数据安全保护法律制度的完善思考

张燚兰
浙江工商大学，中国·浙江　杭州　310018

【摘　要】随着信息技术高速发展，各类数据得到大幅增长，数据已成为重要的国家战略资源，但与此同时，数据安全风险也随之提高。为应对数据领域现存的安全风险和挑战，切实维护我国数字经济的安全发展，保障相关当事人的合法权益，亟需完善数据安全立法，构建更为严密的数据安全法律制度。基于此，本文从数据安全的定义出发，简述数据安全保护法律制度的现状，为解决我国数据安全法律保护多重困境提出建议。

【关键词】数据安全 法律保护 制度完善

Thinking on Improving the Legal System of Data Security Protection

ZhangYilan
Zhejiang Polytechnic University,Hangzhou,Zhejiang, 310018

[Abstract]With the rapid development of information technology, all kinds of data have increased substantially, data has become an important national strategic resource, but at the same time, data security risks have also increased.In order to cope with the existing security risks and challenges in the data field, effectively safeguard the security development of China's digital economy, and protect the legitimate rights and interests of the relevant parties, it is urgent to improve the data security legislation, and build a more rigorous data security legal system.Based on this, this paper starts from the definition of data security, briefly describes the status quo of data security protection legal system, and puts forward suggestions to solve the multiple difficulties of data security legal protection in China.

[Key words] data security legal protection system is perfect

随着互联网全面普及，信息技术与社会生活紧密联系，数据在推动经济发展、促进社会治理能力现代化等方面呈现出日益重要的影响。然而，每项技术的演进发展也会有潜在的风险，数据在发挥价值效益的同时也易产生数据盗用、泄露等现象。可见，数据安全已成为网络治理的基点和难点。相关部门针对网络安全领域，尤其是数据安全等为各界关注的热点问题，做出了一系列重要战略部署，取得了一定的制度、实践成果。数据安全已然成为我国网络安全迈向新阶段的重要阶梯，如何使数据安全得到更全面的保障、如何有效解决实践中主要问题和困境、如何科学规制数据安全立法是现阶段亟待思考的问题。

1　数据安全的概念界定及保护的必要性

当前，全球科技革命再次掀起热潮，数据作为人类把握事物整体、关联性、发展方向的工具，不仅为防控疫情、医疗救治等提供了有效途径，也给全社会带去了福利。然而，数据的快速增长，也伴随数据安全风险的提高，如数据泄露、数据盗取、数据滥用.....为有效解决该问题应该从数据安全最基本的概念出发，追本溯源解决难题。

1.1数据安全概念界定

首先，数据的概念。当前数据安全法律体系对其的定义各有不同。一般认为数据“是指对客观事件进行记录并可以鉴别的符号，是对客观事物的性质、状态以及相互关系等进行记载的物理符号或这些物理符号的组合。它是可识别的、抽象的符号。”由此可认为数据的范围不仅包含网络数据也包含线下实体数据。

其次，数据安全的概念。根据《数据安全法》第三条第三款规定①现阶段的数据安全是一种维持数据保护和数据利用间的平衡状态，保证数据处理活动免受内外部威胁。相较之下，“传统”数据安全则更侧重于对数据资源的保护，主要通过防范黑客等外部威胁保护数据不被攻击、泄露等，并运用区域隔离、边界防护等数据技术进行保护。本文认为，数据安全的定义还可展开为对数据完整性、保密性、有价性的理解，即数据在被使用的过程中，不能被减损或虚增；数据未经所有者同意，不可被其他第三人获得使用；数据作为客观事物，需要具有能够满足主体需求的能力。建议对数据安全的理解从以下方面统筹完善：保护所有数据的代表信息的安全，实现数据本身和其内容的双重保障；保护数据之上附着权利的安全，如财产权、人格权等。此外，也需要考虑数据所处环境的制度背景、政策选择等因素的影响。

1.2数据安全保护的必要性

当前，数据的应用已经普及于社会生活的各个领域，不仅影响经济、医疗等行业，更影响人的价值、消费观念。但数据也是一把双刃剑，在享受数据带来福祉的同时，面临隐藏的各种安全风险。

从个人安全利益出发。当人们使用淘宝、抖音等软件，个人数据便可能于泄露风险的境遇，海量的数据被泄露或非法出售，间接促成不法分子进行诈骗、推销或者实施其他违法行为。据统计我国公安机关2020年共侦办电信网络诈骗案件20万余起，数据类犯罪已成为多数犯罪的基础性犯罪模式。②如侵害个人信息罪中的敲诈勒索，无疑是以非法获得个人数据为前提。由此可见网络犯罪数量多、惩处难度大，数据安全保护至关重要。

