



个人信息保护的利益衡量与制度构建

李美燕

(国家计算机网络应急技术处理协调中心, 北京 100029)

摘要: 海量数据时刻记录着人们生产生活的轨迹, 通过分析、挖掘这些数据可为网民提供个性化、精准性的服务。但数据利用的力度越大, 个人信息保护面临的风险就越大, 失衡现象就越发严重和常见。探索中国个人信息保护之道, 需要符合数字中国的实践需要, 需要结合中华民族伟大复兴的宏大背景进行具体制度的安排。首先以美国、欧盟、我国为例介绍个人信息保护的立法路径与模式, 然后分析了我国个人信息保护的特点, 最后对个人信息保护的利益平衡与制度进行了思考。

关键词: 个人信息保护; 人格权益; 经济权益; 网络安全; 数字中国

中图分类号: D923

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018235

Interest measurement and system construction of personal information protection

LI Meiyang

National Internet Emergency Center, Beijing 100029, China

Abstract: Massive data always records the trajectory of people's production and life. Through analysis and mining, it can provide personalized and accurate services for netizens. But the greater the intensity of data utilization, the greater the risk of personal information protection, and the imbalance is more serious and common. Exploring the way of protecting personal information in China requires meeting the practical needs of digital China. Firstly, taking United States, European Union, and China as examples, the legislative path and mode of personal information protection were introduced. Then, the characteristics of personal information protection in China were analyzed. Finally, the balance of interests and system of personal information protection was considered.

Key words: personal information protection, personality right, economic interest, network security, digital China

1 引言

当前, 以互联网为代表的信息通信技术和人类生活生产交汇融合, 互联网快速普及, 消费互联网百花齐放, 产业互联网跨界融合并持续激发创新浪潮, 企业竞争力和影响力持续提升, 互联

网用户和市场规模日益庞大, 海量数据的集聚对经济发展、社会治理、国家管理、人民生活都产生了重大影响。正是这些海量数据使人工智能得到广泛应用, 使深度学习成为可能, 企业则通过数据的分析、挖掘为网民提供个性化、精准性的服务。人们主动拥抱数字化生产生活的过程, 也

收稿日期: 2018-07-03; 修回日期: 2018-08-10

意味着对个人信息使用权的主动让渡。数据利用的力度越大,个人信息保护面临的风险就越大,失衡现象就越发严重和常见。个人信息的滥用、泄露引起了社会各界的广泛关注,也成为各国立法关注的热点。从立法层面来看,世界各国纷纷在个人信息保护方面做了前瞻性布局。欧盟地区从个人权利角度论证个人信息保护的必要性;美国则更关注个人信息的经济属性,将个人信息保护作为风险管理来对待;我国个人信息保护的框架体系雏形已经显现,但需要合理的制度设计和实现路径予以保障,其关键是要处理好3个平衡之间的关系。

2 个人信息保护的立法路径与模式

个人信息保护和数据治理成为全球的新问题,也成为各国立法关注的热点。截至2017年,全球已经有120个国家或地区先后颁布个人信息保护法律。2018年,欧盟《一般数据保护规范》正式实施,美国《2018加州消费者隐私法案》签署生效,我国个人信息保护立法尽快出台的呼声进一步高涨。从个人信息保护的权益关系来看,传统法律框架将个人信息纳入隐私权或通过一种独立人格来加以保护,并通过个人信息的自决功能等特殊效力,以用户知情同意的方式建立数据流通的关系,当然还有其他管理需要的例外情形。随着时代变迁和产业发展,个人信息更多地强调其流通、利用的价值,也就是其经济属性。如何适应这种形势,需要理清其中关系和平衡权益。

2.1 美国模式

美国模式以分散式立法为特点,即在各个行业分别制定有关个人信息保护的法律法规、准则,而不制定统一的个人信息保护法律。从立法层面来看,个人信息被置于隐私的范畴而加以保护,更重视对公共领域政府机关涉及利用个人数据的行为进行规范,如1974年的《隐私法》和1980年的

