doi:10.13582/j.cnki.1672-7835.2022.06.013

隐私计算的行政法规制

尹华容,王惠民
(湘潭大学 法学院,湖南 湘潭 411105)

摘 要:隐私计算具有推动数据“可用不可见”的功能,能够满足数据价值运用与数据安全保护兼顾的需求。然而,隐私计算也潜藏着数据合规风险、数据泄漏风险、歧视放大风险、数据群岛风险、信任瓦解风险,亟须通过法律进行规制。我国现行法律针对隐私计算风险的治理存在立法不完善、标准不统一、监管不全面、救济不平衡、引导不及时五大问题。行政法规制可以实现事前、事中、事后全链条治理,具有及时、灵活、系统等优点。通过完善法律法规、构建统一标准、巩固信任体系、强化监管力度、引导合规意识五大措施,可有效为隐私计算的发展系上“安全带”。

关键词:隐私计算;行政法规制;数据权利
中图分类号:D912.1 **文献标志码**:A **文章编号**:1672-7835(2022)06-0093-09

数据要素是数字经济深化发展的核心引擎①,数据的开放共享与交换流通则是释放数据要素价值的关键。但是,数据价值释放过程中产生的数据安全问题,已然成为阻碍数据应用进而限制数字经济发展的难越“关山”。2022 年 1 月,国务院办公厅印发的《要素市场化配置综合改革试点总方案》适时提出探索“原始数据不出域、数据可用不可见”的交易范式。隐私计算作为一种新型信息技术,具备“在保证数据提供方不泄露原始数据的前提下,对数据进行分析计算,有效提取数据要素价值”的功能,契合了保障数据在产生、存储、计算、应用、销毁等各个环节中“可用不可见”的要求,成为破局之道,被广泛应用于金融、政务、通信、医疗、互联网等重要领域。

然而,隐私计算也潜藏着数据合规、数据泄漏、歧视放大、数据群岛、信任瓦解等风险。目前,针对隐私计算风险治理的研究主要集中于计算机科学领域,这些研究试图通过技术路径治理隐私计算的安全问题。而法学领域的相关研究尚少,且主要受“科斯定理”的启示,通过明确数据权属的民事路径来防范风险,但数据权属的性质在学界存在较大争议,适用“科斯定理”的低交易费用前提也不符合现实。进退维谷之际,综合运用行政法的规制措施,对于维持良好市场秩序、保护企业与公民合法权益具有不可替代的作用,《个人信息保护法》和《数据安全法》也通过诸多条款发挥行政法规制的积极效应。对此,根据隐私计算的技术原理,基于法律法规的有效授权,对隐私计算的风险进行全面而精准的行政法规制,成为治理的重要手段。

一 隐私计算存在的社会风险

隐私计算是隐私保护计算(Privacy-Preserving Computation)的简称,是指对数据进行隐私保护的基础上进行数据加工、分析处理、分析验证,实现数据价值挖掘的技术体系,包含了人工智能、密码学、数据科学等众多学科的交叉融合②。隐私计算并非是某一种计算方法的名称,而是对一系列具有隐私保护能力的计算方法的统称,如联邦学习、多方安全计算、机密计算、差分隐私、同态加密

收稿日期:2022-06-12
基金项目:国家社会科学基金重大项目(21&ZD204)
作者简介:尹华容(1973—),男,湖南洞口人,博士,副教授,主要从事宪法与行政法学研究。
①《国务院关于印发“十四五”数字经济发展规划的通知》,《中华人民共和国国务院公报》2022 年第 3 期。
②中国信息通信研究院,阿里巴巴(中国)有限公司,北京数牍科技有限公司:《隐私保护计算技术研究报告》,中国信通院网 2020 年 11 月发布,第 6 页,http://www.caict.ac.cn/kxyj/qwfb/ztbg/202011/t20201110_361696.htm。

等。目前最具代表性、使用最广泛的隐私计算主要表现为三种技术路线,其一是以多方安全计算为代表的基于密码学的技术,即多个参与方基于密码学技术共同计算一个目标函数,保证每一方仅获取自己的计算结果,无法通过计算过程中的交互数据推测出其他任意一方的输入和输出数据的技术。其二是以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术,即通过分布式学习的方式,由客户终端(使用方)从中央服务器下载预测模型,并将自有的数据投入模型中进行机器学习,同时将所更新的内容上传云端,预测模型针对各个终端所更新内容进行优化,客户终端再下载完善优化后的模型进行使用,过程不断重复,而数据始终存储于客户端避免泄漏①。其三是以可信执行环境为代表的基于可信执行环境的技术,即通过软硬件方法在中央处理器中构建一个安全区域,保证其内部加载的程序和数据在机密性和完整性上得到保护。

