《学术界》(月刊)
总第302期,2023.7
ACADEMICS
No.7 Jul. 2023

大数据时代个人信息保护的理论反思与规则优化〔*〕

高志宏

(南京航空航天大学 人文与社会科学学院,江苏 南京 211106)

〔摘 要〕新技术的发展弱化了以知情同意机制和匿名化机制为主的传统个人信息保护手段功效,公共数据的需求推动着个人信息保护模式的创新变革,公共利益的相对优位更是限制了个人信息保护的内容范围。《中华人民共和国个人信息保护法》对大数据时代个人信息保护面临的重大挑战作出了制度回应,并在基本原则、调整范围、保护模式等方面呈现出诸多亮点。数据时代的个人信息财产权属性日益增强、公共属性日益明显、积极权利属性日益突出。从隐私向个人信息再向数据的发展演进过程中,立法理念和价值导向亦发生了相应变化,即从严格保护隐私到个人信息保护和自由利用并重,再到鼓励大数据开发和数据产业发展。现代信息技术的发展客观上增加了个人信息保护的难度,以隐私权或自决权为主要内容的个人信息权保护模式受到重大挑战甚至陷入困境。构建具有中国特色的个人信息保护法律制度,必须实现个人信息保护与促进经济发展之间的利益平衡。具体而言,要将个人信息保护事先预防和事中控制确立为主模式,在对信息主体赋权的同时更要强调企业、社会组织、政府机关等在个人信息保护中的义务和责任,采用"积极确权+行为规范"规范模式,完善公共数据和公共利益规则体系。

〔关键词〕大数据时代;个人信息;公共利益;个人信息保护法;数据产业促进法

DOI:10.3969/j.issn.1002-1698.2023.07.011

一、问题的提出

作为我国首部个人信息保护领域的专门性、系统性、综合性法律,《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)已于2021年8月20日经十三届全国人大常委会第三十次会议表决通过,并于2021年11月1日起施行。这是继2016年《网络安全法》专门规定网络信息安全、2018年《电子商务法》专门规定电子商务个人信息保护、2019年《儿童个人信息网络保护规定》专门规定儿童个人信息保护、2020年《民法典》"人格权"编中扩大个人信息保护范围、2021年《数据安全法》专门规定数据安全之后,我国个人信息法治建设的又一里程碑事件,

作者简介:高志宏,法学博士、博士后,南京航空航天大学人文与社会科学学院院长、教授、博士生导师,主要研究方向:经济法。

〔*〕本文系江苏高校哲学社会科学学习贯彻党的二十大精神重点专题研究项目"数据财产法律保护制度研究"(SJZT202311)、中央高校基本科研业务费研究阐释党的二十大精神专项课题"第三次分配、共同富裕与慈善事业高质量法治化发展"(NZ2023004)的阶段性成果。

翻开了个人信息立法保护的新篇章。《个人信息保护法》在禁止“大数据杀熟”、敏感个人信息保护、网络平台特别义务、个人信息跨境流动等规范设计上呈现出诸多亮点,为世界提供了一个充满借鉴价值的中国方案。[1]科学阐释、正确解读和全面落实《个人信息保护法》的基本概念、价值理念、内容体系特别是信息处理规则,成为理论界和实务界的当务之急。

同时,大数据时代的个人信息保护已经突破了传统私法中的二元立法体系,面临着数据利用和信息安全的两难窘境。当前,云计算、区块链、人脸识别、移动互联网等技术方兴未艾,违规收集、肆意获取、过度利用、不当使用,甚至泄露、侵犯、非法买卖个人信息等问题日益凸显,个人信息保护已成为国际博弈的新赛场和国家间竞争的新手段,信息安全作为国际贸易新壁垒的趋势逐渐增强。如何在信息保护与数据共享之间实现平衡,如何在个人利益、企业利益、公共利益之间保持适度张力,亦值得思考和研究。

基于此,本文拟对大数据时代背景下个人信息保护面临的理论困境及其制度突破展开研究。具体从以下三个层面渐次展开:一是学理层面,以数据与个人信息的概念分野入手,梳理学界关于个人信息权益(利)属性的学术观点和分歧焦点,分析大数据时代个人信息保护面临的困境、知情同意机制的弱化以及公共数据和公共利益对个人信息保护的限制。二是解释论层面,以法教义学入手,分析《个人信息保护法》具体规则的立法背景、含义指向及实施建议,为正确落实《个人信息保护法》提供理论支撑。三是从立法论层面,以制度创新入手,分析隐私、个人信息、数据三元法律体系构建的必然性,及其在个人信息保护规则、公共数据规则和公共利益规则等方面的优化要求,从而为我国进一步完善数字经济立法提供智力支持。

二、大数据时代个人信息保护面临重大挑战

随着数字经济的不断发展,数据集聚开发应用背后的隐私侵犯、信息泄露、数据泄密等现象引起社会高度警惕和公众普遍担忧,如何应对大数据时代个人信息保护面临的挑战成为学界亟待解决的问题。

(一)新技术发展弱化传统个人信息保护手段功效

建立在“告知—同意”规则基础之上的知情同意机制被认为是个人信息保护的根基和有效手段。有学者从隐私政策入手,认为“经用户同意的隐私政策将在用户与网络服务提供者之间成立合同关系,在个人信息收集、利用方面具有取得用户授权的效力,此类隐私政策的变更在性质上属于合同变更,应当取得用户同意,否则对用户不产生拘束力”。[2]应当说,这种观点具有相当合理性。以控制权为核心的个人信息保护制度要求收集和处理个人信息应当事先告知并征得信息主体的同意,即使在数据共享中收集、利用个人信息也应当获得信息权利人的授权。[3]《个人信息保护法》所确立的一系列法律制度规则也是以“告知—同意”为核心,这与《民法典》的规定一脉相承,即对个人信息的处理行为原则上都应当以当事人本人的知情同意为前提。

然而,信息技术的发展使得“告知—同意”规则陷入僵化,传统个人信息知情同意机制明显弱化。知情规则是同意规则的前提和基础,知情规则科学与否直接决定了“同意”的质量高低。为保障个人信息主体自由意志的行使和自我决定的作出,需要以透明度标准来判断知情规则,即以一般理性受众在具体场景下能否知情作为判断标准,即所谓的“理性人标准”。[4]对透明度的判断通常以信息处理者是否履行了披露义务为标准,然而实践中,披露的信息收集使用规则往往因为冗繁的表述和专业的内容而“几乎无人有时间、能力和决心浏览复杂的条款和同意的条件”。[5]尤其是在区块链技术的推动下,个人信息“去中心化”“去标识化”“去信任化”,给建立在传统“中心化网络”基础之上的个人信息标识、数据分享自决、监管指向清晰、责任主体明确等

个人信息处理和管理规则带来重大挑战,[6]信息的控制者与信息的处理者之间分离趋势更加明显。因此,信息技术的发展往往会导致知情同意机制流于形式。[7]

知情同意机制的弱化并非意味着弃之不用,相反,对于敏感信息的收集和处理仍应严格遵守单独同意或书面同意的原则,同时应当开启个人信息保护的新路径,即从收集阶段的知情同意机制转向使用阶段的风险监管。[8]一般而言,对个人信息的收集应当遵循“知情同意”原则,即使在紧急情况基于公共利益目的可以不经过信息主体的同意,但在涉及个人敏感信息和隐私信息时仍应当得到信息主体的书面同意或单独同意,且在信息共享时应当遵循风险评估、控制以及责任追究等特别机制。

(二)公共数据需求推动个人信息保护模式变革

传统严苛的僵化的个人信息保护模式不仅限制了数字经济的快速发展,而且也难以满足现代行政管理和社会治理对公共数据的迫切需要。公共数据,顾名思义,是指政府等公权力部门进行行政管理和提供公共服务过程中收集和累积的数据信息。在信息时代,公权力部门在国家管理和社会治理中时常需要收集和存储公民个人信息,并且随着政府管理的精细化,收集信息的广度和深度不断拓展,产生了海量的公共数据。从主体功能角度来看,公共数据是公权力部门基于公共管理/治理需要收集、整理、存储而形成的诸多个人信息,是提高服务效率、改进服务效能的重要举措,并构成了公共资源重要的组成部分,因而,行使公共管理职能的组织是公共数据的权利主体,公共数据不仅为经济发展模式改革提供了动力,而且为传统政务模式变革带来了机遇。

