法商研究 Studies in Law and Business
Vol. 37 No. 6 (2020)

我国个人数据的法律规制

——域外经验及其借鉴

于 浩*

摘要:信息时代个人数据的个体性和公共性双重属性凸显,个人数据问题的时代性及其所涉关系的复杂性使得既有法律难以对其进行有效规制。当前,我国个人数据的法律规制在实践层面面临司法适用冲突与立法表达缺位的困境,在理论层面存在个人数据权利性质争论。放眼域外针对个人数据的规制,美国较为强调数据的财产权属性而实施市场导向规制模式,欧盟则偏重个人数据的人权色彩而实施强政府干预的家长式控制模式,美欧的立法与司法实践可以从不同视角为我国提供有益的经验借鉴。为实现个人数据的公共经济价值和个人权益保障的双重平衡,需要创新规制思维,以个人数据分级分类保护为基础,采取公法与私法协调规制的路径,建立多元主体参与的法律规制体系。

关键词:个人数据 数据分类 公私法协同 法律规制

一、问题的提出

信息时代个人数据的重要性不言而喻。截至2020年3月,中国网民规模达9.04亿,互联网普及率达64.5%,网络购物用户规模达7.10亿。① 如此庞大的网络用户基数,辅之以4G/5G技术、云计算、大数据等新兴技术和互联网金融等新兴产业,产生的个人数据数量和其中蕴含的商业价值将无法估量。数据不断刷新和重塑人们的生活习惯和行为方式,对数据的保护也由传统的个人隐私或商业秘密上升至国家战略高度。② 个人数据具有个体性和公共性双重属性,一方面个人数据是有关个人具体的信息,且由当事人个体参与才得以产生;另一方面,个人数据在数字经济时代又是社会经济运行的基础,生产、流通、分配、消费各个环节都不同程度地需要个体数据参与。倘若不能充分保障个人数据安全,极易出现非法收集、出售个人数据,利用数据侵害他人人格、名誉、隐私等违法乱象;但如果

* 华东师范大学法学院研究员、博士生导师
基金项目:国家社会科学基金项目(19FFXB056)

① 参见《CNNIC发布第45次〈中国互联网络发展状况统计报告〉》,http://www.cac.gov.cn/2020-04/28/c_1589619527364495.htm,2020-08-10。

② 参见[英]舍恩伯格、库克耶:《大数据时代》,盛杨燕、周涛译,浙江人民出版社2013年版,第239页。

武断地全盘否定收集、共享、分析、使用和交换个人数据,势必会造成社会资源的结构性浪费和紧缺,对数字经济产业带来釜底抽薪式的打击。因此,对个人数据的法律规制,需要平衡合理使用与个人利益的双重价值,在保障个人数据安全的同时又不妨碍数据产业的发展。

个人数据法律规制所关注的是相关主体对个人数据享有的权利、承担的义务以及违反义务所应承担的责任问题。个体、企业以及政府都在不同程度上关涉个人数据的产生、使用与保护,对个人数据的法律规制关涉多元主体之间多种关系的法律调整,既有个人与市场企业的私法关系,也有企业与政府之间的公法关系;既涉及财产关系规制,也关系到人格权益保障。当代个人数据问题作为信息时代出现的新事物,加上个人数据所涉关系的复杂性,现行的法律制度未能对个人数据进行有效规制。但是,现代法律作为回应型法,对新出现的社会现象及其可能引发的社会问题,必须做出制度回应。笔者在此从个人数据规制的实践面向出发,通过对现行法律规范体系和实践模式的检视,结合域外个人数据规制的经验,以期构建我国的个人数据法律规制体系。

二、我国个人数据法律规制的困境分析

个人数据对个人与社会都具有重要价值,但其内在的利益冲突不可避免,国家已经出台相关法律法规对此进行规制,然而由于立法存在的不足以及司法实践中存在的冲突,对个人数据的法律规制效果差强人意,其背后更深层次的原因在于,当前对个人数据的理论研究聚焦于数据的人格权与财产权属性之争,过于强调个人数据规制的私法和市场路径,对公法以及政府在数据规制领域的作用关注不够。构建有效的个人数据规制制度,首先要分析当前我国个人数据规制面临的困境。