隐私计算可以有效实现数据"可用不可见",纾解了数据共享流通过程中的数据泄漏与滥用问题,有利于消除数据孤岛、合规避险、弥合"信任鸿沟",既保护了数据主体的隐私权益,也促使数据处理者实现合规使用,更有助于数字经济的长效发展和数字社会的秩序稳定。因此被广泛应用于金融、医疗和政务领域,根据毕马威预测,隐私计算将撬动国内千亿级规模市场②。然而"患生于所忽,祸起于细微"。"技术从来就是好坏参半",它"既赋予我们创造性,也赋予我们毁灭性"③。在隐私计算被一路唱好的同时也应当注意到其背后更为隐蔽的社会风险:以隐私计算处理过程为轴线,主要存在数据合规风险、数据泄漏风险、歧视放大风险、数据群岛风险、信任瓦解风险。

(一)数据合规风险

《数据安全法》第八条规定数据处理必须合法合规,同时,《个人信息保护法》第十三条、十四条也规定除特殊情形外,处理个人信息需满足"知情同意"原则。一般情况下,在使用隐私计算对数据进行处理前,数据提供方和数据使用方必须征得数据主体的有效授权,但是,与普通的数据处理技术相比,隐私计算是在"不可见"的前提下进行数据处理,具有匿名化特点,并且往往需要经过加密或多方学习模型等程序去除数据的可识别特征。所以,要从本就模糊的数据中获取准确信息的难度随之增大,这导致隐私计算对原始数据的处理范围要求更广、挖掘程度要求更深,以此才能实现各方数据在"不可见"状态下做到处理结果"可用"目的,这使得授权内容难以被授权协议完全涵盖。如联邦学习的多方参与模型建构过程中,各方模型会根据更新需求反复进行轮回适配,对数据的使用目的、使用深度等授权呈动态需求,而传统的一次性授权呈静态状态,动态需求与静态授权之间的矛盾导致数据处理以及处理结果无法满足《个人信息保护法》所规定的"知情同意"原则,并极易使得数据处理者产生数据滥用的偏向,进而从事数据监控、数据欺骗、数据杀熟等行为,公民的数据权益无法获得有效保障。此外,在隐私计算中因多方数据"分布式学习"的特点,某一方滥用数据造成的数据合规风险会迅速在数据流通过程中呈倍增效应扩散,最终致使各参与方的数据处理结果均成为"毒树之果"。

(二)数据泄露风险

隐私计算的数据泄漏可以分为主动泄漏和被动泄漏。主动泄漏是指因参与方违背公约将模型或数据主动泄漏给第三方,此为绝大多数数据处理活动都存在的问题,在此不多赘述。隐私计算的数据被动泄漏主要是指原始数据被复原和模型攻击。一方面,复原原始数据的常用手段是反向工程技术,其原理是对目标模型进行测试,以此推导出他人产品的功能、组织结构、处理流程、算法、界面等设计要素④。隐私计算本身的技术属性使得其存在可能被反向工程突破的弱点,尽管隐私计算致力于将数据达到法律规定的"非识别性与

①例如,谷歌预优化旗下输入法的联想输入功能,即输入一个字,输入法会根据用户的习惯推荐候选字句,但广泛收集数据面临成本和安全问题。此时,由谷歌构建一个模型,由同意参与测试的用户下载在手机上,实现去中心化,该模型在用户手机中对用户数据进行分布式训练学习并将训练成果传回谷歌服务器,达到优化目的后模型会自动消失,以此达到多个参与者之间共享训练数据而不会泄露其数据隐私的目的。

②郝亚娟,张荣旺:《风口上的隐私计算》,《中国经营报》2021年12月20日。

③Ray Kurzweil:《奇点临近——2045年,当计算机智能超过人类》,李庆诚等译,机械工业出版社2011年版,第240页。

④杨婵:《论计算机软件反向工程的合法性问题》,《法律科学(西北政法学院学报)》2004年第1期。

不可复原”脱敏处理，但若对隐私计算过程或源代码进行反向推演获取原始数据，非授权主体依然有可能通过“多次尝试输入数据生成特定关系的结果”倒推原始数据①。另一方面，模型攻击主要是指黑客对隐私计算基础技术的恶意破坏，以联邦学习技术为例，各参与方需要通过上传或共享模型参数或梯度信息，以此完成联合模型的建立，达到联合使用数据的目的。然而，联邦学习场景极易遭到投毒攻击、用户端 GAN 攻击、服务器端 GAN 攻击、推理攻击等恶意破坏②，任一参与方遭受攻击均可能导致联合模型泄漏，从而引发大规模数据泄漏。隐私计算主要应用于政务、金融、通信、医疗领域，占比达 93%③，同时，前述领域的数据大部分事关国计民生，一旦泄漏，将严重危及产业发展、网络安全甚至国家安全。

（三）歧视放大风险

算法歧视又称算法偏见，根据生成来源不同，可以分为“先行存在的算法偏见、技术性算法偏见、突发性算法偏见。”④算法歧视是算法技术应用中普遍存在的问题，而智能算法技术又是隐私计算进行数据分析的基础技术之一，隐私计算难以避免会出现前述歧视。然而，相较于其他的算法技术应用而言，隐私计算会导致算法歧视更加放大。一方面，隐私计算因为使用匿名化数据、模型学习、加密技术等方式实现“可用不可见”目的，计算结果的偏差性较于其他可见条件下的计算更为普遍、严重，而结果的偏差性是引发算法歧视的关键诱因。另一方面，隐私计算各方提供的数据在匿名化后模糊性提高，往往需要多个数据提供方的数据作为样本，将大量的数据样本参与匹配才能产生具有实用性的数据处理结果。在此过程中，各数据方模型和中央模型之间的反馈与调整会进行多次轮回训练，直到形成各方适配的模型，一旦某个数据样本含有歧视内容或数据间错搭乱配，都会直接导致计算平台的模型以及各参与方的模型被污染，污染后的模型导致结果偏差扩大，歧视覆盖群体放大，最终对海量数据背后所指向的众多数据主体产生无法估量的危害。