《隐私保护法》^[1]。同时,针对敏感信息特别保护需求进行特别立法,如2013年的《儿童在线隐私权保护法案》和美国加利福尼亚州的《商业和专业条例》。这种立法模式与美国法律隐私权概念的开放性有关,在实践中,美国从实用主义出发,并未对个人信息和隐私权进行严格分界^[2],更关注个人信息的经济特征和个人价值^[3],将个人信息保护作为风险管理来对待,采用行业自律和市场调节机制来实现。这种设置有利于信息的流通和利用,将个人信息的搜集、利用交由企业,由其与权利主体通过合同进行协商解决。但是,由于个人与企业所处地位、掌握信息的不对等,企业相继出现了不当收集、使用和移转个人信息的情况,从而使个人的权利难以获得全面充分的保护。在实践中问题就折射出来,如Facebook数据泄露事件,引发民众对个人信息保护的质疑和巨大的担忧。在此背景下,美国加利福尼亚州的《2018加州消费者隐私法案》获得民众高票通过。该法案被称为美国“最严厉、最全面的个人隐私保护法案”,不仅大幅扩充适用范围,还创建访问权、删除权、知情权等一系列消费者隐私权利,进一步加重企业保护个人信息的责任。

2.2 欧盟模式

欧盟模式以制定统一法为特征,采取个人信息人格权保护模式,对数据处理者和控制者进行严格规范。在欧洲,多国曾尝试制定个人数据法,其中德国特征最为明显。德国联邦议会于1977年生效《联邦数据保护法》,第一次系统地、集中地保护个人信息,并彰显出其民事权利的属性。1981年欧共体制定《关于自动化处理的个人信息保护公约》对大规模的自动化信息处理活动进行规范^[4]。基于欧盟国家个人数据流动的实际情况,决定在一体化进程下统一个人数据保护立法。1995年,欧盟通过《关于在个人数据处理过程中保护当事人及此类数据自由流通的95/46/EC指令》(简称《95指令》),确立了个人信息保护的价



值,包括“基本权利”“自由”以及“隐私”的概念,构建了查阅权、更正和删除权、反对权、免受完全自动化决定权等权利。1997年欧盟颁布《有关电信行业中的个人数据处理和隐私权保护的97/66/EC指令》(简称《97指令》),适用于电信行业。2002年《电子通信隐私指令》取代《97指令》,要求电信和互联网服务商确保个人数据安全,确定了存储和使用数据时的主体同意规则。2009年的《欧洲Cookie指令》对cookie使用和必要信息披露进行规范和管理。

但是上述规则面临着适用统一性的困境,并随着公众对数据安全质疑的进一步增强,欧盟开始着手制定更加一致、细致的数据保护框架,以提高个人数据控制能力,并规范数据利用市场。自2010年起,欧盟启动《个人数据保护指令》的修订计划,最终于2016年通过《一般数据保护条例》(GDPR)。GDPR于2018年正式实施,适用范围大幅扩大,进一步明确数据主体的“知情同意”原则,细化并扩展了《95指令》的查阅权、更正与删除权、反对权以及免受完全自动化决定权的内容,并增设限制处理权、可携带权、遗忘权^[5]。

比较两种模式的立法经验,美国关注个人信息经济特征,更多地将个人信息保护作为风险管理来对待,采用行业自律和市场调节机制为主的松散式立法。以欧盟为代表的国家(地区)从个人权利角度论证个人信息保护的必要性,尤其是GDPR对全球立法的推动与影响是巨大的,大有成为主导型的立法模式之发展态势。正如维克托教授所说,“当世界开始迈向大数据时代时,社会也将经历类似的地壳运动。在改变人类基本的生活与思维方式的同时,大数据早已在推动人类信息管理准则的重新定位。然而,不同于印刷革命,人没有几个世纪的时间去适应,人们也许就只有几年的时间”^[6]。在这样的时代背景下,给我国个人信息保护立法留下的窗口期也不多了,

民众的诉求和产业的需求持续高涨。从全球视野来看,不论是欧盟立法模式,还是美国立法模式,都有其合理的地方,都有各自的价值观和社会基础作为支撑。传统不能涵盖一切,它只能划一条模糊的界限,其内容不明确^[7]。我国个人信息保护的立法路径的关键不在于模式差别,而在于制度设计是否符合中国文化的需要和产业发展的实际。