公共数据与个人数据的一个重要区别在于公共属性。公共数据来源于个人信息,是个人信息的集合,似乎具有一定的私权属性,但其作为行使公共管理职能的部门在履行职务过程中收集、整理和存储的个人信息,已经超越了传统的私权范畴,属于公共产品。其一,从公共数据的产生目的看,公共数据是公权力部门为了增进和保护公共利益而在行政管理和公共服务中所形成的,因而具有公共属性。其二,从公共数据的产生依据看,公共数据是公权力部门行使国家权力的结果,因而具有公权属性。其三,从公共数据的使用目的看,公共数据只能用于国家管理和公共服务,因而具有公共资源属性。公共属性也是公共数据与企业数据等其他数据相比所具有的典型特征。公共数据与其他数据一样都不具有人格权属性,但其独特性在于,其属于公共产品但不属于可用于市场交换的“财产”。公共数据有利于提高行政管理和公共服务的实效性、科学性,并且只有在共享中才能体现出交换价值和使用价值,也具有一定的经济属性和财产属性,但来源的公权性以及目的的公益性决定了其具有公共属性,具备非竞争性、非排他性和不可分割性特质,[9]只能用于公共目的,不能用于直接的市场目的。公共数据与个人信息/数据的另一个重要区别在于,公共数据在使用中必须去“个人化”。在社会契约理论视野下,公共数据是公民让渡个人私权(个人信息)给国家公权的结果和表现形式,其必须为了公共利益目的且应当保护个人信息安全。因此,通常情况下公共数据只能是宏观抽象数据,不能识别到具体个人,除非基于特定行政管理需要时才能分解到某个特定个人信息。因此,从范围角度看,个人信息的范围应该比公共数据的范围要广。质言之,政府在履职过程中只能收集那些与公共利益有关的个人信息,对于那些与履行公务无关的个人信息不能收集。

随着互联网、大数据、生物识别、人工智能等技术手段的广泛应用,公权力部门在行政管理和公共服务中收集、累积和存储了海量公共数据,有力推进了数字政府建设,推动了国家治理体系和治理能力现代化。数据具有重要的企业转型、行业发展等商业价值,具有重要的理论研究、公

共服务等社会价值,具有重要的国家治理、社会管理等行政价值。[10]包括经济统计数据、人口普查数据等在内的公共数据,对于预防犯罪、维护社会治理、保障国家安全等方面意义重大。然而,在公共数据管理方面存在的困境亦不可忽视,突出体现在:其一,公共数据的内涵边界模糊不清,信息收集标准缺乏统一的科学标准导致信息被滥采滥用;其二,公共数据形成的正当性不充分,对个人信息的采集缺乏有效约束;其三,公共数据处理与个人信息保护之间的博弈与平衡,致使个人信息泄露空间较大;其四,公共数据处理和监督机制阙如,存在公共数据利用效率低下和信息壁垒等弊端。[11]尤其是在行政权扩张的时代背景下,多部门重复收集个人信息、滥用甚至泄露个人信息的问题广遭诟病。如何在加强公共数据共享与保护个人信息安全之间实现平衡,优化公共数据治理和监管,是公共数据管理面临的主要问题。因此,公共数据治理中,既要满足政府行政管理和公共服务的需要,又要保护个人信息的安全,还要提升公共数据的利用实效,在信息采集、数据处理和数据使用中实现公共利益与个人利益的有效平衡,这对变革传统个人信息保护模式提出了更高的要求。

(三)公共利益优位导致个人信息保护内容受限

"法益论有两个思考方向:一是往理念、价值性方向思考,二是往事实性、因果性方向把握。"[12]利益相关者理论最初应用于公司治理领域,后普遍运用于社会治理之中。所谓利益相关者,是指"任何影响组织目标实现或者受组织目标实现影响的个人或群体"。[13]在利益冲突时,法官在个案中利益衡量也不过是根据个案具体情况赋予不同法益不同的"重要性"。[14]

公共利益为政府收集个人信息并形成公共数据提供了正当性基础,也是限缩个人信息权益的合法理由。究其原因就在于,在个人利益和公共利益的异质利益博弈中,价值位阶决定了公共利益具有优先地位。[15]换言之,公共利益与个人利益相比,由于其涉及不特定多数人长远的、根本的、重大的利益,因而具有优先性,即个人利益为了公共利益应当部分牺牲或让渡,也即可以基于公共利益需要收集和处理个人信息。更何况,某些个人信息与国家安全、公众健康、数据主权等公共利益密切相关。因此,公共行政的目的是维护和增进公共利益或者大众福祉,这是一个不成文的基本原则。[16]尤其是在风险社会,可以为了公共利益适当牺牲甚至剥夺个人利益,"为了保障公共安全,可以采取有害且通常是不道德的方法"。[17]这彰显出大数据时代个人信息保护从个人本位向社会本位的转变趋势和从自主支配到有序共享的逻辑转换,[18]是行政应急原则和行政效能原则的客观要求,也是行政公益目的原则的具体体现。实际上,基于人口普查、预防犯罪、公共安全等重大公共利益而收集和处理个人信息是世界各国的普遍做法。[19]为此,需要从利益相关者角度以及个人信息保护和数据利用两个维度,进行情景化分析和综合考量,[20]消解个人信息保护中各主体之间的紧张关系,实现个人利益、企业利益、公共利益之间的平衡。

保护个人信息是国家的重要义务,[21]保障个人信息安全更是国家机关的应尽责任。然而,国家机关在管理社会事务和惩治违法犯罪过程中会接触和处理大量个人信息,如果职权缺失、程序不当或范围超限,极易成为侵犯个人信息的"危险源"。实际上,由于公权力部门个人信息保护意识不强、保护措施不到位、保护流程不规范等原因导致的个人信息泄露事件已引起了社会的普遍关注。

三、《个人信息保护法》的制度因应与规范亮点

《个人信息保护法》聚焦我国个人信息保护领域社会各界的重大利益关切和突出现实问题,确立了个人信息处理基本原则,健全了个人信息保护体制机制,细化了个人信息保护规则规范,明确了个人信息管理权利义务边界。可以说,《个人信息保护法》在基本原则、内容体系、条文

规则等方面既吸收了国际立法，又开创了中国路径，呈现了诸多亮点，是我国网络数据法律体系中重要的“一块拼图”，填补了数字社会重要的法律板块，具有划时代意义。

（一）处理个人信息原则的确立

法律原则作为法律制度的基本遵循，彰显着法律制度的根本准则和价值取向，具有直接的普遍效力、补漏效力和续造效力。世界范围内，美国在 1973 年“公平信息实践准则”（FIPs）中较早地确立了五项个人信息处理原则，欧盟在 1995 年《个人数据保护指令》（DPD）中规定了处理个人数据的三项原则。《个人信息保护法》立足于我国实际基础并借鉴域外先进经验，通过第 5—9 条确立了个人信息保护的五项基本原则，贯穿于个人信息处理活动的全过程、各环节。这五项基本原则的核心在于对处理个人信息的限制，并通过正反两个方面予以明确：从正面来看，其规定了处理个人信息必须遵守的基本规则，包括合法、正当、必要和诚信，目的明确、合理、直接且影响最小，程序公开透明，保证个人信息质量，保障个人信息安全等，为个人信息处理范围最小化提供了上位法指引。从反面来看，其明确了不得从事的行为，包括误导、欺诈、胁迫处理个人信息，过度收集个人信息，不准确、不完整处理个人信息等，为个人信息处理提供了禁止性规则。