（四）数据群岛风险

数据孤岛本是指不同的数据由不同的数据主体独立持有，各主体之间互相孤立、无法互通，形成物理意义上的“孤岛”。隐私计算造成数据“孤岛”成为“群岛”的原因主要在于客观技术标准的差异与主观开放意识的薄弱。客观技术上，一是算法原理的差异性导致平台间难以实现互联互通，不同的隐私计算平台或适用的不同的算法，各类算法之间的底层数据加密、数据计算逻辑、数据交互流程均存在差异。二是各平台在系统设计中所使用的功能组件不同，诸多的组件源于不同的厂商或不同的应用功能，平台之间建立互通的成本极大幅度增加⑤。主观意识上，各企业考虑到企业竞争、安全防护和知识产权等问题，除了对一些非核心组件进行开源，在其他方面并不愿或不敢公开自己的底层协议。总而言之，数字中国战略下的数字政府、数字经济、数字社会依赖于数据要素的价值释放，而数据要素的价值释放又源于流通和应用，隐私计算原始目的是为了促进数据流通，打破数据孤岛困境，但由于主客观原因，掌握大量数据的数据平台之间却无法交互数据、发挥效能，可能导致数据重复收集、平台协作不良、工作效率低下等连锁反应。“数据孤岛”反而恶化为“数据群岛”，数据互联互通的设想成为乌托邦。

（五）信任瓦解风险

“数字社会的到来改变了信任产生的社会情境，信任从人际信任、系统信任发展为数字信任。”⑥数字信任是基于数字化代码来构建的新型系统信任机制，其既是人们对技术的信任，也是以数字技术为中介包含人际信任、系统信任和技术信任的综合体，这种互相信任是数字化经济交易和数字化社会合作的基础。隐私计算技术应然层

①赵精武：《破除隐私计算的迷思：治理科技的安全风险与规制逻辑》，《华东政法大学学报》2022 年第 3 期。

②陈兵，成翔，张佳乐，等：《联邦学习安全与隐私保护综述》，《南京航空航天大学学报》2020 年第 5 期。

③中国新闻网：《中国隐私计算加快落地 金融、通信、政务等行业应用居前》，http://www.chinanews.com.cn/cj/2022/07-13/9802815.shtml。

④学者刘友华认为，算法偏见主要分为三种，即因嵌入算法设计者主观意识或社会影响而形成的先行存在的算法偏见、因技术限制造成的技术性算法偏见和因突发性事件形成的突发性算法偏见。参见刘友华：《算法偏见及其规制路径研究》，《法学杂志》2019 年第 6 期。

⑤王思源，闫树：《隐私计算面临的挑战与发展趋势浅析》，《通信世界》2022 年第 2 期。

⑥吴新慧：《数字信任与数字社会信任重构》，《学习与实践》2020 年第 10 期。

面是为了解决互不信任参与方之间在需要保护隐私信息以及没有可信第三方的前提下进行协同计算的问题,通过技术手段弥合数据信任鸿沟,但是在实然层面上隐私计算又引发了新的信任危机:一方面,如前文所述隐私计算的内置算法协议不尽相同,协议安全根基也各有差异,技术原因造成隐私计算各参与方之间的数字信任机制难以构建;另一方面,算法技术作为隐私计算的底层应用技术,预示着隐私计算同样需要面临"算法黑箱"难题——数据的处理过程处于不透明状态,导致数据主体与隐私计算参与方之间、数据主体与隐私计算平台方之间对数据处理的相关信息处于不对称状态。信息不对称的社会环境中各方主体难以建立信任关系①。隐私计算行业的数字信任一旦出现裂缝,恶意竞争或违法行为导致行业难以进入良性发展阶段,经济活动中的交易成本也随之增加,政府的宏观调控有效性降低②,最终导致数据价值无法释放,数字经济难以赋能高质量发展。

二　我国隐私计算法律规制存在的问题

吉登斯认为,社会风险是"人为制造的不确定性"③。隐私计算所潜藏的数据合规风险、数据泄漏风险、歧视扩大风险、数据群岛风险、信任瓦解风险对公民的隐私权益和数据权益、公共利益和社会秩序造成了威胁,给现代数字社会带来了极大的不确定性,而其形成的主要原因也可以归纳为客观技术局限、主观合规意识欠缺、配套制度缺乏三个方面,具有强烈的人为性。因此,隐私计算所潜藏的风险不能简单地归类为由技术原因导致的技术风险,而是有人为因素的、具有社会危害性的社会风险,对隐私计算的风险治理不能仅凭借技术,还需要通过法律的规制功能进行治理。主要可以从构建法律法规解决合规困境、建立技术标准解决技术难题、监管介入维护成效、赋予救济保障权利、宏观引导筑造信任环境五个方面联动治理风险,但目前各项机制尚未形成行之有效的联动规范体系。