2.3 中国模式

我国个人信息保护立法之初走的是一种逆常规路线,即“最后法先行、刑法先行”。随着产业的蓬勃兴起,立法日益结合中国互联网产业高速发展的实践需要和中华民族伟大复兴的宏大背景。从刑法视角来看,顺应发展需要及时扩展个人信息的内涵,划出权利保护的红线、底线,并形成了刑法倒逼之势,促进行政立法、民事立法完善。从行政法视角来看,将个人信息作为产业运行安全、国家网络安全的重要组成部分。从民法视角来看,个人信息保护从重归属向重利用或者归属和利用并重的方向发展。具体来看,具有以下特点。

(1) 及时回应个人信息和隐私保护的迫切需求

2012年全国人民代表大会常务委员会《关于加强网络信息保护的决定》规定,涉及公民个人隐私的电子信息以及可识别的公民个人身份信息受国家保护,任何组织和个人不得非法获取、出售公民的个人信息。2015年《刑法修正案(九)》将“出售、非法提供公民个人信息罪”和“非法获取供个人信息罪”整合为“侵犯公民个人信息罪”,放宽了侵犯公民个人信息罪主体范围。2017年《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》在《网络安全法》的基础上,进一步扩大了个人信息范围,将其特定自然人活动情况的各种信息(如行踪轨迹信息等)纳入保护的范畴。从立法进程来看,《中华人民共和国刑法》首先划出了一

条“高压线”。通过应该前置的低度的法先行，让秩序法优先发挥管理作用，使法律发挥规范、引领、保障的作用。然而，我国为何形成了“最后法先行”局面呢？这反映了一个很迫切的现实，如个人信息泄露助长电信诈骗、人肉搜索酿成生活悲剧。个人信息的滥用或对公民个人信息破坏、侵犯到了一个难以容忍的地步，迫使《中华人民共和国刑法》不得不出手。同时，从刑法视角来看，个人信息内涵也及时回应了产业发展需要，特别是人工智能应用服务纵深延展，从身份属性的信息向活动情况的各种信息方向延展。

(2) 坚持信息和数据安全以及其他公共利益的底线

2013年工业和信息化部《电信和互联网用户个人信息保护规定》要求电信业务经营者、互联网信息服务提供者应当对收集和使用的用户个人信息的安全负责。2017年《中华人民共和国网络安全法》正式实施，将个人信息保护作为网络安全的重要组成部分，并明确了经营者在发生数据安全事件向用户和主管部门“双报告”的规定。保护个人信息是维护国家安全和公共安全的基础，我国也不例外，在立法中加重信息控制者和处理者在接触个人信息过程中的安全责任。

(3) 兼顾商业利用与产业发展的需要

2017年《中华人民共和国民法总则》第111条就对个人信息权益进行专门的确认和保障，第127条对数据和网络虚拟财产进行保护和调整。在我国民事基本法和单行法中首次出现了个人信息保护的有关规定。过去立法，权利概念中比较重归属。但是，随着我国产业发展和人工智能应用推进，《中华人民共和国民法总则》第111条与第127条，把个人信息保护和数据保护进行分置规定，既明确了个人信息的归属和保护问题，还考虑了数据开发利用和保护问题，将个人信息保护转向重利用或者归属、利用并重的方向延展。

总体来看，我国个人信息保护虽然没有统一立法，但已经形成了比较体系化的规定，表现出了先进性。当然，立法目前的先进性更多地表现在原则以及理念层面。

3 个人信息保护的利益平衡与制度思考

我国个人信息保护的制度设计超越了欧美两种模式的简单对比或移植，进一步回应个人信息和隐私保护的迫切需求，坚持信息和数据安全以及其他公共利益的底线，兼顾数据商业利用与产业发展的需要，其核心是相关主体的权利及权利体系的安排。在利益格局下，立法需要考虑个人信息在社会的作用并根据比例性原则与其他基本权利保持平衡，结合数字中国和中华民族伟大复兴的宏大背景来进行考虑。