（二）个人信息范围的扩大

世界各国由于文化传统和法律制度的差异，有的立法采用“数据”概念，譬如欧盟、英国、新加坡等；有的采用“信息”概念，譬如日本、韩国、加拿大等。就我国而言，《民法典》第 1034 条[22]和《网络安全法》第 76 条[23]对“个人信息”作出了明确界定，《数据安全法》第 3 条[24]对“数据”作出了明确界定。申言之，我国法律将“数据”和“信息”予以区别对待，信息是数据的内容，数据是信息的载体或形式。

《个人信息保护法》采取“关联说”，将“个人信息”定义为“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”（第 4 条），并进一步将其分为一般信息、敏感信息、匿名化信息、去标识化信息等类别。同时，《个人信息保护法》对未成年个人信息、生物识别、行踪轨迹等敏感信息予以更高强度的保护。首先，通过“内涵 + 列举”的方式对敏感个人信息作出界定（第 28 条），并明确将“不满十四周岁未成年人的个人信息”纳入敏感个人信息范畴。其次，明确了处理个人敏感信息的基本原则，包括特定目的、充分必要性、严格保护措施等。最后，规定了处理个人敏感信息的特别规则（第 29—32 条），如单独同意、书面同意、事前影响评估并告知，以及处理不满十四周岁未成年人个人信息规则。可以说，严格保护敏感个人信息是《个人信息保护法》的亮点之一。

我国个人信息权益内容立法呈现出逐步丰富发展态势。从内容角度看，个人信息权益经历了从隐私权到独立权利、从人格权到人身权财产权并重、从自由权到安全权、从独占权到自决权（包括知情权、同意权、公开权、更正权、删除权、查询权、利用权等）的发展历程。与此同时，个人信息在收集和使用中的利益主体也从初始权利主体扩展至企业、政府等信息的收集者、管理者、利用者，相应地，个人信息的法益价值从单一化向多元化转变而具有了复合性。个人信息权益内容及主体的这一变化给传统个人信息保护立法带来了严重挑战。《个人信息保护法》设专节特别规定了国家机关处理个人信息行为，并与《数据安全法》相结合构成了政务数据处理规则体系。同时，《个人信息保护法》明确“匿名化处理后的信息”不属于个人信息，这一规定对于匿名化处理技术在个人信息保护和数据安全等方面的研发应用具有重要推动作用。

（三）权利保护模式的创新

一方面，《个人信息保护法》通过第四章“个人在个人信息处理活动中的权利”赋予个人充分权利，包括知情权、决定权、查阅权、复制权、可携带权、更正权、补充权、删除权、起诉权等，特别是对个人信息跨平台转移和死者个人信息保护作

出了专门规定。这些权利不仅包括“具体性权利”,而且包括“抽象性权利”,兼具法定性和开放性特征。

另一方面,《个人信息保护法》将个人信息处理者视为个人信息保护的第一责任人,强化其法律义务。这些法律义务除了合规管理义务、信息安全保障义务、活动措施监督义务、合规审计义务、影响评估义务、补救义务之外,更重要的是明确了大型网络平台的特别义务。互联网平台服务是大数据时代的显著特征,也是数字经济区别于传统经济的重要标志。但由于大型网络平台对个人信息处理具有较强的支配力和控制力,因而需要承担更多更大的法律保护义务。为此,《个人信息保护法》第58条专门设定了大型互联网平台特别个人信息保护义务,从而为完善平台内部治理、强化平台外部监督、提高平台经营透明度、构建社会共同保护机制奠定了制度基础。然而,随着人工智能、生物识别、基因检测等新技术、新应用的发展,小型网络平台或者个人信息处理者接触、收集、掌握个人信息甚至敏感个人信息的情形将越来越多,法律将如何应对仍需进一步探讨。

再一方面,《个人信息保护法》在《网络安全法》和《数据安全法》基础上加大了对侵犯个人信息行为的惩罚力度,包括严格的行政责任、民事赔偿责任、刑事责任和信用责任(计入信用档案),明确了国家机关不履行个人信息保护义务的惩罚措施,特别是赋予特定公权力机构(人民检察院)及公益组织(法律规定的消费者组织和由国家网信部门确定的组织)针对侵害众多个人权益的个人信息处理行为享有提起公益诉讼的权利,进一步拓展了我国公益诉讼的范围。

另外,大数据时代,经济全球化不断推进,数字经济方兴未艾,个人信息的跨境流动不可避免且日益频繁,由此而产生的个人信息侵权乃至国家安全风险显著加大。《个人信息保护法》在第三章构建了相对比较系统完善的个人信息跨境流动规则。其一,明确了向境外提供个人信息的条件,包括业务需要、安全评估、保护认证、订立标准合同等;其二,明确了向境外提供个人信息的要求,包括告知义务和单独同意严格规则;其三,明确了维护国家安全和公共利益要求,包括个人信息存储境内规则、限制或禁止提供个人信息规则、采取对等措施规则等。

(四)知情同意机制的强化

知情权和决定权是个人信息权的核心内容,“告知—同意”是保障知情权和决定权的重要手段,因而也被视为个人信息保护的关键规则。《民法典》采取了“知情同意”(第1035条)+“免责事由”(第1036条)的规则设计模式,而《个人信息保护法》采取了更为多元化的规则设计模式,包括个人同意、订立履行合同、人力资源管理、履行法定职责(义务)、维护公共利益等。

《个人信息保护法》第二章围绕“告知—同意”机制构建了我国个人信息处理规则体系。一是确立了告知同意的一般规则和具体类型,包括“充分告知—同意”“重新告知—同意”“单独同意”及“撤回同意”“同意例外”等内容,对“一揽子授权”“跨境转移个人信息”“强制同意”等社会反映强烈的问题作出了回应,不允许过度收集个人信息和以个人不同意或撤回同意为由拒绝提供产品或者服务。根据该规定,互联网平台企业应当在2021年11月1日前调整内部数据合规体系、“隐私协议”(“隐私政策”)以及“注册协议”等,并符合“告知—同意”规则、青少年个人信息保护规则、自动化决策规则、敏感个人信息保护规则等要求。需要强调的是,《个人信息保护法》在适用场景上针对“图像采集识别”“个性化推送”“差别化定价”等人民群众重大关切予以特别规制,要求“公开个人信息”“处理敏感个人信息”“向第三方提供个人信息”“个人信息出境”等活动必须征得个人“单独同意”。二是确立了自动化决策规则。“大数据杀熟”已成为社会反映突出的问题之一,[25]越来越多的个人信息被用于精准营销甚至实行差别性歧视待遇,严重违反了诚实信用原则,也侵犯了个人作为消费

者所享有的公平交易权。《个人信息保护法》第24条对自动化决策进行了规范,禁止“大数据杀熟”。可以说,该条款确立了我国治理算法等自动化决策的基本法律框架,划定了电商平台经济以及数字政府在自动化决策中的合法边界。据此,“数据爬虫”“强制同意”“一揽子授权”“大数据杀熟”“隐私数据售卖”等目前常见的互联网平台行为将受到规制。三是在“告知”义务方面,《个人信息保护法》明确了对个人信息处理者的具体要求:1. 时间要求,即必须在处理个人信息前告知;2. 程度要求,即必须是充分告知义务,包括以显著方式、清晰易懂的语言,真实、准确、完整地向个人告知;3. 内容要求,即必须告知处理者相关信息(包括名称或姓名、联系方式等)、处理相关信息(包括处理目的、方式、信息种类、保存期限等)、个人行使法定权利信息(包括方式、程序等)以及其他依法应告知事项。四是在“同意”方面,《个人信息保护法》明确规定了个人同意的方式、撤回同意或拒绝权利等内容。特别是针对实践中“撤回同意”方式过于隐晦、过于复杂等现象,《个人信息保护法》明确要求个人信息处理者提供“便捷撤回同意方式”,并且明确“个人撤回同意,不影响撤回前基于个人同意已进行的个人信息处理活动的效力”(第15条)。所以,从这个角度看,《个人信息保护法》形成了以“告知—同意/拒绝—撤回同意/拒绝”为逻辑主线的个人信息处理规则体系。