(一)法律法规不完善

隐私计算作为兼顾保护数据权益与促进数据流通的有效技术方案,面临着现有法律规范针对性不强而新制度尚未构建的困境,导致隐私计算的合规性缺乏法律法规的背书,在技术产品设计、业务流程、责任划分等方面欠缺规范指引。我国关于隐私计算的现有规范制度主要表现为以《数据安全法》《个人信息保护法》《网络安全法》三驾马车作统摄、部分政策性文件相配套的局面④。其中,前述法律并未直接提及隐私计算,主要是对数据、个人信息的收集、流通、交易等合规要求作出宏观规范,而政策性文件虽直接涉及隐私计算,但主要是对隐私计算的发展提出政策指向⑤。法律法规的不健全主要体现在以下两个方面。

一是隐私计算的法律定位不明确。根据《网络安全法》第四十二条第一款规定"未经被收集者同意,网络运营者不得向他人提供个人信息",隐私计算技术本意是在保护隐私的基础上尽可能汇集多方数据,但参与方从数据主体处所获得的授权往往仅止步于参与方自用,与其他参与方共同使用的行为一定程度上破坏了这一规定。与此相反的是,该条款存在"经过处理无法识别特定个人且不能复原的除外"的豁免条款。但现阶段,我国并未出台匿名化技术标准或相关指引性文件,仅在《个人信息保护法》第七十三条规定,匿名应当满足数据无法单独识别特定个人且匿名数据与其他信息结合也无法识别特定个人的条件。一般来说,隐私计算可能符合"无法识别"及"不能复原"的要求,却仍无法经受技术进化和时间迁移的考验——理论上而言,类似神威等超级计算机的巨型计算能力可以轻松突破"匿名",同时,此刻的匿名并不能代表多年后的彼时仍旧安全。因此,隐私计算处理数据是否符合法律规定的匿名化尚未有定论。

①张清,郭胜男:《人际信任、法律信任与数字信任:社会信任的谱系及其演进》,《哈尔滨工业大学学报(社会科学版)》2021年第6期。

②欧阳日辉:《数字经济时代新型信任体系的构建》,《人民论坛》2021年第19期。

③安东尼·吉登斯:《现代性的后果》,田禾译,译林出版社2000年版,第115页。

④隐私计算联盟、中国信息通信研究院云计算与大数据研究所:《隐私计算白皮书(2021年)》,隐私计算联盟微信公众号2021年7月发布,第3页,https://mp.weixin.qq.com/s/LrZSlyIhZmDJGS8qcPGd6w。

⑤参见工信部《大数据产业发展规划》、中国人民银行《金融科技发展规划》、国家发改委、中央网信办、工信部、国家能源局《中国一体化大数据中心协同创新体系算力枢纽实施方案》、工信部《网络安全产业高质量发展三年行动计划》。

二是法律规范中“知情同意原则”的失效。该原则作为个人信息保护领域的“帝王条款”，正面临着不具有合理性与可行性的适用困境：一方面，知情同意原则不具有合理性，数据处理者自身并不能完全预知对信息的处理范围，也就没有告知信息主体处理范围并获得其相应同意的可能，同时，相较于传统信息，网络时代的信息往往生成于网络服务提供平台中，不符合知情同意原则的前提——信息控制在信息主体手中。另一方面，知情同意原则不具有可行性，其一是过高的成本导致不具有经济上的合理性，其二是形式大于实质，基于技术的不对称地位，网络服务商可以通过格式合同强制获取信息或越权获取信息。① 尤其是在对包括个人信息在内的数据处理呈动态需求的隐私计算中，这种不合理与不可行更为明显。数据主体的局限性与数据收集者、数据处理者逐利需求之间产生的张力，共同导致“知情同意原则”的实效性大打折扣。