从社会安全利益出发。大数据、云计算等科学技术正以前所未有的速度改变着人们的生活，智能家电、智能汽车、智能服务随之深入推进。于创新同时带来的是隐患，以自动驾驶为例，车辆在其专用信息传输通道上进行信息交互，指令系统做出反应，而攻击者恰好可以利用信息交互的开放路径，发布虚假信息、篡改具体数据，对其进行精准攻击。一旦攻击成功，将会影响行驶的安全，给不特定的使用者带去损害。以此类推，通过对数据的拦截、篡改，控制智能应用的功能，制造社会混乱，这对公共安全利益的维护无疑是极大的威胁。

从国家安全利益出发。2021 年 7 月，国家网络安全审查办公室对滴滴展开全面网络安全审查，强制要求滴滴出行 APP 下架。此事件的发生警示人们，数据安全问题不再仅仅是安全的维护更是国家之间的博弈。域外国家或地区适用长臂管辖原则实施的行为，无疑会给国家安全造成更大的威胁。

当数据的重要性日渐提高，潜在风险却仍得不到有效管控，对个人、企业和国家都会造成重大的损害。数据安全不仅关乎个人隐私的保护，关乎市场经济的正常运行、数字行业的未来发展，更关乎国家安全和国际关系。在此背景下，数据安全保护显得更为重要，加大数据安全保护的研究力度，提高数据收集、传输、使用的安全性，进而，激活数字市场，推动国家经济、科技发展。

2　我国数据安全保护法律制度的现状及困境

数据在推进经济社会发展的同时，也带来了前所未有的风险和挑战。为使数字经济健康发展，法治建设的完善和发展将起到关键性作用。

2.1 我国数据安全保护法律制度的现状

我国数据安全保护领域基础性的法律框架体系已初步构建，以《网络安全法》《数据安全法》《个人信息保护法》三法为支撑，为现代网络安全、数据安全、个人信息安全保护提供坚实的制度保障。其一，提出有效解决网络安全问题的制度规则，促进我国网络空间立法进程，提升我国网络空间竞争力；其二，力在规范数据处理活动、保障数据安全、推进数据开发，填补数据安全保护立法空白，提高数据安全保障能力；其三，结合国内信息保护实际经验，对“个人信息权益”以私法和公法结合的方式协同监管和重点保护，为个人信息权益筑起保护屏障，利于个人信息应用活动的开展。可见上述数据安全立法体系已为网络安全、数据安全、个人信息保护安全提供了基础制度保障。

同时，我国数据安全保障工作随着相关法律法规规章的陆续出台，从国家、社会、个人层面落实以数据安全为重点的管理防御制度，已取得一定成效。国务院率先发布的《关于促进大数据发展行动纲要》重点保护国家利益、商业秘密、个人隐私等数据。与之相应，各地方、重要行业和领域也以数据安全、数据开放、数据跨境等问题为中心展开立法设计，如《天津市数据安全管理办法》《医疗机构病例管理规定》等。

数据安全保护立法迅速发展，但不得不承认，数据安全保护立法体系仍有待加强，目前仍停留于原则性立法模式，尚缺集中型的规范体系和具体化的制度规定。近期《数据安全法》的出台虽昭示着我国数据保护和应用将全面进入法治轨道，但从当前法规来看，其中对于数据跨境、重要数据的保护等关键制度没有更深入的思考和完善。因此，我们需要通过分析数据安全法律保护现阶段的成果，反观数据安全法律保护存在的不足，为完善法治建设提供方向。

2.2 我国数据安全保护法律制度的困境

2.2.1 调整对象不明确

《数据安全法》将“数据”定义为任何以电子或者其他方式对信息的记录，即所有形式记录的信息，可见调整对象界限模糊、范围过广。《网络安全法》第七十六条所规范的网络数据，从语义上可简化为以一定条件产生的电子数据。此外，《促进大数据发展行动纲要》中提出“信息技术与经济社会相融触发了数据的巨幅增长，将数据提升到国家基础战略资源的关键地位”。从该表述中可得国家保护的数据源于信息技术，间接指明该数据的范围偏向为电子数据。随信息化、数字化的推进，无论是电子数据范围的扩大还是传统非电子数据向电子数据转化的趋势都是不可逆的，于数据这一领域的安全风险更多指向电子数据，数据立法调整和规范的也主要指网络电子数据。为与《网络安全法》等法律相互协调，避免制度交叉导致立法资源的浪费，“数据”的定义需要精简。如果数据调整对象过于宽泛，会提高立法工作难度，无法全面覆盖规制对象。