(一)司法适用之冲突与立法表达之缺位

我国关于个人数据保护的立法散见于各层级、各部门的法律规范中,[①]整体上呈现出条块化、分散化、层级低的特征。通过梳理这些法律规范,可以看出立法中有关数据安全的规制大多是自下而上、标准先行,某种程度上论证的科学性、严谨性有所欠缺,同时因其效力层级不高,所以社会关注度往往较低。例如,《数据安全管理办法》(征求意见稿)第 30 条规定“第三方应用发生数据安全事件对用户造成损失的,网络运营者应当承担部分或全部责任,除非网络运营者能够证明无过错”,要求网络运营者承担过错推定责任的规定明显与民法的一般归责原则相冲突。过错推定仅适用于特殊情形,并须有法律规定,部门规章能否对此进行调整值得商榷。另外,数据规制实践中“九龙治水”“前后不一”的尴尬情形亦是屡见不鲜。

相继出台的各类规范虽对个人数据保护较为重视,但过于原则化的规定使得保护手段和救济标准并不充分和明确,从而减损了其可操作性和执行性。例如,《中华人民共和国民法总则》(以下简称《民法总则》)第 111 条规定“自然人的个人信息受法律保护”,这标志着国家以基本法律的形式对自然人个人信息的民事司法救济作出了原则性规定,但个人信息的范围、判断标准仍然未明确规定,使得实践中对个人信息的保护处于一种力有不逮的状态。《中华人民共和国民法典》(以下简称《民法典》)

① 例如,《中华人民共和国侵权责任法》第 2 条、第 36 条;《中华人民共和国消费者权益保护法》第 29 条、第 56 条第 9 项;《中华人民共和国网络安全法》《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》《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》《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》《互联网安全保护技术措施规定》《计算机信息网络国际联网安全保护管理办法》《互联网电子公告服务管理规定》《电信和互联网用户个人信息保护规定》;等等。

将个人信息置于人格权编，虽有明确个人信息的使用原则以及信息主体的权利，但具体规定仍有待进一步完善。

司法适用中对何种行为构成对个人数据的侵犯这一问题的认定亦意见不一。例如，在“朱烨诉百度隐私权纠纷案”[①]中，朱烨称在使用百度搜索引擎对相关关键词进行搜索后，会在其他网站出现与键入关键词高度相关的广告。朱烨认为，百度公司利用网络技术追踪其线上行为，并将其行为偏好、生活需求等信息披露给相关商业网站，对其进行有针对性的广告投放，不仅违反了知情同意规则，也侵害了其隐私权。一审法院判决认为，朱烨的搜索行为在网络空间中留下其个人的活动轨迹，进而反映出其兴趣爱好和需求，这在一定程度上标识了个人基本情况和私人生活情况，属于个人隐私范围，即属于人格权范畴。二审法院却认为，百度的个性化推荐并不符合个人信息的“可识别性”要求，且原告未能证明百度向合作方披露的事实，不构成《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第12条“侵害个人隐私和个人信息责任”中对“公开行为”的要求。再者，储存在用户本地终端上的数据(Cookie)技术是网络搜索引擎普遍使用工具，百度在其使用说明中也已有提及，用户的使用行为表明其默示同意百度对其推送个性化服务。因此，法院判决百度不构成隐私权侵权。[②] 两级法院就同一案件作出截然相反的判决，足以反映在我国现有法律语境下，个人信息和隐私权的内涵及外延已经因数据而发生深刻变革。事实上，该案的二审判决存在诸多可商榷之处：就举证责任层面而言，用户对互联网公司是否未经授权便向第三方提供用户信息这一事实取证、举证十分困难；就技术层面而言，即便互联网企业未直接向合作方提供用户账户、姓名、身份证号等敏感信息，但随着技术的发展，企业只要掌握用户足够多的信息或与其他信息进行结合，就能通过对数据的分析与交叉验证识别出用户的真实身份；就“知情－同意”规则而言，其形式上虽表现为保护个人数据权利，但其实质却形同虚设，现实中大多数人每天接触不同的网页与手机应用程序，并不会对相关说明或须知进行详细阅读，即使阅读过也未必能够理解其真实含义。举证责任划分的形式公平并不能掩藏其实质的不公，个人就其掌握的社会资源和技术而言，举证和取证始终处于弱势地位。