应当说明的是，法律法规无法对技术进行细致入微的规范，但对于隐私计算的合法性、运行合规条件、责任划分等宏观框架应当作出指引，而现有法律规范并未及时作出回应。

（二）国家标准不统一

隐私计算技术标准制定已经成为实务界的共识，国内的隐私计算标准大致能够分成理论层面、测评层面到互联互通层面三个阶段，三个阶段下隐私计算标准的实用性和覆盖范围逐渐变高，标准的参与和发布机构也由企业和行业机构逐渐转向国家和国际层面的机构。现有国际标准主要是对隐私计算的框架和功能规定为主要内容，而国内则主要涉及隐私计算基础功能的标准制定，如中国信通院云大所进行牵头，制定出的《基于多方安全计算的数据流通产品技术要求与测试方法》《基于联邦学习的数据流通产品技术要求与测试方法》《基于可信执行环境的数据计算平台技术要求与测试方法》《区块链辅助的隐私计算技术工具技术要求与测试方法》。这些措施虽然表现出逐渐完成基础功能标准，向性能和安全方面拓展，并力求突破各产品之间的技术壁垒，以推动跨平台之间的互联互通的局面，但不可否认的是，隐私计算相关技术标准仍处于制定初期，其成果与现实需求仍有较大差距②。此外，由中国支付清算协会发布的《多方安全计算金融应用评估规范》作为我国第一个有关隐私计算的金融规范，虽然对数据标准、技术规范提供了指向，但并未形成具有权威性、全国性、统一性的基础标准规范。总的来说，隐私计算技术的发展主要由商业公司开发与运营，市场的无序性、技术的差异性、规范标准的缺失，共同造成现有技术标准的失序，导致技术的安全合理性存在疑虑，从而只能在小范围内测试和监管沙盒内应用③。

（三）监督管理不全面

监管的目的在于矫正。客观上，隐私计算通过密码学、计算机科学等技术对原始数据进行处理转换，技术本身具有复杂性与黑盒属性。主观上，技术使用者的主观意思也使得隐私计算技术成为双刃剑。在此基础上，自然发展所产生的隐私风险、权利瑕疵、数据群岛、歧视放大等弊端，需要通过监管进行矫正。根据《数据安全法》第六条规定，我国数据监管采用以网信部门协调统筹，各地区、各部门对本地区、本领域的数据进行安全监管的模式，该模式虽然结合了欧盟与美国的监管模式，即一元模式下由独立的数据监管机构履行监管职责的独立性与集中性优势和多元模式下各行业分散独立监管的灵活性与专业性优势，但在实践中却难以发挥出应然的效果。首先是各监管机构之间的监管范围与责任不明确，除《数据安全法》用笼统的“依据有关法律、行政法规在职责范围内负责”外，没有再次进行具体规定，而除个别行业如金融、公安等领域有相应的行政法规或部门规章进行具体规定，绝大部分行业领域并未具有配套的规定，同时，对于何为“统筹协调”也未作明确规定。其次是数据本身涉及多领域、多群体、多行业，难以将数据划分至某一领域或行业进而由某一机关进行监管，强行强调部门分殊极易造成各监管部门之间有利可图则相互争取、

①梅夏英，朱开鑫：《论网络行为数据的法律属性与利用规则》，《北方法学》2019 年第 2 期。

②零壹财经 · 零壹智库：《开启新纪元隐私计算在金融领域应有研究（2021）》，零壹财经网 2021 年 10 月发布，第 25 页，https://www.01caijing.com/viewer/pdf.htm?filePath=attachment/202110/1E69951CB597495.pdf。

③毕马威，微众银行：《深潜数据蓝海 2021 隐私计算行业白皮书》，毕马威网 2021 年 4 月发布，第 24 页，https://mp.weixin.qq.com/s/jXWvDSiDP9nGPBsuSIDbBA。

无利可获则相互推诿的乱象。最后是我国的数据安全监管模式偏向于事后监管,虽然数据安全监管通过设定“知情同意原则”的事前监管发挥头阵作用,但该原则在现实中的效果已经难掩颓势,主要依靠对数据侵权结果进行惩戒的方式进行管控,缺乏有效的事前、事中监管,因此难以形成全方位的监管链条。

(四)救济保障不平衡

隐私计算中的数据掌控者多为掌握大量数据的大型平台,形式上而言与数据主体均属于平等民事主体,但实质上,基于对数据的控制优势和处理优势,数据控制者获得数据权力,导致数据掌控者与数据主体之间形成影响与被影响、支配与被支配的不平等地位①。平台对其所在领域业务生态内的数据有着极强的掌控力,特别是“算法黑箱”的不透明性,导致数据主体一旦被侵权,难以具备足够的专业技术和条件去收集、固定证据。事实上,隐私计算数据一旦泄漏,涉及的数据主体众多,而当事人单独提起诉讼难以系统性解决问题,有学者提出通过“集体诉讼”或“公益诉讼”谋求被侵权人的聚合与举证责任的平衡,打破大规模侵权与群体性小额争议救济难问题②。但是数据侵权中各数据主体地处五湖四海,过于分散,且聚合存在技术上的困难③,并可能面临“搭便车”或诉讼收益与成本不平衡等新问题。此外,事后救济具有滞后性,较多地注重于事后惩处,而缺少事前的风险预防功能。

(五)宏观引导不及时

隐私计算技术的发展应当尊重“看不见的手”,但隐私计算技术所适用的领域具有明显的公共性,完全依赖市场化路径极易造成市场失灵,政府的宏观调控可以引导隐私计算客观技术朝合规方向发展,促使隐私计算各参与方形成构建信任维系的主观能动,但现行制度下缺乏明确的拉动性政策和标杆性示范项目等引导性措施④。隐私计算的参与者一般包括数据提供方、技术提供方、数据使用方,一方面,对于隐私计算技术平台来说,信任维系的建立及部分基础标准的统一缺乏相应规范引导,导致隐私计算技术产品互联互通存在较大壁垒,形成资源浪费。同时,政府天然具备可以塑造行业和市场认知的重要标杆性应用项目,可推动隐私计算等新型技术的普及发展快速越过磨合期,政府助力的缺失不利于技术实现跨幅度进步。另一方面,对于数据提供方和数据使用方而言,隐私计算技术的选择、适配、安全工作成为使用隐私科技的重要前提,隐私计算科技平台缺乏审查监督、隐私计算科技产品缺少认证评估、尚未建立权威机构定期发布厂商图谱等引导失力导致隐私计算缺乏信任维系。