(1) 个人权益的保障与数据商业利用之间的平衡

用户的人身特征、行为状态时时被海量数据记录，尤其是指向特定主体的个人信息，能够轻松地勾勒用户的人格形象，显现其生活轨迹。用户发出的每一条信息、浏览的所有痕迹，都不再是自己独有的存储记录，不会被时间磨损，将清晰地成为善意或恶意的他人通向他的路标。个人信息的利用增进了社会福祉，也导致了信息主体权益受到威胁和侵害。个人信息保护的重要性被描绘得具体而真切。马斯洛在其需要层次理论中指出，“人格标识的完整性和真实性是主体受到他人尊重的基本条件”^[8]。在具体制度构建中，个人信息对于权利主体的尊严和自由价值应当首先被考虑，即人格权益的保护，需要赋予用户信息知情权、信息决定权、信息更正权等权利。另一方面，个人信息保护需要兼顾数据商业利用的需要。毕竟，数据的流通使人们生产生活彰显便捷性，决策更加智能化，服务获取变得精准化。就用户而言，权利配置需要确立其人格权益，还要兼顾信息的经济属性，配置财产权益；就经营者



而言,分别配置数据经营权和数据资产权。因为没有经营者投入大量的人力、物力、财力,数据利用、挖掘以及人工智能应用难以延展,用户也无法时时获取免费的网络服务^[9]。

同时,在具体制度的安排过程中要保持一种动态与弹性,以平衡个人权益保障和数据商业利用之间的关系。就人工智能应用而言,就会推翻很多过去确立的个人信息保护规则。在当下的产业环境下,企业收集的数据越多,分析能力越强,消费需求越大,商业利润就越多,以互联网公司通过 cookie 技术实现用户画像为例。虽然可以基于算法对人的工作表现、经济状况、兴趣爱好、行为习惯、位置等进行分析,并精准评价,但是在应用的过程中可能会出现性格歧视、隐私侵犯等问题。从个人信息保护的角度,赋予用户知情同意权利十分必要。但在具体的权利构建的过程中,仍需要处理好利益平衡的关系。比如,采用欧盟 GDPR 的“明示同意(opt-in)”方式,就难以满足企业收集海量用户数据的连贯性需求,在一定程度上会阻碍人工智能应用的创新发展。基于合理的数据商业利用目的,在非高风险数据或非敏感数据的应用场景下选择“退出同意(opt-out)方式”就能够较好地处理二者的关系。同时,知情同意原则还需要结合产业发展实际,设定例外原则。比如,新加坡立法,在互联网应用场景下所有数据的收集需要征得用户同意变得不现实的情况下,在符合合法商业目的的情况下,可以不征求用户同意,只要对例外情形进行安全影响评估即可。可以看出,日新月异的技术发展给个人信息保护带来直接的冲击和调整,迫使用户知情同意原则保持动态和弹性。

总之,我国个人信息保护既要及时构建权利保护屏障,也要使数据“物尽其用”,给产业创新与发展留有空间。只有保持数据的流通,才能以数据为纽带促进产学研深度融合,形成数据驱动型创新体系和发展模式,培育造就一批国际领

军的互联网企业,筑牢数字中国之基。在个人信息保护的制度安排上,要坚持个人权益保障与数据商业利用并重,保持规则的动态与弹性,最终才能让中国互联网的发展成果造福更多国家和人民。

(2) 公权力与私权利之间的平衡

在个人信息保护的具体制度构建中需要兼顾公权力与私权利之间的平衡。信息社会,不同于传统隐私保护中政府超然的中立地位,在个人信息保护和利用中,政府具有了利用者和管理者的双重角色:一方面,政府作为社会管理和社会福利的承担者,公共安全、公共管理和公共福利的推进离不开对居民个人信息的掌握;另一方面,出于对行政效率的追求,也不断促进政府积极探索个人信息利用的限度和价值^[10]。