同时,《个人信息保护法》已经意识到公共利益责任豁免原则导致的知情同意机制某些情况下缺乏效益的问题。与《民法典》不同,《个人信息保护法》已不再将“知情同意”机制作为唯一的合法处理信息的理由,而是将其与其他五项合法性基础并列。换言之,《个人信息保护法》跳出了简单的“信息自决”或“告知—同意”二元立法思维模式,而是认可了处理个人信息的复杂性并在此基础上确认了多样化的合法性基础,这也是我国个人信息保护立法模式和立法思路的重大改变。

四、个人信息保护理论的再突破

《个人信息保护法》不仅在立法模式和规范内容上与现行国际通用规则充分接轨,而且在数据处理、信息分类、跨境流动等方面作出了中国探索,为全球数据治理贡献了中国智慧。然而,大数据时代,新技术、新应用、新场景日新月异,数据处理已成为产业升级和社会进步的重要驱动力,个人信息保护理论亦需要再突破。

(一)数据与个人信息的概念界分

个人信息与数据的关系是大数据时代个人信息保护的首要问题,对此理论界存在不同观点。有学者认为,个人数据包含着个人信息,二者实际上是同一事物;[26]有学者认为,个人信息和数据在范围、属性和存在状态等方面存在着区别;[27]也有学者认为,个人信息是内容层面的信息,数据文件则处于符号层面,两者应当进行分别讨论;[28]还有学者对个人信息与数据的关系进行了研究,认为二者在产生基础、内容属性、表现形态、可公开程度等方面都存在很大不同。[29]

数据乃至信息的概念,最初来自符号学、信息学,数据是以0和1二进制单元所表示并能重新还原的信息,是抽象化并用于处理的信息。数据的客体虽然本质上仍然是信息,但应当是经过匿名化或去标识化处理,与信息主体并未直接关联的批量信息的汇集。在个人层面,个人信息与个人数据范围等同,个人数据即是个人信息,这也是个人享有信息权益的客体。但在数据控制者层面,其不能直接处理个人信息,而只能将其进行脱敏处理,形成无法识别或者不能直接识别的数据,此即数据权的客体。在大数据时代,数据已经从个人信息中分离出来,成为一种独立的法律概念,信息与数据之间不是简单的内容与形式抑或内容与符号之间的关系。

数据是信息生成、存储和应用的主要方式,二者可以理解为手段与目的的关系。但个人信息除了以数据为载体和表现形式外,也能够以非数据的其他形式出现。[30]“大数据越发展,信息

分析者就越可能通过某些信息而识别个人,某些之前无法单独识别个人身份的信息,在大数据时代都可能用于识别个人。”[31]换言之,从表达方式角度看,信息的表达方式多种多样,其可以表现为数据,也可以通过其他媒体、媒介、形式表达。隐私当然属于个人信息,且属于个人信息中的敏感信息,而数据是经过收集、加工、脱敏等处理之后的信息。严格意义上来说,数据主要存在于且使用于网络空间,至于数据中与自然人无关的信息内容,则不属于个人信息保护的范围。可以说,个人信息更加关注内容,具备可识别性和主体意义;数据则更加关注形式,不具备可识别性和主体意义,二者隶属于不同的权利束,[32]应当分别以人格权和财产权为重点进行保护。[33]

(二)个人信息权(益)的属性变迁

在信息时代,数据因稀缺性而具有经济价值,成为重要的社会资源,并且与其他资源不同,数据的存在样态决定了其因共享流通才能发挥更大的价值。因此,从隐私向个人信息再向数据的发展演进过程中,立法理念和价值导向亦发生了相应变化,即从严格保护隐私到个人信息保护和自由利用并重,再到鼓励大数据开发和数据产业发展。数据时代的个人信息权体现出不同于传统权利的重要特征,具体表现为以下几方面:

其一,个人信息权的财产权属性日益增强。关于个人信息权是属于人格性权利抑或财产性权利,理论界存在不同看法。有学者认为个人信息权属于一种人格利益,[34]有学者认为个人信息权属于一种财产权益,[35]还有学者认为个人信息权兼具有人格权和财产权属性,属于一种复合权益。[36]换言之,个人信息上承载的自然人的利益是多元的,既包括自然人的人格利益,也包括经济利益或财产利益,因此对于自然人个人信息应给予人格权和财产权的双重保护。[37]也有学者提出,数字时代的个人信息权益是具有宪法性质的权利,[38]《个人信息保护法》于三审过程中在第1条加入了“根据宪法”四个字,亦表明我国已将个人信息权上升至宪法高度,提升了我国个人信息权利(益)的法律位阶。毋庸置疑,个人信息权脱胎于传统隐私权,与人格尊严密不可分,具有典型的人格权属性。个人信息是自然人“可识别”的信息,其“既是自然人参与社会交往的载体,也是个人人格表现和人格发展的工具……因此,信息主体对个人信息流转范围和流转方式的掌握,和个人人格的发展密切联系,这也是在现实社会中保护个人信息相关权益的价值基础”。[39]个人信息一旦被泄露必然会给权利人造成一定困扰甚至带来精神痛苦,“自然人对个人信息并不享有绝对权和支配权,而只享有应受法律保护的利益。该利益是指自然人享有的防止因个人信息被非法收集、泄露、买卖或利用进而导致人身财产权益遭受侵害或人格尊严、个人自由受到损害的利益”。[40]然而,在大数据时代,个人信息所具有的商业价值以及所产生的经济利益日益凸显。“个人信息财产权是主体对其个人信息的商业价值进行支配的一种新型财产权,它能且只能存在于对个人信息进行商业性使用的条件下。在信息时代,个人信息具有潜在的商业价值故而都应该受到财产权的保护。”[41]或许,单个的个人信息无法产生商业价值,自然人作为个体也无法直接从个人信息中获得经济利益。但是,企业可以根据个人的消费信息进行大数据分析,从而进行精准营销;行业可以根据个人信息统计结果,推动行业转型和数据产业发展等。因此,从这一角度看,个人信息权兼具人格权属性和财产权属性,但又不同于知识产权,而是一种新型财产权。“个人信息具备人格和财产双重属性,在保护上,也应当以此出发,立法上秉持双重保护态度,司法中做好个案衡量,同时加强行业自律,并在一切个人信息保护活动中贯彻利益平衡原则。”[42]质言之,个人信息权是时代发展的产物,已经超越了传统个人私权的范畴,而与国家安全、公众健康、社会稳定、经济发展等密切相连,具有价值的多元性。当然,我们不能过分强调个人信息的财产性质,将个人信息与(大)数据相混淆。从财产权的发展历史来看,财产权

的客体逐步扩张是一个不言自明的事实,经历了一个“从无形到有形”、从“狭义到广义”的重大变化。[43]现代社会,个人信息因具备独立性、价值性、稀缺性等法律意义上“财产”的基本特征,而成为一种新型财产形式。“每个人都拥有各种形形色色的信息,这些信息对他人甚至整个社会来说具有意义或者价值,可以为他人提供方便或者资讯,这时他人会愿意付出对价来购买这些信息。”[44]虽然,从《民法典》的篇章结构及其具体内容角度,可以将个人信息权视为一种具体人格权。但不可忽视的是,个人信息在数字社会中的财产价值日益增强。换言之,个人信息双重属性对个人信息的财产利益保护提出了要求,亦产生了个人信息人格利益与其财产权益的平衡问题。

其二,个人信息的公共属性日益明显。无论是根据“利益说”“主体说”判断,抑或是根据“行为说”判断,个体信息的私人属性自不待言。作为建立在自然人主体信息之上的个人信息权首先是以保护个人利益为旨归,亦应当以个人信息自决权为核心,从这个角度来说,个人信息保护法属于私法。但现代社会法治的发展,已超越古罗马时期法律公私二元划分体系,利益也并非简单的非此即彼的划分境地,利益交叉、利益多元现象非常普遍。具体到个人信息而言,其不仅涉及私人利益,而且因其整合、流通、管理而具有了特殊的公共属性,与行业利益、国家利益、公共利益密不可分。[45]个人信息的公共物品属性决定了个人信息保护的制度设计不等同于传统的私法,而具有了公私混合属性。尤其是在万物互联的环境下,由个人信息所产生的大数据存在重大的外溢风险,从而给国家安全带来重大挑战。对我国当前而言,在核心技术、关键信息基础设施等受制于西方发达国家的背景下,数据安全、国家安全更应当引起高度重视,防止个人信息安全外溢至军事、政治、经济、文化、社会等领域。因此,不能把个人信息绝对归为“私益”范畴,亦不能仅按照私法逻辑对个人信息进行保护,传统私法的“知情同意”调解机制以及“填补损害”事后救济方式亦不能完全满足大数据时代的个人信息规制问题。