三　我国隐私计算的行政法规制出路

隐私计算同诸多人工智能技术一样,复杂、多样、难以预测的风险具备更强的外溢性和系统性,超出了个人自治范畴,涉及更为广泛和重大的社会公共利益,这决定了需要国家进行干预风险的立场⑤。从刑事保护角度出发,刑法的谦抑性决定了其处罚范围不宜过宽。隐私计算中可能出现的刑事法律责任主要集中于非法获取计算机信息系统数据罪与侵犯公民个人信息罪,然而,并非所有涉及数据与个人信息侵权的行为都符合相关犯罪的构成。最高人民法院和最高人民检察院均通过司法解释对此类案件的入罪标准进行了设定⑥。而对于不符合此类标准的大量侵权事实,则无法通过刑事路径进行制裁。从民事保护角度出发,主要通过事前赋权和事后救济的手段进行

①尹华容,王惠民:《数据权力的兴起、异化及规制》,《湖南大学学报(社会科学版)》2022年第3期。

②钟瑞华:《美国消费者集体诉讼初探》,《环球法律评论》2005年第3期。

③学者唐林垚认为:“隐私计算‘可用不可见’的特性依赖于数据流通过程中以加密技术、噪点干扰、分布式学习、分属不同的安全物理环境等去标识化与匿名化处理技术,被侵权人欲进行身份的群体互识,必须先实现破解加密、分离噪点、整合模型、击穿物理隔绝等措施,还原数据标识并进行显名化。”简而言之,隐私计算实现数据流通与数据保护依赖于最为核心的去标识化和匿名化安全技术,而这种技术与集体诉讼和举证责任所需的群体身份互识及举证之间存在难以调和的矛盾。参见唐林垚:《隐私计算的法律规制》,《社会科学》2021年第12期。

④毕马威,微众银行:《深潜数据蓝海 2021隐私计算行业白皮书》,毕马威网2021年4月发布,第41页,https://mp.weixin.qq.com/s/jXWvDSiDP9nGPBsuSIDbBA。

⑤孔祥稳:《面向人工智能风险的行政规制革新——以自动驾驶汽车的行政规制为中心而展开》,《行政法学研究》2020年第4期。

⑥最高人民法院、最高人民检察院2011年联合发布的《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》及2017年联合发布的《最高人民法院、最高人民检察院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》。

保护，在事前保护方面，《个人信息保护法》在第四章明确了公民对个人信息处理的知情权与决定权、查阅复制权、可携带权、更正补充权、删除权、解释说明权等权利。隐私计算所造成的数据泄漏中，涉及个人信息和隐私的部分数据有望通过前述规定进行维权，但数据的范畴远大于个人信息①，对既不涉及隐私也不属于个人信息的部分数据，法律尚未赋予相应的民事权利进行保护。即便是已经赋予的知情权与决定权即“知情同意原则”，也面临适用困境。事前赋权不全面，实效不佳的局限凸显。而事后救济方面，如前述所言，存在主体地位失衡和救济不系统、不及时的局限。

相较于民事和刑事保护而言，行政法规制主要依靠行政机关实施，适用范围广，且可以形成事前、事中、事后全链条治理②。隐私计算作为新兴科技正处于难以预测而又高速发展的阶段，弹性需求与变化较大，行政法角度的治理方式多元且灵活，既可以通过行政处罚或行政强制实现预防与惩戒，也可以通过行政奖励、行政征用、行政给付等手段进行柔性引导，更具有灵活性。最后，行政法规制处于持续运行状态，无需依托特定主体的请求启动程序，可以依据风险的状态自主启动规制，并设立一般性规则对类型问题进行系统性规制③，具有及时性、直接性、系统性。对于隐私计算的行政法规制，应当秉持促进数据流通与保障数据权益的平衡，形成技术与法律耦合的总思路。行政法规制包括消极的限制性规制行为，也包括积极的引导性规制行为，具体的行政法规制可以基于五个方面展开：完善法律法规、构建统一标准、巩固信任体系、强化监管力度、引导合规环境。

（一）完善法律法规

隐私计算技术只有在相应治理体系初具雏形的前提下，才能够让优势得到充分发挥。一方面，对于隐私计算的法律定位，欧盟《GDPR》第二十六条规定数据匿名化采用穷尽一切合理可能性的严苛标准，根据我国《个人信息保护法》第七十三条规定，数据匿名化应当满足数据无法单独识别特定个人且匿名数据与其他信息结合也无法识别特定个人的条件，同样采取绝对匿名化的标准。但这一标准在实际中的可行性尚低，有学者提出可以使用“功能性匿名化”标准来进行判断，即数据的匿名与否应当取决于此数据与环境之间的关系④。通过该标准，作为数据使用者的隐私计算各方只要在现有技术和资源情形下保证数据中含个人信息的部分不被识别出即可。因此，隐私计算技术在法律上的定位应当被认定为符合数据匿名化条件的数据处理技术。