作为信息的利用者,政府不能无节制地、肆意地收集和利用个人信息。也就是说,公权力需要受到必要的限制。作为信息的管理者,在特定的情况下,需要对个人信息私权利进行必要干预。比如,为了公共安全,国家对跨境数据设定本地化存储的要求或要求跨境数据转移符合本国对个人信息保护标准。虽然互联互通的产业背景以及商业模式的创新迭代都需要数据的开放,但是基于公共安全对私权利进行必要限制,也是无可非议的。比如,为了公共利益或保护公众的知情权,不赋予相关主体删除有关数据权利或遗忘权。日本一名因猥亵儿童的罪犯起诉谷歌,依据遗忘权要求 Google 删除他被捕的信息,最后日本最高法院判决 Google 不需要删除上述信息。在本案中,相比删除权,保护公众的知情权就显得更为重要。再比如,欧盟 GDPR 第 112 条就规定为了完成《日内瓦公约》的义不容辞的任务或遵守适用于武装冲突的国际人道主体法,因为公共利益的重要原因或为了数据主体的切实利益,任何向国际人道主义组织客观上或法律上无法做出同意的数据主体的个人数据的传输可以被认定为是必

要的^[1]。也就是说,为公共利益而传输、共享特定主体的个人信息,即使权利主体不同意,个人数据的传输、共享也具有合法性。

当下关口,我国正在全力实施国家大数据战略,运用大数据提升国家治理现代化水平,建立健全大数据辅助科学决策和社会治理的机制,推进政府管理和社会治理模式创新,实现政府决策科学化、社会治理精准化、公共服务高效化;推行电子政务、建设智慧城市等为抓手,以数据集中和共享为途径,推动技术融合、业务融合、数据融合,打通信息壁垒,形成覆盖全国、统筹利用、统一接入的数据共享大平台,构建全国信息资源共享体系,实现跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务。这些战略的部署都需要政府通过广泛的样本分析了解社情民意、发展的痛点、治理的难点。毕竟,政府决策科学化、社会治理精准化、公共服务高效化都需要依赖信息的收集和利用。个人信息对于线索收集、信息溯源与情报分析的意义是巨大的,在具体制度的构建过程中需要有大局意识,处理好公权力与私权利的关系,并结合数字中国和中华民族伟大复兴的宏大背景来进行考虑。

(3) 技术与法律共治的平衡

法律并不能一劳永逸地解决个人信息保护的所有问题。完全寄希望于法律制度来实现对个人信息的全天候 360 度保护,并不现实。个人信息保护需要从法律层面,结合国情明确各主体的权利与义务,并使其规则切实可行;另一方面,需要主动迎接科技进步给个人信息保护带来的全新挑战,通过技术手段设立权益保护屏障,通过创新促使保护方式变得更加智能与快捷。毕竟,新技术的应用给治理带来诸多挑战,尤其是人工智能应用使得数据采集成为常态化,区块链分布式特点会使信息暴露在大众面前,而互联网时代的个人信息保护又面临违法成本低与维权成本高的双重困境。个人信息保护需要通过技术手段来应

对技术带来的难题,避免保护手段的单一化、简单化,综合运用法律、技术等多种方式求得治理效果全方位贯通无纰漏。

在实践中,有很多通过技术功能设计来保护个人信息的有益尝试。比如,电子身份证标识(eID)就是一种以密码技术为基础、以智能安全芯片为载体,由“公安部公民网络身份识别系统”签发,能够在不泄露身份信息的前提下在线远程识别身份。2017年10月,全国首个将eID运用到不动产登记领域的项目在海口正式运行。比如,企业在研发产品时注意对个人隐私的保护,将“经设计保护隐私(PbD)”的理念贯彻产品设计之中,把隐私保护作为产品的默认设置,以预防用户隐私侵犯发生。比如,Google(谷歌)早期推出街景服务,用街景车收集街道图像,并实时展示在谷歌在线街景地图上。但谷歌街景服务却涉嫌非法收集信息、侵犯个人隐私,受到多国处罚或频频被消费者起诉。为回应规则的要求,Google开发用户人脸和车牌虚化处理功能嵌入设计,通过技术将可识别人物身份的信息进行模糊化处理,有效地保护了个人信息。再比如,为提升用户搜索结果的准确率,Amazon(亚马逊)通常会及时存储和当前账户关联的语音搜索记录。但为了保护用户个人信息,Amazon提供选项以供用户根据需要决定是否删除以往的搜索记录。

当下,我国正在建立网络综合治理体系,探索出一个比较好的、有利于数字中国发展的个人信息保护框架模式,应当是紧跟科技进步的步伐,导入科技驱动型的数据治理体系,坚持技术与法律共治局面。