2.2.2 责任义务落实不到位

企业作为数据资源主要掌握者，理应承担维护数据安全的重要责任。《数据安全法》第八条规定在进行数据处理活动的过程中，应当遵守规定，遵守社会、商业道德，秉持诚信，切实维护数据安全。笼统的责任要求，一定程度放宽了对企业的限制，易使牟利者在追求经济利益时钻法律空子。例如：第二十七条虽然补充建立健全流程数据安全管理制度、倡导开展数据安全教育培训，但未明确指出其适用对象，难以束缚相关企业的行为。此外，当企业违反原则性条款，并没有针对性的惩处手段进行追责。由此可知，现有的法律对企业数据安全保护义务的规定仍不够明确，为确保数据安全管理工作有序进行，发挥法律制度的权威性，需要构建更为完善的责任类型体系。

2.2.3 有效监管制度缺位

世界范围内为维护数据环境的安全在执法层面纷纷设立相应的监管机制和监管机构，瑞典《数据保护法》、法国《信息、档案与自由法》率先提出了科学的数据监管制度，美国、英国、欧盟也紧随其后。而我国数据安全监管在数据利用、处理等核心环节欠缺有力的监管机制。一方面，《网络安全法》第 8 条规定由国家网信部门统筹协调网络安全和相关监督管理工作，但该保护制度侧重于对网络运行安全的监管，未将数据安全作为关注重点对象，只能给予数据安全有限的保护。另一方面，《数据安全法》没有确定统一的监管机构，仍然延续多部门、多地区交错的管理体制，容易造成不同监管主体间的冲突，增加治理成本。总体而言，数据安全监管需要将个人信息、商业秘密、国家安全数据作为主要对象，由系统的监督体系进行统筹兼顾、专项管理，从而保障数据安全、国家主权。

3　数据安全法律保护的完善思考

近期，工业和信息化部召开互联网行业专项整治行动动员会议，宣布开始为期半年的数据整治行动。其中，于数据安全领域，着重管理企业数据收集、传输、存储等行为，重点

防范企业违规操作等问题。

可见，数据作为资源、作为资本引发的数据安全问题已成为关注焦点。构建完善的数据安全保护法律体系，有助于解决数据安全立法困境。下文通过分析立法困境，提出数据安全法律保护的完善建议，从理论上增强我国法律体系的时代适应性。

3.1构建和完善数据安全制度

目前，我国解决数据安全问题相关的《民法典》《网络安全法》已开始施行，《数据安全法》也落地实施，《数据安全管理条例》被列入《国务员2021年度立法工作计划》，数据安全管理法律体系正在逐步形成。本文认为立足我国实际探究完善我国数据安全法律保护，可以促进基层实际与顶层设计双向互动，从而提升数据应用效能。

3.1.1细化数据定义，缩小调整范围

《数据安全法》第三条对数据的定义与数字经济时代，以电子数据为主的表现形式和传播形式相悖。随大数据的发展，传统数据数字化成为必然结果。而且《网络安全法》、《关于加强网络信息安全的保护决定》都已明确将大数据时代的数据理解为电子数据。建议《数据安全法》对数据的定义进行限缩性修改，缩小其包含范围。

其次，将对个人信息数据保护的任务交给正准备施行的《个人信息保护法》。该法明确个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。对比数据与个人信息概念的范围，可知个人信息被包含于数据之中，个人信息作为子概念已被该法明确保护，无需《数据安全法》重复规范浪费立法资源。将数据内涵限为代表国家利益的基础战略资源，以及涉及企业、个人权益的重要数据。除此之外，为增强法律的实用性，应将重要数据电子化，排除对非电子数据的管控，明确界定数据安全保护法律制度中的数据定义。