另一方面，对于用户协议的问题。诸如用户协议之类的大量自制规范制定尚未做到规范化和程序化，解决的办法就是对于社会规范的制定建立备案审查机制，使其符合法治化要求⑤。对此，可以通过立法规定进行内部审查和外部审查相结合，主要对协议的合宪性、合法性、合规性、合理性、可行性进行审查，内部审查主要由隐私计算参与方内部工作人员或借助法律顾问制度、公职律师制度和公司律师制度进行自我纠错。外部审查则由法律、法规、规章规定的行政主管机关进行承担，主要针对用户协议中部分含基本权益的条款进行审查，以行政机关的专业性、高效性以及低成本性弥补数据主体审查的业余性、低效性、高成本性，既有利于数据合规，也体现服务型政府所为。另外，在原“知情同意”原则基础上，要求隐私计算参与方保证用户授权链条的完整性，即用户的授权应当覆盖全部的隐私计算参与方和隐私计算全部的操作行为。同时，部分隐私计算参与方因计算的动态调整，授权需求具有不确定性。因此，可以尝试采用动态协议规定，要求数据处理主体对确有需要的授权与数据主体进行多次协商。

①《个人信息保护法》第四条规定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。而《数据安全法》第三条规定数据是指任何以电子或者其他方式对信息的记录。可见个人信息具有可识别性，而数据则既包含可识别性信息也包含不可识别性信息，个人信息的范畴小于数据。

②相较于民事和刑事保护而言，行政法对隐私计算风险的治理可以通过行政立法、行政许可、行政审批、行政指导等手段在事前对隐私计算各参与方的合法性进行审查和引导，及时将不符合法律规定的隐私计算参与方和计算平台剔除。对于符合准入门槛的参与方和计算平台，行政机关可以根据法律法规的相关规定及时进行监管。一旦隐私计算过程中出现侵权，可以运用行政强制、行政处罚等方式进行惩处，及时提供救济。事前、事中、事后联动的全链条保护，不仅可以及时预防风险、应对风险，更能促进良性秩序的构建。

③孔祥稳：《论个人信息保护的行政规制路径》，《行政法学研究》2022 年第 1 期。

④张建文，高悦：《我国个人信息匿名化的法律标准与规则重塑》，《河北法学》2020 年第 1 期。

⑤刘作翔：《论建立分种类、多层级的社会规范备案审查制度》，《中国法学》2021 年第 5 期。

(二)构建统一标准

隐私计算使用的技术多样、隐私计算平台标准要求不一、隐私计算产品硬件规格各异,符合市场"百舸争流"的需求,也是角逐出符合市场所需产品与服务的必经之路,同样,法律不应该也不具备为技术细节进行规定的功能,但法律可以引导并建立"和而不同"的标准,如汽车制造行业备受关注的"滑板式底盘"①,可以兼容各种不同的车型,实现了上下车体的解耦。构建隐私计算的行业标准同样可以借鉴这一理念,对行业所急、所盼且具有可行性的领域制定统一标准,如隐私计算的安全标准、技术框架标准、互联互通接口标准、关键技术标准、数据格式标准目前为行业之急需,对其中的安全标准、互联互通标准完全可以在采取公众参与机制、遵循意见征集和论证程序的前提下,依托现有技术、参照法律合规要求制定统一的行业标准。此外,对于现有的行业标准,可以适当将具备可行性的部分升格为具有强制性、普适性的规范。统一而可行的行业标准不仅可以降低成本,也可实现互联互通,增加数据流通度,解决"数据群岛"难题。

(三)巩固信任体系

行政机关的产品认证是对于某项产品、服务或主体合格与否的较为权威的认定,可以成为隐私计算平台之间、平台与用户之间构建信任维系的重要推力。行政机关可以根据《中华人民共和国认证认可条例》及隐私计算相关制度、标准,自行或委托第三方对隐私计算平台、产品的合规性进行认证或检测,经具备资格的机构安全认证或检测,对符合相关国家标准强制性要求的产品予以公布,以此带动隐私计算朝合规方向发展,同时增强市场对隐私计算的使用信心。同时,行政机关可以制定隐私计算产品评估体系,对产品的基础能力、性能、安全进行评估、认证,既可以间接促进隐私计算产品能力提升,也可以解决用户不敢用的问题②,巩固信任体系。