其三,个人信息的积极权利属性日益突出。传统上,个人信息通过隐私权予以保护,而隐私权具有典型的消极权利特征,即“个人生活安宁不受干扰”。无论是积极私权说抑或是消极私权说,还是基于人格尊严的信息自决权说,[46]都没有否认隐私权的私权范畴,因此,认为隐私权具有公共利益、公共产品、公共资源属性的看法是值得商榷的。[47]但随着信息技术的快速发展,个人信息的收集、分析、利用日益便利,个人信息权也逐渐演变为现代的具有积极意义的“信息隐私权”。质言之,现代社会更加注重个人信息的积极利用面向,这种变化体现在个人信息规范内容上具有更丰富更具体的权能方面,也体现在对相关义务主体更高更积极的法律要求方面,譬如严格的信息安全保障义务、完善的采取补救措施、及时的告知义务等,这也决定了需要对个人信息单独立法。

(三)个人信息保护的法治路径

个人信息赋权保护已成学界共识,但前已述及,现代信息技术的发展客观上增加了个人信息保护的难度甚至陷入了困境,使得传统个人信息保护机制日显不足。在这一背景下,受保护的个人信息的法律属性就成为一个重要的理论问题和制度选择,即个人信息是一项具体的法定权利抑或是一种法定权益?对这一问题的不同回答意味着不同的个人信息法律保护路径。

有学者从《民法总则》第111条(后被《民法典》第111条所承继,现已废止)出发,认为个人信息权属于民事权利,但该条关于个人信息权的规定是“推导式”“宣示性”的,需要配套立法进一步明确个人信息权的边界、行使及侵权责任等。[48]有学者则认为,《民法总则》第111条没有直接使用“个人信息权”这一概念,因此应当将个人信息作为“权益”对待,[49]并且该条选择了“行为规制模式”而非“权利化模式”来保护个人信息,从“权利”到“权益”的变化反映出对个人

信息保护力度的弱化。[50]还有学者基于文义和体系分析认为,民法对自然人个人信息提供的保护既可能是一项民事权利,也可能仅仅是一项民事权益。[51]笔者认为,根据文义解释和体系解释规则,《民法典》第111条"自然人的个人信息受法律保护"中"个人信息"应当理解为"法益"而非"权利"。这说明,个人信息不具备权利的"绝对权"特征,立法通过对个人信息权益作出的保护性规定,更大的意义在于宣示个人信息受法律保护的基本立场,而非法律确权。从法律属性上讲,该条款是一种引致性条款,也是一种兜底性规定。[52]对此,也有学者认为,个人信息与姓名权、肖像权、隐私权等其他人格权的客体难以区分,个人信息权不足以成为独立人格权,否则容易与既有人格权发生交叉重合,因此个人信息权利最多算是在信息自动化处理环境中对姓名、肖像、隐私等人格利益的特别保护,不能构成一种新的具体人格权。[53]

无论是《网络安全法》抑或是《民法典》,都只是规定"自然人的个人信息受法律保护",而对于个人信息的法律性质采取了回避态度,《个人信息保护法》则同时使用了"权利"和"权益"两个概念,这在客观上导致了个人信息权利化陷入困境,这是其一。其二,个人信息打破了传统民事法律关系客体的基本特性要求。传统民法视野下,产权明晰是私权保护和经济发展的重要前提,确定性、有体性、独占性是法律关系客体的基本特征,而个人信息显然不具备上述三个特性。个人信息具有无形性,并不必然依附于某种载体,更为关键的是,个人信息价值的彰显主要通过流动实现,难以确定独占主体。相反,个人信息具有多重价值属性,个人信息处理过程具有复杂性,个人信息的利益诉讼具有多元性,既有自然人的人格权利益诉求,也有企业的财产权益诉求,还有政府部门的公共利益诉求,这反过来阻碍了个人信息权利化进程。其三,以隐私权或自决权为主要内容的个人信息权保护模式受到重大挑战甚至出现异化。[54]从域外法治实践来看,美国在"以权利对抗权力"的政治理念和法律架构下,通过隐私权保护方式,如《加州消费者隐私法案》(California Consumer Privacy Act),赋予个人信息自决权,从而实现个人信息(隐私)免受政府公权力侵害。[55]而欧盟则选择了另外一种法治路径,即通过制定专门的数据保护法——《通用数据据保护法案》(General Data Protection Regulation,下文简称GDPR)明确规定个人数据自决权来实现对个人信息的保护。质言之,美国采取拓展隐私权范围的方式对个人信息进行保护,欧盟采取独立权利的方式对个人信息进行保护。然而,这两种模式在大数据时代都面临着重大挑战。一方面,个人信息的隐私权属性逐渐弱化,其人格权依赖(无论是个人尊严还是个人自由)所蕴含的精神利益逐渐转向以财产权依赖所蕴含的物质利益。"被视为涉及个人私人人格的决定权的个人信息,应当被定义为一种财产权"。[56]然而,尴尬的是,自然人对个人信息的控制能力非常有限,其重要缘由是,个人信息财产权主要通过数据池(data pool)的占有和使用来实现,[57]而数据池属于企业、政府等集体组织收集、构建、占有和使用,且具有相当的公共产品属性。虽然经过脱敏、匿名化处理的信息不再具有可识别性,但计算机技术的发展使个人信息的可识别和非可识别之间在某种情形下是可逆的,并不存在绝对的匿名状态。因此,个人信息的控制权实际上已经从自然人转向企业、政府等集体组织,通过个人财产权的方式保护个人信息是低效率的甚至是无效的。[58]

将个人信息作为"法益"进行保护的问题在于,我国立法中对"合法利益"的界定非常模糊。我国《民法典》第3条,将"其他合法权益"与"人身权利""财产权利"一并作为法律保护对象,但对于何谓"合法权益"则语焉不详。究其原因就在于,我国民事立法借鉴德国法上"权利"与"利益"相区分的保护模式,[59]但并未设计专门的"利益"法律保护机制,也没有提供具体的独立的"利益"保护规范,[60]从而导致区分"权利"和

“利益”的保护模式、构成要件及制度设计仅停留在学说讨论的层面。[61]因此,我国需要探寻更具理论基础和行之有效的个人信息保护模式。有学者针对这种困境,明确提出我国民法应当采取权利保护模式,为个人信息提供确定的权利基础,从而防止科技和商业的非理性发展。[62]但笔者认为,赋予自然人以个人信息“绝对权”不仅会妨碍个人信息因流通而产生的公共性价值,而且会妨害个人信息自由,进而对公众知情权和公共事务造成负面影响。[63]因为,正如前文所述,大数据时代的个人信息保护涉及的利益关系更为复杂,不仅要考虑自然人的人格利益,而且要充分考虑个人信息整合后产生的数据所具有的资源性和财产性特征。[64]

(四)利益平衡机制的制度设计

大数据时代的个人信息立法,不应止步于对个体权利的保障,而是应当确立以人为本位的权利界碑,构建以个人利益与公共利益为协调的平衡机制,即个人信息的保护必须将数据合理利用的现实需求和数字经济发展的社会趋势纳入考量范围。我们既不能选择以保护个人信息为借口排斥数字经济的发展路径,更不能选择以牺牲个人信息安全为代价来换取数字经济发展的基本立场,应当将“保护个人信息权益”和“促进数字经济发展”作为双重价值目标,在强化个人信息保护的同时促进个人信息的合理利用。