(二)人格权抑或财产权性质之争

随着权利日益成为社会主流话语，权利表征价值正当性的身份逐步被认可。个人数据权是何种性质的权利？目前学术界尚未形成统一的话语体系，论争主要分为以下两点：

1.个人数据的人格权保护。坚持人格权说的学者认为，个人数据之所以需要进行特别保护，主要是因其具有“可识别性”即具有强烈的人格特征。[③] 从我国部门法层面考察，首先，《民法总则》第111条作为个人数据保护的基本法律依据，紧跟确认与保护人身权的条文之后，根据体系解释，说明立法者的态度是从人身权的角度看待个人数据保护。虽然学者在该项权利属于一般人格权还是独立人格权等问题上仍存在争议，但将其纳入人格权框架已基本达成共识。其次，从文义解释的角度看，《中华人民共和国网络安全法》(以下简称《网络安全法》)第76条、《民法典》第1034条以及涉及个人数据的各类法律规章文件等，基本形成了将“可识别性”作为界定个人数据要素之一的共识。再次，从比较法视阈考察，欧洲议会制定的《一般数据保护条例》(General Data Protection Regulation，以下简称GD-

① 参见江苏省南京市鼓楼区人民法院(2013)鼓民初字第3031号民事判决书。

② 参见江苏省南京市中级人民法院(2014)宁民终字第5028号民事判决书。

③ 参见王利明：《论个人信息权在人格权法中的地位》，《苏州大学学报》(哲学社会科学版)2012年第6期。

PR)第4条旗帜鲜明地提出了“可识别性”的要求,即当数据可独立或与其他数据结合后可指向个人时,该数据就应当属于需要保护的个人数据。同时,GDPR的某些条款体现出禁止处理涉及人格利益数据的倾向,如第9条规定“对于那些能够识别宗教信仰、种族、基因、健康等信息的数据应当禁止处理”。因此,个人数据具有强烈的人格权属性。

然而,个人数据的人格权保护面临诸多问题。人格权保护模式看似能为个人数据提供有效且全面的保护,但泛化保护的另一面则是权利的边界难以确定。例如,GDPR虽然给中小企业规定了豁免条款,但在排除“可能给数据主体的权利和自由带来风险”这样的条件之下,小企业仍将面临非常不确定的执法,这将有悖于针对中小企业设立豁免条款的初衷,也不利于中小企业的健康发展,并可能对整个数字经济造成影响,目前已出现数据供应商将与自己相关的合规成本转嫁给客户的现象。① 再如,关于“被遗忘权”的规定,互联网企业在收到用户的“擦除”请求时,应当对该请求进行实质性审查以保证公众的知情权、隐私权及其他权利,而这势必耗费大量的资源,并增加互联网企业的负担。② 不仅如此,当下人格权保护的形式也难尽如人意。目前,人格权保护模式多采用“知情-同意”规则,强调对自然人赋权以保证自然人控制管理个人数据的能力,但这一规则越来越面临形式主义的困境。因为“知情-同意”规则虽然形式平等但实际却是格式条款,且片面加重了用户的知识负担,要求普通用户具备完全清楚规则所有条款的能力,着实是强人所难。此种形同虚设的人格权保护模式,背后更多的是用户对隐私公告的一次漫不经心或无可奈何地点击。③

