用条例》,此条例围绕大数据发展应用的迫切需求和趋势,充分发挥大数据在商用、民用、政用方面的价值和作用,构建大数据发展应用新格局,并在极大程度上保护用户的信息和数据⑮。政府部门存储的数据要比私营部门大得多,且往往重要得多,但是经常将其保存在陈旧且更易受攻击的系统上,因此公共部门面临的挑战更加严峻,打算进行数字化转型的政府将网络安全视为一项重大挑战。可以说,公共部门比任何其他部门都面临更多的安全事件和数据泄露⑯。

(2)个人数据安全保护。《国家统计信息网络管理暂行规定》《互联网信息服务管理办法》等法规规章从各个角度对各种个人信息进行了多维保护。同时,在一些特殊行业和领域,也制定了相关法规对个人信息加以保护,如卫生部关于印发《对艾滋病病毒病感染者和艾滋病病人管理意见的通知》、国家卫生和计划生育委员会、国家中医药管理局关于印发《医疗机构病例管理规定(2013版)》等。随着大数据和云计算技术的发展,个人信息被收集的途径和方式越来越多,但是收集的目的、方式和类型缺乏统一和明确的法规和制度来进行管理。政府面临着网络数据监管的失控,个人信息泄露事件频频发生,非技术性因素引发的隐私泄露已严重影响互联网的信任度。

3. 数据安全标准

数据安全是组织机构信息安全体系的重要环节,许多组织机构并不充分了解自身的数据安全能力,行业内急需一套评估组织机构数据安全能力的标准规范。为落实《网络安全法》中"国家鼓励开发网络数据安全保护和利用技术,促进公共数据资源开放"及"国家建立和完善网络安全标准体系"等要求,响应《大数据发展行动纲要》中"健全大数据安全保障体系,强化安全支撑;完善法规制度和标准体系,科学规范利用大数据,切实保障数据安全"的主要任务。2016年,全国信息安全标准化技术委员会(TC260,简称"信安标委")成立了大数据安全标准化特别工作组(SWG-BDS),连续开展了数项数据安全标准研制项目。至2019年12月,已有四项数据安全国家标准正式发布:GB/T 35274-2017《信息安全技术 大数据服务安全能力要求》、GB/T 37932-2019《信息安全技术 数据交易服务安全要求》、GB/T 37973-2019《信息安全技术 大数据安全管理指南》、GB/T 37988-2019《信息安全技术数据安全能力成熟度模型》。这样的标准能够帮助各行业、组织机构基于统一标准来评估其数据安全能力,发现数据安全能力短板,查漏补缺,最终提升互联网行业的整体安全管理水平和产业竞争力,促进数字经济发展。同时,2020年,国家信安标委正式立项国家标准《信息安全技术重要数据识别指南》,从公布的草案稿来看,该标准简化了重要数据定义、明确提出了重要数据的主要分布;不再沿用行业分类的方

⑭ 胡健,基于大数据的国家实力:内涵及其评估,中国社会科学,2018年第8期,第185页。

⑮《天津市促进大数据发展应用条例》见 https://www.pkulaw.com/lar/6defd43bea317b6912b17aa70e516405bdfb.html?keyword=《天津市促进大数据发展应用条例》。

⑯"2015 Data breach investigations report" Verizon, 2015.see http://higherlogicdownload.s3.amazonaws.com/GOVERNANCEPRO - FESSIONALS/a8892c7c-6297-4149-b9fc-378577d0b150/UploadedImages/Landing% 20Page% 20Documents/DBIR% 20Execu - tive%20Summary%20vv%204-10-15.pdf. 最后访问时间:2020年8月14日。