与传统法律客体不同,数据具有无形性、公共性、可分享性等特点,并且数据主要是通过流通来实现自身价值,因此,传统私权保护模式不能完全适用于数据治理。实际上,赋权模式并未真正达到保护个人信息之目的,亦与大数据时代利用个人信息的现实需求相悖,因此,采取有限个体主义与个人信息的动态保护路径,从而在公共性价值和安全风险防范之间实现平衡,是切实可行的方案。[65]质言之,传统私法理论下,权利主体对权利客体享有排他性独占权,控制权是权利核心,如果这一理论框架和规范模式机械地适用于数据问题,很容易得出赋予企业或者其他主体以“数据权利”进而构建数据归属体系和数据利用秩序的结论。但很显然,这种私权控制模式忽略了信息时代数据的公共属性,忽视了个人信息保护背后的公共利益。因此,应当突破传统私法理论局限的制约,从私益保护转向公益保护,从数据控制转向风险控制,对数据控制保持适当谦抑态度。[66]

在数字经济时代,要平衡好经济发展和信息安全的关系,坚持权利保障与信息共享并重原则,推动个人信息保护与数据合理利用相统一相协调。一方面,要回应广大人民群众对个人信息保护领域突出问题的重大关切,强化个人信息保护法律规范的系统性、针对性和可操作性。个人信息保护是关乎民生的大事要事,数字时代的个人信息收集呈现出随时性、共享呈现出全面性、使用呈现出普遍性、存储体现出永久性、传输体现出发散性、处理呈现出综合性等新特点,[67]对个人信息安全造成严重威胁。另一方面,应当承认,个人信息的收集使用是大数据时代的基础,也是便捷普惠互联网服务的保障。从技术角度看,信息采集越全面,数据分析越精准,个性化服务就越贴切。从世界范围来看,在新一轮的全球数字科技革命和数字产业变革中,大力发展数字经济已经成为世界主要大国和地区提升新经济竞争力的共同选择,数据资源和数据治理成为国家博弈新领域。就我国而言,数字化转型全面提速,需要在保护个人信息的前提下尽量释放大数据红利,积极享受大数据时代成果。所以,要考虑到个人信息保护边界和个人信息控制权的动态化发展趋势,为进一步加强个人信息保护、维护网络空间的良好生态、促进数字经济健康发展保留制度空间。

因此,大数据时代的个人信息不仅具有私人属性,而且具有公共属性,立法应实现各方利益的平衡,在个人信息保护与个人信息利用之间保持适当张力,既维护自然人的人格尊严又鼓励信息合理利用。质言之,科学严密的个人信息保护法律体系,应当在有效保障公民权利的前提下最

大限度地释放数字经济主体潜能,坚持“在开发中保护、在保护中利用”,从而最大限度地推动数字科技创新和社会经济发展。[68]《个人信息保护法》第1条开宗明义:“为了保护个人信息权益,规范个人信息处理活动,促进个人信息合理利用,根据宪法,制定本法。”这说明,《个人信息保护法》虽名为个人信息“保护”法,但其立法目的并非单纯地保护个人利益,而是将保护个人信息权益与促进个人信息合理利用并重,并以此制定了个人信息保护的基本原则以及处理个人信息的具体规则。

五、大数据个人信息保护体系规则的再完善

我国作为发展中国家,虽然在私法领域的隐私权立法和公法领域的个人信息保护立法起步较晚,但在社会法领域的数据保护立法已经走在了世界前列,这归根于我国互联网经济的蓬勃发展和数字大国的快速推进。“可识别性”是判断个人信息的标准,即能够直接或间接“识别”出特定自然人的信息属于个人信息,信息技术发展推动能“识别”的个人信息不断拓展,给个人信息保护带来了挑战。我国大数据时代的个人信息保护应从立法模式和规则体系两大方面进行完善。

(一)立法模式的现实选择

私权保护和信息自由的冲突和博弈是个人信息保护立法面临的基本问题,围绕该问题,世界各国基于不同的价值取向与利益衡量原则选择了不同的制度设计,主要形成了以欧盟为代表的“私权至上模式”和以美国为代表的“信息自由模式”。也可以说,欧盟与美国的个人信息立法是截然不同的两条建构路径:欧盟从公民基本权利立场出发,对个人信息采取全面而彻底的保护原则和统一立法模式,对可直接识别的个人信息以及任何可组合起来间接识别的个人信息都予以保护;美国从保障信息自由立场出发,对个人信息采取弱保护原则和分散立法模式,对个人信息的界定范围较窄,保护力度也远不及欧盟。也正基于此,有学者把美国个人信息保护模式归纳为“消费者保护模式”,即侧重于维护交易安全与交易秩序;把欧盟个人信息保护模式归纳为“数据保护模式”,即侧重于数据主体对数据的控制和监管。[69]美国信息自由模式推动了美国信息产业的迅速发展,但企业的逐利性本质决定了“自我规制”模式下个人信息经常被企业滥用,个人信息安全空间不断被挤压。而欧盟将个人信息权视为一项基本人权,基于对人格尊严的尊重,由政府主动承担保护个人信息的责任,但对于非欧盟国家而言,欧盟GDPR起到了贸易保护主义实际效果,构成了数字经济时代的新型贸易壁垒,也阻碍了数字产业的发展。[70]

我国作为发展中国家,互联网行业被视为超越西方发达国家的难得领域,大数据产业被视为国家战略产业,法治建设要为数据强国建设服务。事实证明,在我国个人信息保护宽松的制度环境中,我国互联网行业取得了突飞猛进的发展,数据产业也跃居世界领先地位。但同时,我们也面临着个人信息泄露的重大风险、个人合法权益被侵犯的严重局面,在这一背景下,我国个人信息保护立法迫切需要转型,即在个人信息保护与促进产业经济发展之间寻求平衡。然而,我国个人信息保护法治实践面临重重困境:民事立法保护滞后、经济立法保护阙如、刑法保护被动和民事司法救济无力等。[71]因此,我国应当构建适合中国国情、具有中国特色的个人信息保护模式。笔者认为,可以走第三条道路,即强化企业责任、行业自律的同时,加强国家个人信息立法,在数据产业已经相当发达的情况下逐渐偏重于个人信息保护。

着眼于未来,我国要确立以个人信息保护事先预防和事中控制为主的保护模式。传统上,保护法益的主要方式是事后救济,而在互联网时代,个人信息蕴含的法益具有复杂性,个人信息侵权给受害人造成的损害具有不可逆性,这就决定了个人信息保护方式具有复杂性以及保护机制具有系统性,进而需要改变传统法益事后救济

保护模式,而以事先预防和事中控制即以个人信息过程性保护手段为主,这主要体现在赋予和落实个人知情权、同意权、选择权、访问权、查询权、更正权、公布权、删除权等更多的程序性权利。[72]

(二)个人信息保护规则体系的再优化

《个人信息保护法》在借鉴域外发达国家成熟经验的同时,立足于我国社会发展现实,将个人信息权益私权保护与个人信息处理公法监管一并立法,兼顾个人信息保护与数据有效利用,统合私主体和公权力义务责任,与《网络安全法》《数据安全法》一道共同搭建了大数据时代我国网络安全和个人信息保护的基本法律框架。但至少应在保护机制和规范方法两方面可以再优化:

在保护机制方面,在对信息主体赋权的同时更要强调企业、社会组织、政府机关等在个人信息保护中的义务和责任。当前世界通行的个人信息保护框架规定,个人信息的控制者不得超范围收集和处理信息,必须保证个人信息的安全,必须保证个人信息使用的可解释性,在这一方面,《个人信息保护法》已经有所体现,不仅详细规定了个人信息处理义务规范,而且重点规定了个人信息处理规则即行为规范,同时还明确规定了个人信息保护的责任机制。个人信息保护除了刑法、民法、经济法保护机制,还需要行政法保护机制。我国当务之急,是要建立统一权威的个人信息保护部门。欧盟要求各成员国设立专门的个人数据监管机构以加强对个人信息的收集、利用、流通等环节的监控管理,德国根据这一要求设立了个人数据保护联邦委员会,这是世界首个专司个人数据保护监督、解决个人数据保护纠纷、提出个人数据保护建议的独立机构。英国设立了专门的信息委员会,以保障英国《数据保护法案》(Data Protection Act)的实施执行,对违法的个人或企业进行追责。日本为了加强个人信息保护的行政监管,于 2017 年成立了日本个人信息委员会,从而确立了个人信息保护集中监管体制。