2.个人数据的财产权保护。个人数据的人格权保护架构难以适应数字经济对数据交换、数据共享等快速发展的需求,在推动数据共享、促进数据交流的背景下,个人数据财产权化的理论应运而生。个人数据财产权化反对为保护个人信息而对数据活动进行简单粗暴的限制,要求在保护个人信息的天平上向推动数据流通方向倾斜。从数据安全角度考虑,对个人享有的数据赋予财产权后,个人对自己的数据享有控制、处理、收益、处分等权益,企业若期望获取个人数据,应当在获得个人同意后,以支付合理对价或提供服务的方式交换数据,若未经个人允许而擅自获取和使用个人数据,则构成侵权,应按照侵权法等相应规定追究其相关责任。④ 从经济学角度观察,在实践中,企业已经广泛采用个人数据财产权化的做法,在用户使用或登录其网页、应用程序后,企业将对用户提供或产生的数据进行收集、存储、分析甚至出售,这已然成为一种常态,许多互联网企业甚至将数据作为其核心竞争力之一。⑤《中华人民共和国数据安全法(草案)》也将数据作为一种财产客体,其第17条明确提出要“建立健全数据交易管理制度,规范数据交易行为,培育数据交易市场”。个人数据财产权化符合市场趋势,既将选择权交于消费者,同时也为企业利用数据资源提供了便利与通道。

然而,个人数据财产权化的设计也面临诸多问题。首先,个人数据财产权化或面临较高的交易成本。通过建立“数据市场”可以将财产权化设计落到实处,但个人数据市场良好规范地运转需要通过

① See Angelique Carson, Should vendors be able to pass along costs of GDPR compliance? https://iapp.org/news/a/should-vendors-be-able-to-pass-along-costs-of-gdpr-compliance/, 2020-08-10.

② 参见于浩:《被遗忘权:制度构造与中国本土化研究》,《华东师范大学学报》(哲学社会科学版)2018年第3期。

③ 参见丁晓东:《个人信息私法保护的困境与出路》,《法学研究》2018年第6期。

④ 参见[美]劳伦斯·莱斯格:《代码2.0:网络空间中的法律》,李旭、沈伟伟译,清华大学出版社2009年版,第248页。

⑤ See Jessica Litman, Information Privacy/Information Property, 52 Stanford Law Review, 1283 (2000).

建立一个完善的监管机制与市场流通机制，而这将带来巨大的交易成本。[①] 更重要的是，个人数据财产权化设计是否会真正增加个人数据的安全性仍未可知。其次，将个人数据视为私有财产可能并不会增加对隐私的保护力度。当个人将其财产权益转移到数据中时，个人就失去了对数据的控制，买方可以毫无限制地将其出售。在此状态下，数据保护所面临的困境将是数据复制的无限性与人力所能防范风险的有限性之间的矛盾。而在企业向个人支付对价获取数据后，企业仍无法完全获取对该数据的使用权限，且在个人仍可通过主张被遗忘权或数据携带权要求企业删除数据的条件下，该项权利很难被纳入财产权范畴。[②] 最后，个人数据财产权并不能消除侵犯隐私的风险，如果法律赋予个人数据财产权，那么它应该或至少包含权利人在一定程度上限制他人转售其个人数据的权利。[③] 即使是通过匿名数据出售方式，隐私披露风险依然存在。例如，美国一些州的法律一般禁止在未经患者同意的情况下向第三方披露患者的保密信息，但联邦《健康保险携带和责任法案》允许共享不能识别单个病人身份的信息。[④] 事实上，无法识别身份的病历仍可通过结合就诊医生、药房、医院、保险公司、住址等侧面信息来再次确定病人身份。[⑤] 由此病人的隐私还是处于风险之中。

三、个人数据法律规制的国际镜鉴

欧盟与美国的数据规制实践处于世界领先地位，基于各自的历史沉淀与现实挑战，欧盟与美国形成了各具特色的个人数据规制体系，前者是强政府干预的家长式控制模式，后者是强调私人财产权的市场导向规制模式，政府、市场与个人在其中扮演的角色各有侧重。深入分析欧盟与美国制度的特征，可以为我国实施个人数据的法律规制提供有益的经验。