式，而是从数据的作用、受破坏后可能带来的影响等角度，对重要数据做分类。这对重要数据保护实施起到了指导作用。

（二）我国现行数据安全保护法律制度的不足

我国数据安全法律制度是对当今数字化世界中出现的不安定因素提出的中国方案和对策，对全球数据治理有着积极意义，也是未来指导数据安全实践的重要法律基础。但看具体制度本身，普遍偏原则性，缺乏实施指导性。就文章论述的主题而言，主要存在两点不足。首先，《数据安全法（草案）》第九条规定的数据安全协同治理体系，只是对保护主体作了明确，而各主体的实施重点及如何协同都未规定。其次，《数据安全法（草案）》对重要数据比《网络安全法》规定的更系统、明确，但是尚未明确保护的对象，具体存在如下问题：尚未细化管理制度和要求；重要数据保护权限过度“下放”；需要协同重要数据和个人数据保护；需要协同重要数据和数据分类分级。

此外，政府既是政府数据的直接管理者，也是落实国家数据安全实施的重要执行和监督主体。但是，由于缺乏法律的明确指引，现实中存在以下问题：政府数据安全管理主体分散，政府机构内部、企业，甚至第三方机构，都会因直接或间接接触数据而影响数据安全；法律问责机制缺失，一旦发生数据泄露，对相关责任人的惩处不足以使当事人严肃对待；政府数据安全的投入不足，无论是资金、技术还是人才方面的投入都远低于发达国家。此外，政府需出台更详细的规则或指令以指导企业数据安全保护实践，同时还应加强个人数据隐私侵犯的执法活动等。

三、我国数据安全保护法律制度的完善建议

鉴于上文分析的数据安全保护法律制度存在着诸多不足，本文提出如下相关的完善建议。

（一）尽快制定通过我国的《数据安全法》

2020年7月3日，全国人大常委会第二十次会议审议了《数据安全法（草案）》并公开征求意见，本法作为数据安全领域的专门法律，体现了国家立法层面对数据安全的高度重视，也为实践中各数据保护主体具体实施数据保护指明了努力方向。《数据安全法（草案）》公布后受到了学界、实务界等领域的学者与专家的广泛关注和探讨，并提出了许多建设性的完善建议，相关立法部门应尽快汇总、综合并提炼社会各界的有益意见、建议，争取早日通过并颁布《数据安全法》，为我国的数据经济的安全发展保驾护航，为保护有关当事人合法权益提供立法依据。

（二）在全球数字治理背景下构建和完善数据安全制度

随着信息技术发展日新月异，数字经济蓬勃发展，极大影响着人类的生产生活，对各国经济发展、全球治理体系、甚至人类文明都有着深远影响。数据已代替了传统的商品、货币成为了21世纪跨境流通最主要的要素。在全球分工合作日益密切背景下，保护数据安全与促进数字经济发展同样重要。数据安全法律制度的构建和完善应放眼全球，分析全球数字治理发展现状和趋势，将中国数据安全治理方案融入到全球数字治理体系中去。中国近期提出的《全球数据安全倡议》便是对全球数字治理的最新实践，《数据安全法》的最终稿形成和出台也应响应这一时代主题。

（三）避免过度原则性规定，注重法律的实施指导意义

纵观数据安全法律制度，尚存在待改善之处，其中最重要的一点是增强法律的实施指导性，避免抽象化和原则化。《数据安全法（草案）》中规定的由政府、企业、个人等构成的数据安全协同治理体系应明确相关原则及各自的侧重点，如政府层面应着力于顶层设计、加强数据安全执法等；企业应致力于完善内部数据安全合规管理机制；个人应加强对数据安全和数据隐私本身的识别和认识，并熟悉个人数据（隐私）保护相关法律法规。具体应从以下几个层面进行完善。

1. 完善政府数据保障体系

第一，确保数据安全。首先，政府部门必须审查其数据以确定敏感程度；其次，加强内部人员管理并进行数据安全培训。此外，应充分利用大数据和成熟的分析技术检测行为异常的员工，以应对政府部门的内部威胁。总之，网络威胁的不断演化需要政府协同企业和安全服务提供商以共享有关漏洞、威胁和补救措施的信息。第二，保持警惕，充分认识威胁。这意味着需要了解哪些数据是入侵者最想要的，哪些网络犯罪分子对这些数据最感兴趣以及网络入侵者最有