在规范方法上,应制定《个人信息保护法实施条例》等法律法规,并采用和强化“积极确权 + 行为规范”模式。“积极确权 + 行为规范”模式是欧美个人信息立法发展的整体趋势,[73] 为我国个人信息保护立法提供了一定的借鉴指引。所谓“积极确权”,是指通过法律正面界定权利方式来划定个人信息主体的权益范围;所谓“行为规范”,是指通过法律直接规定处理个人信息行为规范方式来反推个人信息主体的权益范围。所以,前者又可以称为直接保护模式即权利界定模式,后者又可以称为间接保护模式即行为规制模式。

(三)公共数据规则体系的再创新

大数据时代,个人信息已经突破了传统绝对私权范畴,合理使用个人信息具有正当性。关键是如何平衡作为个人信息主体的自然人与作为数据控制者的企业、政府等之间的利益,如何确定是否合理使用个人信息,如何确保安全利用个人信息。随着建立在数据和算法基础之上的人工智能的迅猛发展,更多的个人信息乃至隐私被获取且具有极强的迷惑性,由此引发了严重的隐私危机,传统隐私法律保护框架在有效保护个人隐私和充分发挥个人信息价值之间的平衡作用捉襟见肘,需要探索新的法律保护路径。[74] 而公共数据是解决这一问题的重要视角。换言之,探讨公共数据生成的内在机理及其法律属性,分析公共数据治理的现实困境及其内外成因,研究政府在公共数据治理的角色定位与权力边界,从而实现公共数据的充分共享与个人信息保护的有效协调。

下一阶段,我国应通过制度创新破除公共数据共享鸿沟,在数据利用和个人信息保护之间实现平衡。具体而言,其一,通过制定数据产业促进法明确和细化对于公共数据的收集及共享的权责分配,制定详尽的数据资源协同整合的实施细则,将数据资源系统性安排从征信、公安、金融等特定领域拓展至社会各领域各方面。无论是

从隐私和个人信息保护视角看,抑或是从数字经济发展和公共数据治理视角看,政府都扮演着重要角色。其重中之重在于,解决采集个人信息的正当性基础问题以及提高公共数据的共享效率问题。其二,从静态层面,要严格限定公共数据的范围,将其限定在公共利益目的领域,增强公共数据正当性基础。对于一般领域的个人信息的收集和处理,可以采取"通常允许+特殊排除性规定"立法模式;对于敏感领域的个人信息的收集和处理,可以采取"通常不允许+列明允许范围"立法模式。同时,敏感领域个人信息收集和处理的情形应当仅限于为了维护国防安全、国家安全、公共安全等重大公共利益领域或犯罪惩罚与预防领域。其三,从动态层面,要严格规范公共数据的处理,政府收集和处理公共数据应当严格遵循法律授权、最小比例、权利保障、正当程序等基本原则和具体规则。其四,从机制创新角度,我国可以借鉴域外信息专员制度和信息分级分类制度、个案判断机制和风险评估机制等,进一步优化法律制度建构。

(四)公共利益规则体系的再构建

合理适度是科学立法的应有之义,个人信息立法时利益衡量必不可少。[75]个人信息保护和数据安全不仅仅是技术问题,更是国家政策、法律法规、技术开发等相结合的系统工程。建立健全个人信息保护法律制度,尤其要考虑到合理适度,既要避免法律缺失、数据被滥用,也要避免防护过度,抑制"数字经济"正常发展。质言之,数字经济时代,科学理性的个人信息保护观念,既不是为了企业利益和经济发展而置公民个人信息保护于不顾,也不是强调个人信息权的绝对化,而是要在保护和限制之间达到某种平衡,即将对个人信息的收集和使用限制在合法合规合理的框架内,而确定这一合理边界的重要因素就在于公共利益。

公共利益的优位不是绝对的。为了公共利益而限制个人信息也并非绝对的,而是相对的,仍应当遵守目的正当、法律授权、最小比例、权利保障等基本原则,遵循"知情同意"程序机制。可以说,无论是学理研究抑或是法律规范,都能推导出基于公共利益收集和处理个人信息的正当性,但目的正当性并不意味着手段的任意性。[76]个人信息保护需要结合具体场景,即"个人信息保护的合理程度要置于其所处的环境中具体审视"。[77]所以,对于个人信息的处理应当严格落实"三最"原则:一是范围最小原则,即收集个人信息应当将范围限于实现目的的最小范围;二是影响最小原则,即处理个人信息应当采取对个人权益影响最小的方式;三是期限最短原则,即保存个人信息的期限应当以实现处理目的所必要的最短时间。

问题在于,我国目前立法中"公共利益"条款较少且相对粗陋,这一方面源自于"公共利益"概念的抽象性和公共利益问题的复杂性,另一方面源自于我国立法阶段的初级性和立法技术简单化。随着我国立法工作从"有法可依"迈入"科学立法"阶段,应当完善公共利益规则体系,从而为公权力部门处理个人信息提供明确而具体的边界。

六、结　论

信息化时代,加强个人信息保护是人民群众的热切期待;大数据时代,促进数字经济发展是政府和企业的迫切需求。如果说,公共利益为限制个人信息注入了"价值理性",那么,数字经济发展则为利用个人信息提供了"工具理性"。大数据是对万事万物全景式的记录,被称为"信息时代的石油",对于推动实施我国大数据战略、加快推进数字中国建设意义重大。然而,人工智能等科学技术的广泛应用给传统法律制度、伦理道德以及社会治理带来了严重挑战。如何让大数据更好地服务于经济发展和社会进步,在避免信息孤岛的同时解决算法歧视、信息泄露、隐私侵权等问题,更是成为大数据时代的重要法治课题。从实践看,大数据的广泛应用使得擅自使用或者滥用公民个人信息的状况时有发生,严重侵

害公民合法权益。在推动数字经济发展的同时完善个人信息的法律保护,进而在数据充分赋能和个人信息保护之间、个人信息价值挖掘与个人主体信息自决权之间、大数据信息共享与隐私安全保护之间实现平衡,是近年来社会各界高度关注的问题。数据共享是数据利用的重要方式,也是数据产业和数字经济发展的重要基础。数字经济作为一种新的经济形态,是以"数据"作为核心生产要素和关键驱动力,其在推动经济社会发展的同时亦产生了个人信息保护、数据治理、平台责任等一系列法律监管问题,推动法律制度革新。《个人信息保护法》的出台标志着我国网络法律体系已经建立。然而,徒法不足以自行。着眼于未来,一方面,在《网络安全法》《数据安全法》《个人信息保护法》出台后需要执法司法的后续接力,从制定到落实,个人信息保护和数字经济发展任重而道远。另一方面,应当根据良法善治的要求进一步推进我国大数据法律制度建设,通过制定实施条例或者公布司法案例等形式,以创新共治思维、审慎监管理念推动体制机制变革和新业态发展,明确不同主体在个人信息保护中的行为规范与权利(力)边界,着力处理好个人、企业、社会组织和政府部门之间法律关系,既维护个人对信息的自决权,也要促进企业之间的良性数据竞争,并借助大数据提升政府监管能力与服务能力。

注释:

〔1〕龙卫球:《个人信息保护法具有深远的国际意义》,《经济参考报》2021 年 8 月 23 日。

〔2〕王叶刚:《论网络隐私政策的效力——以个人信息保护为中心》,《比较法研究》2020 年第 1 期。

〔3〕王利明:《数据共享与个人信息保护》,《现代法学》2019 年第 1 期。

〔4〕〔77〕范为:《大数据时代个人信息保护的路径重构》,《环球法律评论》2016 年第 5 期。

〔5〕〔德〕迪特尔·梅迪库斯:《德国民法总论》,邵建东译,北京:法律出版社,2013 年,第 807 页。

〔6〕万方:《个人信息处理中的"同意"与"同意撤回"》,《中国法学》2021 年第 1 期。

〔7〕高富平:《个人信息使用的合法性基础——数据上利益分析视角》,《比较法研究》2019 年第 2 期。

〔8〕张新宝:《我国个人信息保护法立法主要矛盾研讨》,《吉林大学社会科学学报》2018 年第 5 期。

〔9〕P. A. Samuelson, "The Pure Theory of Public Expenditure", *The Review of Economics and Statistics*, 1954, (36), pp. 387 - 389.