（一）个人数据法律规制的美国经验

1.“个人－公权主体”框架下对公权力的约束。由于在美国对个人数据的侵犯首先是从公权力开始的，因此美国在“个人－公权力主体”这一范畴中采取了严格甚至近乎刻板的方式保障公民的人格尊严、人身自由等权利不受侵犯。在宪法层面，美国宪法第一修正案规定了信仰隐私，第三修正案规定了未经允许士兵不得擅闯住宅的隐私，第四修正案规定了公权力不得进行不合理的搜查与扣押，第五修正案则通过不得强迫个人自证其罪以保护个人信息隐私。在其他法律规范层面，1966 年出台的《信息自由法》在保障政府信息公开的同时，对政府披露的信息类型也做了一定的限制。1973 年发布的《记录、电脑与公民权的报告》，分析了“自动化个人数据系统可能导致的不良后果”，并提出“公平信息实践原则”以规制政府与企业的个人信息处理活动，奠定了个人数据保护制度的基础。根据这一原则，个人必须能够知道其他人收集了哪些有关他的信息和这些信息如何被使用；个人必须能够拒绝某些信息被使用并能够修改不准确的信息；信息收集组织有义务保证信息的可靠性并保护信息安全。1974 年，在吸收“公平信息实践原则”基础上出台的《隐私法案》进一步对联邦机关的资料收集、使用

① See Kenneth C. Laudon, Markets and Privacy, https://papers.ssrn.com/sol3/papers.cfm? abstract_id=1284878 # #, 2020－08－10.

② See Pamela Samuelson, Privacy as Intellectual Property? 52 Stanford Law Review, 1125(2000).

③ See Jessica Litman, Information Privacy/Information Property, 52 Stanford Law Review, 1283 (2000); Hal R. Varian, Economic Aspects of Personal Privacy, Internet Policy and Economics, 2009, pp. 130－132.

④ See Kenneth C. Laudon, Jane P. Laudon, Management Information Systems, Pearson, 2011, p. 206.

⑤ See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review, 1701(2010).

和散播行为进行了调整。[①]

除了从立法层面对公权力侵害个人数据加以规制之外,美国司法实践也对个人数据的公法规制展现出严肃姿态。1969年,法院在"斯坦利诉乔治亚州案"[②]的判决中确认了个人在家中拥有观看色情作品的权利。在"美国诉伍瑞案"与"莱利诉加利福尼亚州案"[③]中,法院认为,现代手机在存储信息的数量和质量上均具有更大容量,若允许公权力肆意搜查被捕者手机,获取其中的数据,相当于为公权力打开一扇门,让他们了解被捕者生活中最隐私的细节。法院将允许无证搜查手机与向执法部门提供进入被捕者家中的钥匙进行了比较,认为其中一种搜查的侵入性并不亚于另一种搜查,由此援引宪法第四修正案判决不得对手机进行随意搜索。由此可见,美国在个人数据方面对公权力机关始终保持着足够的警惕,并对公权力加以原则性和扩展性约束。

2."分治"与"市场导向"背景下对私主体的规制。在私人行业的治理层面,美国根据各行业特点有针对性地制定行业隐私保护法律,作为以侵权行为为基础的习惯法之补充。例如,在金融领域中,《金融隐私权法案》对银行雇员披露金融记录及联邦立法机构获得个人金融记录的方式予以限制;在保险领域中,《健康保险携带和责任法案》规定个人健康信息只能被特定的、法案中明确的主体使用并披露,个人有权控制和了解本人的健康信息;在电视领域中,《有线通讯隐私权法案》规定闭路电视经营者在未获得用户事先同意的情况下禁止利用有线系统收集用户的个人信息;在电信领域中,《电讯法》规定电讯经营者有保守客户财产信息秘密的义务;消费者信用领域则是由《公平信用报告法》和一些州的法规赋予消费者对信用调查报告的权利,规定消费者信用调查/报告机构对报告的制作、传播、对违约记录的处理等诸多事项,明确消费者信用调查机构的经营方式,旨在保护消费者免受错误信用信息的侵害;在儿童隐私保护领域,《儿童在线隐私权保护法案》规定网站经营者有义务向其父母发送隐私权保护政策的通知,以及对13岁以下儿童个人信息的收集和处理原则与方式等。[④] 美国迄今为止未像欧盟那样出台针对个人数据保护的全国性或统一性的法案,只有行业性、部门性的法律,虽然各个州都在积极出台相关的法律,但保护力度不同,规范亦不统一。