3.1.2建立严格的问责机制

目前我国制定的侵犯数据安全法律救济体系较为分散，惩治力度不足、效果不佳，需要建立更为严格的问责机制。从民事责任来看，我国《民法典》在第一百一十一条和第一千一百九十四条笼统规定“自然人个人信息受法律保护。网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任。”，缺乏对数据安全针对性的问责机制。从行政责任来看，《治安管理处罚法》第四十二条仅规定了侵犯个人隐私情节严重的处罚情节。从刑事责任来看，《刑法》第二百五十三条仅设立了侵犯公民个人信息罪。纵观以上立法，发现我国对数据活动违法行为的问责追责笼统而缺乏针对性，不能明示违法的严重性。通过建立严厉的事后问责制度，提升数据活动的违法成本，从民事、行政、刑事三大层面分别切入增设侵害数据安全保护权承担民事责任的特定情形，加大处罚力度、增设处罚种类，以实现法律的震慑作用。推崇对违法行为进行投诉举报、诉讼；丰富行政处罚手段，对轻微数据安全违法行为进行及时纠正；构建违法数据行为的罪名认定，以国家强制力惩罚犯罪。

3.1.3构建全面的数据安全监管体系

我国现阶段对数据安全监管体系的建设仍停留于行业归口式管理模式、要求行业部门各自负责各自领域。根据《网络安全法》第八条③并结合《数据安全法》第五、六条的规定可以发现，我国现阶段数据安全监管基本框架为：由国家安全领导机构或网络安全和信息化委员会统筹决策，各地区、部门对其工作范围内数据安全承担责任，网信部门对其职务范围内事务及进行协调、监管，行业有关部门履行本行业内数据安全监管职责，公安、国家安全机关执行职务范围内的数据安全监管管理工作。

分主体监管本在于利用各个监管主体的专业性，然而，在监管协调机制尚不健全、监管主体职能范围尚不清晰、数据活动存在地域性的背景下，难以避免各监管主体监管竞争等现象。一套用以统筹各部门职能、协调各部门工作，弥补监管漏洞的监管制度亟待构建。可以通过建立专门的数据安全监管机构，以防出现监管主体之间相互推诿；通过完善监管机构执法依据和规章条例，做到依法执行；还可采取“总分式、多维度”模式，上级统筹安排，下级具体落实保障，由网信部门、公安、国安及电信等行业主管部门共同构成上级监管体系，各地区下级部门、行业各司其职、负责具体的数据安全监管工作。纵横覆盖，建立多重数据安全监管体系，互相协作补位、弥补数据安全管理漏洞。

3.2明确数据企业数据安全保护责任

企业应建立数据安全防范体系。第一，可以根据工信部《电信和互联网用户个人信息保护规定》完善企业个人信息保护制度。目前，部分企业对用户个人信息安全不够重视，安全防范措施不够到位，管理制度不够完善，数据安全责任没有落实，需要进一步完善用户个人信息保护制度，规范企业数据收集、使用的过程。第二，可以建立数据防护专项部门，包含对数据的决策、管理和监督，全面执行数据安全管理工作。第三，可以根据《数据安全》第二十二条、第二十三条建立数据安全风险报告、数据安全应急响应机制，倡导企业建立数据报告制度，对信息实时监测、动态管控；在发生数据安全事件时，及时向有关部门报告，防止危害扩大，并及时向用户发送有关警示信息，将损失降到最低。第四，做好企业数据的备份制度，对数据收集、处理进行重点备案，当系统出现意外时快速、准确的恢复数据。

企业还应制定责任制度，督促自我发展，严格把控数据收集、处理的尺度。在追求最大利润、维护股东利益的同时兼顾社会公共利益，实现社会效益与自身经济效益的协调发展。尝试通过建立社会责任机制，鼓励企业积极保障消费者、数据原始权利拥有者数据权、隐私权等基本权益，有效防治企业违法行为。

3.3提升个人数据安全保护意识

数据安全责任不仅仅于国家、社会，还在于每个参与者。对每个数据拥有者、数据处理参与者开展法规政策培训和风险警示教育更为重要。开展数据安全宣传教育，提高群众个人数据安全保护意识。于个人而言，首先，提高对个人信息的主动防范意识，增强辨识能力，避免无意向他人透露自己的信息，深刻认识数据泄露可能带来的危害和损失。个人在向商业性盈利平台、政府信息网络等提供个人数据前，需要认真阅读用户数据保护协议，明确个人与数据收集者之间的权利义务，以及自身数据被保护的范围。其次，提高个人数据维权意识，配套落实数据保护防范机制，以现有的法律出发分别从不同方面为个人数据安全保护提供了制度屏障。