可能用于渗透系统的黑客。第三、加强复原力构建。复原力指政府机构抵御网络攻击的能力,即能够抵御破坏并动用各种资源以最大程度减少其影响的能力。有复原能力的机构通常会以最小化访问权限,对数据进行加密和匿名化处理以限制其可用性,同时会持续扫描是否存在漏洞,以便在发生入侵事件时仅泄露少量信息。对政府公共机构而言,复原力关乎公众信任重建。总之,政府数据管理应采用柔性技术和管理制度并行,使之成为推动政府职能转变、提升国家治理效能的重要催化剂⑰。

2. 指导企业构建数据安全体系

首先,政府应以确立"监督、促进和协作"为指导准则;其次,政府应加强企业"合理"或"适当"等法律安全合规性要求的指导,无需告知公司必需采取哪些特定的安全措施,但是应指导企业建立相应流程,该流程旨在识别和评估风险,执行针对这些风险的适当安全措施并确保其实施有效且持续更新。总之,安全是一个过程,有关安全的法律义务应侧重于在特定情况下可以达到预期安全目标的合理方法。

3. 加强数据安全执法

为保护公民个人信息,近期我国正开展全国网络安全执法大检查,展开对大数据安全的整治工作,加大对违法违规APP的清理整治力度。这在一定程度上严惩了许多不法网络平台/APP经营者,用行动证明了国家对个人信息保护的重视。但对数据安全的执法应有重点、有区分,重点稽查、惩治涉及人民生命健康、财产安全的网络平台/APP,对于其它一般行业实施企业自律和行业监督双轨制。

(四)明确企业数据安全保护责任,提升个人数据安全保护意识

1. 企业应制定系统的数据安全管理制度以履行安全保护责任

企业应明确其数据安全保护责任并采取有效措施来切实履行,而系统的数据安全管理制度是重要的有效措施。该措施应该至少包含以下五个方面:第一,建立企业数据安全责任制;第二,制定网络服务政策;第三,制定系统安全策略;第四,建立安全事件应对机制。一旦发生安全事件,应在第一时间采取适当的措施应对,包括对事件的评估和报告,以及如何解决导致该事件的源头以及如何防止该问题再次发生,并及时将损失等降低到最小程度;第五,制定内部数据许可使用政策。公司应制定相应规则明确许可使用政策的定义和范围,并让相关员工在相应政策文件上进行签署,以便后续发生不当使用可以采取纪律处分等。企业一旦实施了统一的数据安全政策,那么在该政策生效实施后,应至少每年对其进行两次审查,进行风险合规评估,风险评估包括确定风险、评估风险的发生概率及潜在影响、采取措施纠正严重风险、然后评估这些步骤的有效性。

2. 自然人个人应提升数据安全保护意识

自然人个人信息泄露渠道越来越多,但就个人而言,首先要重视个人信息保护,避免在不经意间向他人或外界透露自己的信息。时刻提高警惕,不断加强个人信息保护意识,增强辨识能力。一方面应深刻认识到信息泄露对自己可能带来的严重威胁和损失,牢固树立对自身信息保护的主动防范意识,切实做到防患于未然,不给不法分子留下侵权或犯罪的机会;如个人通话记录、行走轨迹、网上浏览记录、购物记录、社交网站记录等信息,不法分子可能会通过大数据分析推算出个人的性别、年龄、职业、爱好、社交等隐私信息。另一方面应建立保护隐私和个人数据维权意识并采取积极有效的数据保护防范措施。法律是对个人信息保护最直接的手段。遭遇信息泄露的个人有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止;个人还可向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报;个人还可依据《民法典》《消费者权益保护法》等,通过法律手段进一步维护自己的合法权益,如要求侵权人赔礼道歉、消除影响、恢复名誉、赔偿损失等。