除"分治"外,在"市场导向"下将数据权利定性为"财产权"则是私人行业之列的另一大特点。在市场经济中,继承传统自由主义产权理念的自我监管模式是基于数据(包括牵涉个人隐私等人格利益的数据)被定义为个人财产这样一种假设。[⑤] 在这种情况下,市场中的公司仅是一个合法的交易伙伴,消费者作为一个理性的经济人,在市场中可以基于供需关系同意或授权将个人数据作为商品进行交易。[⑥] 针对由于信息不对称可能带来的消费者不了解其信息价值而盲目出售的情况,一些学者提

① 参见李明:《大数据时代美国的隐私权保护制度》,载彭冰主编:《互联网金融的国际法律实践》,北京大学出版社2017年版,第404页。

② See Stanley v. Georgia, 394 U.S. 557 (1969).

③ 参见刘广三、李艳霞:《美国对手机搜查的法律规制及其对我国的启示——基于莱利和伍瑞案件的分析》,《法律科学(西北政法大学学报)》2017年第1期。

④ 参见李明:《大数据时代美国的隐私权保护制度》,载彭冰主编:《互联网金融的国际法律实践》,北京大学出版社2017年版,第405页。

⑤ See D. Zwick, N. Dholakia, Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right, 11 Electronic Markets, 118(2001).

⑥ See R.S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Georgetown Law Journal, 2381(1996).

出了高度监管的产权制度，其中包括一些以产权为导向的权利和补救措施。[①] 具体包括赋予数据出售个体享有要求数据收集企业对框架协议进行解释阐明、对数据进行修正或删除等权利，要求企业承担针对个人隐私或敏感数据收集的预先通知、保密等义务。整体而言，美国针对个人数据，强调其财产权属性而实施了市场导向的规制模式。

（二）个人数据法律规制的欧盟经验

20 世纪六七十年代，欧洲一些国家逐渐意识到自由放任的信息和通信技术的发展会对社会自由和个人隐私构成威胁。[②] 1981 年，欧洲理事会各成员国签署了欧洲系列条约第 108 号《有关个人数据自动化处理之个人保护公约》，此后陆续制定了《关于保护共同体个人信息及信息安全的指令草案》（1990 年）、《关于涉及个人数据处理的个人保护以及此类数据自由流动的指令》（1995 年，以下简称《个人数据保护指令》）、《电信部门个人数据处理和隐私保护指令》（1997 年）、《关于存留因提供公用电子通信服务或者公共通信网络而产生或处理的数据及修订第 2002/58/EC 号指令的第 2006/24/EC 号指令》（2006 年）、《关于在犯罪问题方面的个人信息保护和司法合作的政策框架》（2008 年）、《欧盟 Cookie 指令》（2009 年）、《一般数据保护条例》（2016 年）等。结合《欧盟基本权利宪章》第 8 条将个人数据权利单独上升至基本权利乃至人权层面进行保护可知，在宪章基本精神的指导下，欧盟正在将个人数据权利以人权的范式，用更高要求、更高标准、更高姿态重新定位个人数据权利并对其进行更全面的保护。

1.“个人－公权主体”：从“分治”到“一体化”。欧盟对公权力的规制，经历了从“分治”到“一体化”的变化进程。德国最早以计算机技术收集和自动化处理公民个人信息并建立信息数据库，但设立数据库所存在的潜在威胁以及可能对私权利造成侵害的恐慌，促使议会制定了《联邦资料保护法》，并以此规制联邦公共机关和执行联邦法的州公共机关收集、处理、转移个人资料等行为。德国著名的“人口普查案”[③]的起因也是公民为防止公权力侵犯个人隐私等问题而进行的博弈。法国也有类似的进程，个人资料的最初规制便是源于法国政府所采取的“儿童医疗自动化管理系统”以及“行政管理和个人档案自动化系统”等搜集公民健康状况等个人信息项目的曝光，公民担心公权力过分介入私人生活，影响个人自由，由此催生了《信息、档案与自由法》。[④]