(四)强化监管力度

数据监管是整个数据领域的难题,隐私计算技术虽然可以在一定程度上解决传统数据处理"可用且可见"的弊病,但正因为处理过程使用的技术隐私性更强,处理过程也愈加隐蔽,所需要的监管力度要求也更大③。数据监管主要的问题是监管机构权责不明、全过程监管缺位。因此,一方面,针对我国数据监管"网信部门统筹协调,各行业、各领域在本行业、本领域监管"所产生的九龙治水问题,最为直接的方式是效仿欧盟建立独立而统一的监管机构,有学者认为可以借鉴临时议事机构形式,解决各监管部门之间监管工作过于分散的问题。然而,出于实用主义而言,我国《数据安全法》尚处于公布实施之初,不宜采用大破大立的重构思维,联合议事机构的合法性与实效性也仍存质疑。在此基础上,应当尽快出台相应的法规弥补《数据安全法》权责过于笼统的问题,对各监管机构的权责以及联合机制进行明确而具体的规定。另一方面,针对全过程监管缺乏的痛点,应当建立涵盖事前、事中、事后的全流程监管机制,事前监管主要以数据收集主体备案登记措施为关键,此处的数据收集并非对所有类型的数据收集都要备案登记,这既不可能也不符合数据经济发展的需求,因此,备案登记的对象主要适用于需要收集敏感数据的主体。此外,可构建含政策专家、业务专家、技术专家、法律专家等组成的评审专家团,事前评估合规性与必要性,事中基于监管友好型架构监管数据共享过程,事后针对数据共享争议,开展审计追踪,并建立仲裁及风险补偿机制。最后,在行政机关监管外,结合"企业是隐私计算发展主力军"的现实条件,充分发挥行业组织等社会力量,推动建立类似律师协会的行业监督组织,形成"行政监管+社会力量监督+行业自律"的多元监管局面。

(五)引导合规环境

行政指导植根于现代市场经济的土壤中,是现代行政发展的产物,是塑造良好政府形象的客观需要,也是现代行政效应原则的必然要求④。对隐私计算行业的行政指导可以从参与方主观方面和客观技术方面进行,主观上,首先,应当引导

①滑板底盘的核心理念是将车辆的底盘和车身分层设计,实现上下层解耦开发。简而言之,就是将传统的汽车底盘标准化、模块化,从而可以像"搭积木"一样将各类车身安装至底盘,实现造车的低成本、高效率、高灵活需求。

②袁博,王思源:《隐私计算产品评估体系》,《信息通信技术与政策》2021年第6期。

③王爽:《合法公开个人信息衍生利用的有限告知同意制度研究》,《浙江工商大学学报》2022年第2期。

④杨海坤,章志远:《中国行政法原论》,中国人民大学出版社2007年版,第267页。

公众数据合规意识,既能加强公众对数据的保护意识,也能促进隐私计算行业的发展。其次,引导参与方广泛形成开源意识,推动隐私计算产品互联互通。最后,政务数据的开放流通可以广泛尝试使用隐私计算技术,发挥隐私计算标杆作用。客观上,积极引导隐私计算技术平台展开交流合作,促进主流技术标准的统一化。此外,对于具有不良行为但未引起轻微以上后果的隐私计算参与者,可以采用劝告、建议等软性手段,引导行业良性发展的同时还可以避免行政相对人的过分抵触情绪,便于行政目的的实质性达到。行政指导可以带动隐私计算技术的使用者主观上接受隐私计算技术,客观上减少技术无法互通带来的不便,形成有效的合规环境。

结语

数据风险的治理是数字时代的重要主题,以隐私计算为代表的数据风险治理技术将会不断更新迭代,而在治理社会风险的同时也会不可避免地产生新风险,“治理—再治理”或许会成为数据法学研究领域的一种新常态。同时,数据内嵌的多种法益也决定了其理想的治理模式需要公私法有效融通。正是基于这种趋势,本文对隐私计算的技术原理、潜藏风险、法律规制现状进行了梳理分析,认为民法和刑法保护具有局限性,而行政法规制方案可以通过其灵活、系统、及时、高效的行政行为,以及涵盖事前、事中、事后的全链条治理状态,有效预防和控制隐私计算的潜藏风险。该方案的提出既是为了解决隐私计算的治理难题,引导其在数字经济领域的赋能效用,也是为了论证行政法规制在“再治理”中的重要性与有效性,更是试图为未来对此类新型治理技术进行公私法治理提供有限的参考,推动法律和科技的相得益彰。

Administrative Law Regulation of Privacy-Preserving Computation

YIN Hua-rong & WANG Hui-min

(School of Law, Xiangtan University, Xiangtan 411105, China)

Abstract: Privacy-preserving computation has the function of promoting the “available and invisible” of data, which can meet the needs of both the application of data value and the protection of data security. However, the privacy-preserving computing technology also hides potential data compliance risks, data leakage risks, algorithmic discrimination amplification risks, data archipelago risks, and trust collapse risks, which urgently need to be regulated by law. There are five major problems of the governance of privacy-preserving computing risks in Chinese current laws, that is imperfect legislation, inconsistent standards, incomplete supervision, unbalanced relief, and untimely guidance. Administrative laws and regulations have the advantages of being timely, flexible and systematic, and can realize the whole chain of governance before, during and after the event. It can can fasten the “safety belt” for the development of privacy-preserving computation by improving laws and regulations, building unified standards, consolidating trust system, strengthening supervision, and guiding compliance awareness.

Key words: privacy-preserving computation; administrative law regulations; data rights

(责任校对　葛丽萍)