结 语

互联网是一个旨在共享信息而非保护信息的平台,这种连通性推动了公共和私营部门的创新和效能。互联网有着自身运转的机制和风险,在过去几十年中,我们通过互联网连接了经济和社会,一定程度

⑰ 谢军,为政务数据"上锁——织密数据安全防护网,人民日报,2020年8月12日,第1页。

上改变了人们的生活方式和学习模式等，为人们带来了诸多便利。同时，互联网也为网络犯罪分子提供了商机，早期的黑客行为主要是为了寻求刺激和娱乐，但是，慢慢地出现了牟利动机，甚至吸引了有组织、有预谋且成集团化的全球犯罪组织。现在很多国家将网络空间归类为新疆域，与海陆空同样重要，有可能成为新的战场。信息系统是该疆域最为重要的运转基础，而其最核心的资产是数据，因为数据构成了互联网运行的基本要素，是信息系统发挥功能的命脉。因此，数据安全的保障是网络安全的核心议题，特别是关乎组织数字化发展和未来的商业模式及竞争力，任何数据泄露事件将对组织的正常运营、收入和声誉造成重大影响。安全是大数据发展的重大挑战，数据需要流动、共享、运用以发挥其应有的价值，但也要保护好国家机密、商业秘密和个人隐私。在技术层面上，区块链技术可以较好地解决数据安全问题，通过加密、溯源，可以追溯数据泄露者，让人不敢轻易违法。上述诸目标的实现需要相应的法律制度的保障，为此，我国应尽快构建和完善以《数据安全法》为基础的数据安全保护法律体系。

参考文献：

[1] DILLON PHILLIPS, Data Privacy vs. Data Security: What is the Core Difference?[J]. DATA SECURITY, JULY 7, 2020.

[2] ISO/IEC 27002:2005, Information Technology-Security Techniques-Code of Practice for Information Security Management (June. 2005).

[3] 何渊. 数据法学[M]. 北京：北京大学出版社，2020:7.

[4] Maddie Davis, Damaging After-Effects of a Data Breach[J]. July 25, 2019.

[5] Cost of a Data Breach Report, IBM Security, 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/Cost% 20of% 20a% 20Data% 20Breach% 20Report% 202020.pdf.

[6] 胡健. 基于大数据的国家实力：内涵及其评估[J]. 中国社会科学. 2018(8)：185.

[7] "2015 Data breach investigations report" Verizon, 2015. http://higherlogicdownload. s3. amazonaws. com/GOVERNANCEPROFESSIONALS/a8892c7c-6297-4149-b9fc-378577d0b150/UploadedImages/Landing% 20Page% 20Documents/DBIR%20Executive%20Summary%20vv%204-10-15.pdf.

[8] 第45次《中国互联网络发展状况统计报告》[R]. 中国互联网络信息中心，2020(4).

[9] 中国网民个人隐私状况调查报告[R]. 腾讯新闻、企业智库研究出品，2018(8).

[10] SANS Institute, "CIS critical security controls: Guidelines," https://www.sans.org/critical-security-controls/guidelines.

[11] Ed Powers and Mary Galligan, "The pursuit of cybersecurity," Risk and Compliance Journal, July 27, 2015.

[12] 谢军. 为政务数据"上锁——织密数据安全防护网[N]. 人民日报，2020-8-12(1).

[13] Risks, Harms and Benefits Assessment Tool, Global Pulse. https://unglobalpulse.org/wp-content/uploads/2019/02/risk-harms-and-benefits-assessment-tool.pdf.

[14] 鲁传颖. 网络空间安全困境及治理机制构建[J]. 现代国际关系，2018(11)：51.

[15] 董青岭. 大数据安全态势感知与冲突预测[J]. 中国社会科学，2018(6).

[16] Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data[J], SETON HALL LAW REVIEW, Vol. 47:995,2017.

(下转第75页)