伴随着欧盟的一体化进程，欧盟的个人数据保护和监管力度逐步加强，以高位阶法规约束管控数据权利，成员国开始以共通的指令或条例来规制数据问题。通过高层立法的统一约束标志着数据保护不再被认为是一个地方性或行业性现象，不应由各成员国根据欧盟指令各行其是，而应成为更高层面的总体性事项，由欧盟以统一方式直接加以规范。在考察欧盟数据规制立法进程时，可以发现大部分国家均对公权主体与私权主体进行了规制，但对公权力的规制多散见于各个法律文件之中。最为典型的属《欧盟基本权利宪章》第 8 条与《欧洲人权公约》第 8 条以及欧洲人权法院 2017 年发布的个人数据保护手册。有学者曾对欧洲人权法院审理的 50 个国家公权力与个人数据权利冲突案例进行梳理，国家败诉的比例约为 2/3。欧洲人权法院在判断公权力是否侵犯个人数据权利时，以“合目的

① See Jacob M. Victor, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. 123 The Yale Law Journal, 522－526(2013).

② See Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers, University of Michigan Press, 1971, p. 246.

③ 参见孔令杰：《个人资料隐私的法律保护》，武汉大学出版社 2009 年版，第 116～118 页。

④ 参见孔令杰：《个人资料隐私的法律保护》，武汉大学出版社 2009 年版，第 124 页。

性”“合法性”“合比例性”三大要素共同判断,可见标准十分严苛。[①] 由此可见,欧盟在个人数据保护方面除以立法加强对公权力的约束之外,在司法实践中对公权力干涉公民个人数据的要求同样严格。

2.“个人—市场私主体”:强政府干预。当下,欧盟法规对个人数据规制的涵盖面愈发广泛,涵盖刑事、通信、网站等多领域,既有以GDPR为代表的统领性条例,也有多领域的协调配套和规则细化。对市场私主体的规制要求也相当严格。以GDPR为例,GDPR对数据运营者在数据收集、使用、存储等环节应当履行的义务作了全方位规定。对在欧盟设立机构向欧盟公民提供商品和服务以及其他控制处理、接收监控欧盟公民个人数据的互联网企业,GDPR提出了较高的软硬件和人财物标准。就数据运营者而言,其承担向数据主体提供个人数据相关信息及数据副本、修正完善错误和不完整数据、被遗忘权对应的删除数据、协助数据主体携带个人数据、避免数据主体受不当自动化决策等义务。以上这些义务仅仅是数据主体享有的权利中需要数据运营者予以配合的实质性义务。[②] 此外,GDPR本身对数据运营者的义务也作了许多规定,如通过设计及默认方式实现数据保护、全面记载处理活动、确保数据处理过程安全性、数据泄露时的通知、数据保护影响评估等义务。诸多义务的罗列与规制,呈现出欧盟偏重个人数据的人权色彩而实施了强政府干预的家长式控制模式。

(三)数据权利现象与规范的比较分析

1.“个人—公权力主体”:不同历史时期同样的人权色彩。美国与欧盟面对“个人—公权力主体”这一范畴时政策基本一致,即较苛刻地限制公权力作为。这一问题根源于公民对政府的不信任,因为政府为恶永远比个人为恶更为可怕。美国学者埃德温·布莱克曾指出,第二次世界大战期间,详细和完备的个人数据曾被纳粹用来清洗犹太人和迫害反纳粹人士。第二次世界大战时期虽然不存在计算机,但借助当时的IBM穿孔卡及卡片分类系统通过种族人口普查可整合宗教信仰等各类数据,纳粹分子便是通过数据整合识别分类出犹太人,从而进行大肆屠杀。[③] 这一创伤为欧盟的数据权利规制留下了深刻烙印——无论是出于何种目的进行的个人信息数据收集,到后来一定会被滥用。这也是德国“人口普查案”的历史根源所在。于美国而言,权力的分立是美国政治、法律、历史上的显著特征,美国对不受约束的权力具有天然的不信任感。正是这种对政府权力刻骨铭心的不信任及对个人自由和尊严的追求,决定了美国的分权政体。也正如美国学者德肖维茨所说:“美国是由少数族群、异议分子、流亡者、冒险者、怀疑论者、异端、实验者、反对者——多疑而易怒的特立独行者——组成的国家。美国是暴君的梦魇与无政府主义者的梦想。”[④]公民个人的自由和尊严—人权—选择了政府,反过来政府应当保障人权,但公权力天然具有的扩张性决定了其本身应当受到限制。公权力若不加以控制,便会成为“不义”的工具,挤压公民的自由和尊严。为防止这一“恶行”出现,作为权利体系中位阶最高的权利,人权范式是在数据爆炸时代经验和历史教会我们的更好的选择。因此,虽然人权与政府息息相关,但美国《权利法案》为了限制政府权力,仍然确立了无法被代议机构剥夺的某些私人权利。