4 结束语

数化万物,智在融通。随着产业和技术的互联互通、商业模式创新迭代与演讲升级,数据的产生、存储、利用从消费互联网向产业互联网融合纵深延展,涉及关键基础设施的安全、产业



持续创新发展以及社会利益的重新流动。个人信息保护制度与服务百姓人格权益和财产权益息息相关,与企业创新创业和经营发展同频共振,与国家发展和社会稳定大局紧密相连。个人信息保护制度安排需要先进的立法原则和理念,需要合理的制度、科学的制度模式和具体的制度和实现路径予以保障。当然,要想制定一个符合当下文化、与经济发展水平相适应的个人信息保护制度,需要处理好个人权益保护和数据商业利用之间的平衡、公权力和私权利的平衡、法律与技术共同治理的平衡。

参考文献:

- [1] 周汉华. 个人信息保护法(专家建议稿)及立法研究报告[M]. 北京: 法律出版社, 2006: 79-80.
ZHOU H H. Personal information protection law (expert draft) and legislative research report[M]. Beijing: Law Press•China, 2006: 79-80.
- [2] 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[J]. 现代法学, 2013, 35(4): 62-72.
WANG L M. Legal protection of personal information: centered on the line between personal information and privacy[J]. Modern Law Science, 2013, 35(4): 62-72.
- [3] 张平. 大数据时代个人信息保护的立法选择[J]. 北京大学学报(哲学社会科学版), 2017, 54(3): 143-151.
ZHANG P. Legislative choice of personal information protection in the age of big data[J]. Journal of Peking University(Philosophy and Social Sciences), 2017, 54(3): 143-151.
- [4] 孔令杰. 个人资料隐私的法律保护[M]. 武汉: 武汉大学出版社, 2009: 164-168.
KONG L J. Legal protection of personal data privacy[M]. Wuhan: Wuhan University Press, 2009: 164-168.
- [5] 京东法律研究院. 一般数据保护条例评书及实务指引[M]. 北京: 法律出版社, 2018: 24-27.
JD Law Research Institute. General data protection ordinance commentary and practice guide[M]. Beijing: Law Press•China, 2018: 24-27.
- [6] MAYER SCHONBERGER V, CUKIER K. 大数据时代[M]. 盛杨燕, 周涛, 译. 杭州: 浙江人民出版社, 2013: 217.
MAYER SCHONBERGER V, CUKIER K. Big data: a revolution that will transform how we live, work, and think[M]. Translated by SHENG Y Y, ZHOU T. Hangzhou: Zhejiang People's Publishing House, 2013: 217.
- [7] BURTON S J. 法律的道路及其影响[M]. 张芝梅, 陈刚, 译. 北京: 北京大学出版社, 2012: 268.
BURTON S J. The path of the law and its influence[M]. Translated by ZHANG Z M, CHEN G. Beijing: Peking University Press, 2012: 268.
- [8] MASLOW A H. 动机与人格[M]. 许金声, 译. 北京: 中国人民大学出版社, 2007: 31.
MASLOW A H. Motivation and personality[M]. Translated by XU J S. Beijing: China Renmin University Press, 2007: 31.
- [9] 龙卫球. 数据新型财产权构建及其体系研究[J]. 政法论坛, 2017, 35(4): 63-77.
LONG W Q. On the construction of new data property and its system structure[J]. Tribune of Political Science and Law, 2017, 35(4): 63-77.
- [10] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.
ZHANG X B. From privacy to personal information: theory and institutional arrangements for re-measurement of interests[J]. China Legal Science, 2015(3): 38-59.
- [11] 京东法律研究院. 一般数据保护条例评书及实务指引[M]. 北京: 法律出版社, 2018: 39.
JD Law Research Institute. General data protection ordinance commentary and practice guide[M]. Beijing: Law Press•China, 2018: 39.

[作者简介]



李美燕(1984-),女,国家计算机网络应急技术处理协调中心助理研究员,中国互联网协会个人信息保护工作委员会秘书长,北京航空航天大学法学院网络空间国际治理研究基地特聘研究员、博士,主要研究方向为互联网产业发展、个人信息保护与数据安全、互联网治理。