3.4参与全球数据安全治理

在数据安全治理领域，也应践行多边主义理念，加强与他国的交流，共同建立一个全球化的数据安全治理合作体系。积极参与国际数据领域的制定，发挥各国、各国际组织的主体作用，推动符合人类发展需要的数据安全国际规则。联合各组织、机构建立数据安全国际交流机制，利用国际合作渠道宣传数据安全，合力打造安全的数据运行环境。从《网络空间国际合作战略》的发布，到《全球数据安全倡议》的提出，中国始终在为推进全球网络安全治理体系的建设努力奋斗。建立多边全球互联网治理体系，保障网络空间和平与安全；拉动网络空间发展优势，共享数字化成果。从网络安全国际治理和国际交流合作中、从全球信息技术革命中汲取有益于中国发展的实践经验，扩大我国数据安全立法制度的国际影响力，为我国的科学技术、经济活力、产业发展带去新动力。

参考文献：

[1]王利明. 数据共享与个人信息保护[J]. 现代法学, 2019, 41(1): 45-57.

[2]刁胜先,何琪.论我国个人信息泄露的法律对策——兼与GDPR 的比较分析[J].科技与法律，2019(03).

[3]姜盼盼. 大数据时代个人信息保护的理论困境与保护路径研究[J].现代情报，2019.39(06).

[4]吴伟光. 大数据技术下个人数据信息私权保护论批判[J].政治与法律，2016(07).

[5]岳文婷. 大数据背景下我国个人信息法律保护的完善[J]. 中北大学学报(社会科学版).2017(05).

[6]张里安，韩旭至. 大数据时代个人信息权的私法属性[J].法学论坛，2016.31(03).

[7]闫立东. 以“权利束”视角探究数据权利[J]. 东方法学，2019(2): 57-67.

[8]黄道丽，原浩，胡文华.《数据安全法》(草案)的立法背景、立法定位与制度设计[J]. 信息安全与通信保密，2020(8): 9—15.

[9]何渊.数据法学[M].北京: 北京大学出版社，2020: 7.

[10]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.

[11]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).

[12]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).

[13]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).

[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]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).49-55,66.

[17]孙嘉蔚.略论我国消费者权益保护法律制度构建与完善[J].时代教育(教育教学版),2012,(7):298.

[18]梁准.完善我国个人信息保护法律体系的对策研究[J].现代经济信息,2017,(6):341.

[19]康秀丽.浅论我国个人储蓄存款保护制度的完善[J].经济技术协作信息,2011,(036):8.

[20]刘润英.试论我国著作权的刑法保护体系及其完善[J].青春岁月,2012,(2):212-213.

[21]王艺颖.再论我国互联网知识产权法律保护工作的问题及对策[J].法制与社会,2011,(35):89-89.

[22]梁战平.情报学若干问题辨析[J].情报理论与实践,2003,26(3):193-198.

[23]孔庆江,于华溢.数据立法域外适用现象及中国因应策略[J].法学杂志,2020,41(8):76-88.

[24]李春华,冯中威.欧盟与美国个人数据保护模式之比较及其启示[J].社科纵横,2017,0(8):89-92.

[25]张涛,马海群.基于政策文本计算的开放数据与数据安全政策协同研究[J].情报理论与实践,2020,43(6):149-155.

[26]马忠法,胡玲.论我国数据安全保护法律制度的完善[J].科技与法律(中英文),2021(2):1-7.

[27]马海群,张涛.从《数据安全法(草案)》解读我国数据安全保护体系建设[J].数字图书馆论坛,2020(10):44-51.

[28]许可.数据安全法:定位、立场与制度构造[J].经贸法律评论,2019,0(3):52-66.

[29]刘金瑞.聚焦维护国家安全定位 健全数据安全管理制度——完善《数据安全法(草案)》的若干建议[J].中国信息安全,2020(7):60-63.

[30]胡尔贵.总体国家安全观视域下数据安全立法探讨[J].河北工程大学学报:社会科学版,2020,37(3):52-57.

[31]蒯正明.制度系统的构成、层次架构与有效运作[J].东方论坛:青岛大学学报,2010(5):34-38.

注释：

①《数据安全法》第三条第三款：数据安全是指通过采取必要措施,保障数据得到有效保护和合理利用,并持续处于安全状态的能力。

②参见：朱晓娟,《论跨境电商中个人信息保护的制度构建与完善》,《法学杂志》，2021年第2期。

③《网络安全法》第八条：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依照本法和有关法律、行政法规的规定,在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责,按照国家有关规定确定。

作者简介：

张燚兰，女，1999.11.6，汉族，浙江省杭州市，本科，浙江工商大学，法学。