〔10〕尹建国:《我国网络信息的政府治理机制研究》,《中国法学》2015 年第 1 期。

〔11〕袁康、刘汉广:《公共数据治理中的政府角色与行为边界》,《江汉论坛》2020 年第 5 期。

〔12〕〔德〕克努特·阿梅隆:《德国刑法学中法益保护理论的现状》,〔日〕日高义博日译,姚培培中译,《中德法学论坛》2017 年第 14 辑。

〔13〕〔德〕卡尔·拉伦茨:《法学方法论》,陈爱娥译,北京:商务印书馆,2003 年,第 276 页。

〔14〕〔美〕爱德华·弗里曼等:《利益相关者理论:现状与展望》,盛亚等译,北京:知识产权出版社,2013 年,第 27 页。

〔15〕唐彬彬:《疫情防控中个人信息保护的边界——一种利益相关者理论的视角》,《中国政法大学学报》2020 年第 4 期。

〔16〕〔德〕汉斯·J. 沃尔夫、奥托·巴霍夫、罗尔夫·施托贝尔:《行政法》第一卷,高家伟译,北京:商务印书馆,2002 年,第 323 页。

〔17〕Harfield, Clive, "Law, morality and the authorisation of covert police surveillance", *Australian Journal of Human Rights*, Vol. 20, No. 2, 2014, p. 136.

〔18〕刘艳红:《公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角》,《法学论坛》2020 年第 2 期。

〔19〕方明:《个人信息多元保护模式探究》,《学海》2018 年第 6 期。

〔20〕〔46〕〔68〕张新宝:《从隐私到个人信息:利益再衡量的理论与制度安排》,《中国法学》2015 年第 3 期。

〔21〕王锡锌:《个人信息国家保护义务及展开》,《中国法学》2021 年第 1 期。

〔22〕《民法典》第 1034 条把"个人信息"界定为"以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息,包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等"。

〔23〕《网络安全法》第 76 条把"个人信息"界定为"以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息,包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等"。

〔24〕《数据安全法》第 3 条把"数据"界定为"任何以电子或者其他方式对信息的记录"。

〔25〕周汉华:《论互联网法》,《中国法学》2015 年第 3 期。

〔26〕程啸:《论大数据时代的个人数据权利》,《中国社会科学》2018 年第 3 期。

〔27〕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。

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

〔29〕李帅:《个人信息公法保护机制的现存问题及完善对策——基于 295 份行政判决书的定量研究》,《浙江社会科学》2018 年第 8 期。

〔30〕蒋坡:《个人数据信息的法律保护》,北京:中国政法大学出版社,2008 年,第 1 页。

〔31〕P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review*, August 13, Vol. 57, 2009, p. 1701.

〔32〕张平:《大数据时代个人信息保护的立法选择》,《北京大学学报(哲学社会科学版)》2017 年第 3 期。

〔33〕〔38〕龙卫球:《数据新型财产权构建及其体系研究》,《政法论坛》2017 年第 4 期。

〔34〕王利明:《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》,《现代法学》2013 年第 4 期。

〔35〕〔41〕〔64〕刘德良:《个人信息的财产权保护》,《法学研究》2007 年第 3 期。

〔36〕谢远扬:《信息论视角下个人信息的价值——兼对隐私权保护模式的检讨》,《清华法学》2015 年第 3 期。

〔37〕〔45〕刘金瑞:《个人信息与权利配置——个人信息自决权的反思和出路》,北京:法律出版社,2017 年,第 256、109 - 119 页。

〔39〕〔49〕王利明:《中华人民共和国民法总则详解》上册,北京:中国法制出版社,2017 年,第 456、456 页。

〔40〕程啸:《民法典编纂视野下的个人信息保护》,《中国法学》2019 年第 4 期。

〔42〕徐美:《再谈个人信息保护路径——以〈民法总则〉第 111 条为出发点》,《中国政法大学学报》2018 年第 5 期。

〔43〕吴汉东、胡开忠:《无形财产权制度研究》,北京:法律出版社,2005 年,第 7 页。

〔44〕〔美〕理查德·A·波斯纳:《论隐私权》,常鹏翱译,梁慧星主编:《民商法论丛》第 21 卷,香港:金桥文化出版(香港)有限公司,2001 年,第 347 页。

〔47〕Cohen. J, "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review*, Vol. 52, No. 3, 2000, pp. 1373 - 1438.

〔48〕陈甦:《民法总则评注》下册,北京:法律出版社,2017 年,第 785 - 790 页。

〔50〕叶金强:《〈民法总则〉"民事权利章"的得与失》,《中外法学》2017 年第 3 期。

〔51〕张新宝:《〈民法总则〉个人信息保护条文研究》,《中外法学》2019 年第 1 期。

〔52〕〔62〕王成:《个人信息民法保护的模式选择》,《中国社会科学》2019 年第 6 期。

〔53〕刘召成:《论具体人格权的生成》,《法学》2016 年第 3 期。

〔54〕〔71〕王秀哲:《大数据时代个人信息法律保护制度之重构》,《法学论坛》2018 年第 6 期。

〔55〕Ian Goldberg et al., "Trust, Ethics, and Privacy", *B. U. L. REV*, Vol. 81, 2001, p. 418.

〔56〕Alan Westin, *Privacy and Freedom*, New York: Atheneum, 1967, p. 324.

〔57〕胡凌:《超越代码:从赛博空间到物理世界的控制/生产机制》,《华东政法大学学报》2018 年第 1 期。

〔58〕吴伟光:《大数据技术下个人数据信息私权保护论批判》,《政治与法律》2016 年第 7 期。

〔59〕杨立新:《〈侵权责任法草案〉应当重点研究的 20 个问题》,《河北法学》2009 年第 2 期。

〔60〕王成:《侵权之"权"的认定与民事主体利益的规范途径——兼论〈侵权责任法〉的一般条款》,《清华法学》2011 年第 2 期。

〔61〕于飞:《侵权法中权利与利益的区分方法》,《法学研究》2011 年第 4 期。

〔63〕丁晓东:《个人信息私法保护的困境与出路》,《法学研究》2018 年第 6 期。

〔65〕丁晓东:《论个人信息法律保护的思想渊源与基本原理——基于"公平信息实践"的分析》,《现代法学》2019 年第 3 期。

〔66〕梅夏英:《在分享和控制之间:数据保护的私法局限和公共秩序构建》,《中外法学》2019 年第 4 期。

〔67〕李朝晖:《数字时代亟须加快制定个人信息保护法》,《深圳特区报》2020 年 10 月 27 日。

〔69〕王叶刚:《网络隐私政策法律调整与个人信息保护:美国实践及其启示》,《环球法律评论》2020 年第 2 期。

〔70〕田晓萍:《贸易壁垒视角下的欧盟〈一般数据保护条例〉》,《政法论丛》2019 年第 4 期。

〔72〕丁晓东:《论数据携带权的属性、影响与中国应用》,《法商研究》2020 年第 1 期。

〔73〕宋亚辉:《个人信息的私法保护模式研究——〈民法总则〉第 111 条的解释论》,《比较法研究》2019 年第 2 期。

〔74〕郑志峰:《人工智能时代的隐私保护》,《法律科学(西北政法大学学报)》2019 年第 2 期。

〔75〕〔德〕汉斯·布洛克斯、沃尔夫·迪特里希·瓦尔克等:《德国民法总论》,张艳译,北京:中国人民大学出版社,2012 年,第 426 页。

〔76〕刘国:《个人信息保护的公法框架研究——以突发公共卫生事件为例》,《甘肃社会科学》2020 年第 4 期。

〔责任编辑:邹秋淑〕