2.“个人—市场私权主体”:“市场话语”抑或“权利话语”。就“个人—市场私权主体”这一范畴而

① 参见闵丰锦:《个人信息权保护的法律界限研究——基于欧洲人权法院50个判例的分析》,《重庆邮电大学学报》(社会科学版)2018年第4期。

② 参见京东法律研究院:《欧盟数据宪章〈一般数据保护条例〉GDPR评述及实务指引》,法律出版社2018年版,第72~90页。

③ See Edwin Black, IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation, Dialog Press, 2012, pp. 54—58.

④ [美]艾伦·德肖维茨:《你的权利从哪里来?》,黄煜文译,北京大学出版社2014年版,第136页。

言，美国多将数据以财产权的方式加以规制，将重点置于个人信息的“市场话语”和“隐私消费者”的保护，即美国的数据隐私法侧重于保护数据市场中的消费者。美国学者米勒曾言，一个人周围的社会空间，他对过去的回忆、对话、他的身体及其形象，都属于个人，个人数据本质上是个人对私人人格所做决定的权利，应当视为一种财产权。① 在后工业时代，资本主义生产的中心已经由劳动力转变为信息的积累和交换。② 事实上，晚期资本主义的核心不是生产，而是消费。③ 因此，消费者的个人数据是当下资本市场中极具价值的东西，而为了获得交换价值，消费者的数据只有作为商品才可以在市场上进行交易，并取得交换价格。美国在“市场话语”的主导下将数据视为财产权的文化与态度可谓一目了然。但个人数据财产化的问题在于，既然公民对其财产拥有绝对的使用、收益、处分等权利，那么个人数据购买者是否可以据此将其交易获取的个人数据随意出售呢？

欧盟进路则迥然不同。个人数据保护是所有欧洲人的一项基本权利，GDPR 就是本着这种以人权为导向的宗旨起草的。④ 欧盟通过将个人数据权利上升至人权，除宣示以及表达其对公民数据权利保护的决心外，更是以一种家长式的方式规定了比美国更为严苛和明确的公民同意规则，进而加强数据主体对其数据的控制。这种人权话语看似效力强、层级高，实则容易造成负面影响。一方面，过于严苛的控制无形中增加了市场私主体的生产成本，加重了其承担的社会责任，在一定程度上阻碍了数据流通和应用。另一方面，对个人数据的保护可能落入形式主义的窠臼，因为判断数据收集、使用和披露效果的好坏取决于实践结果。现实中许多隐私损害是由不同实体在一段时间内聚合数据片段造成的，甚至连市场私主体在搜集数据时也难以穷尽数据在二次、三次聚合分析后所产生的价值，就更不要说公民个体在不了解潜在用途的情况下，权衡披露信息或允许网络经营者收集、使用的成本和收益了。⑤ 因此，只有在实践结果明显不好时，这种家长式作风才容易被证明是正确的，但以结果去判断过程极易陷入一种“隐私狂热”的困境之中。

四、我国个人数据规制体系的建构

我国个人数据规制体系的建构需要立足于本国国情。当前，数字经济方兴未艾，个人数据成为经济发展的重要推动力，我国还处于发展阶段，欧盟强政府干预的家长式控制模式并不适用于我国，过度保护个人数据将不利于经济发展与国际竞争，因此需要尽可能地合理利用个人数据，充分发挥市场在个人数据规制过程中的重要作用。然而，我国又具有一定的全能型政府传统，政府是人民利益的天然代表，只要市场不能做的或者做不好的，政府就有责任去做，⑥美国强调私人财产权的市场导向规制模式也不适用于我国。因此，我国个人数据的规制需要协调好政府与市场的作用，建构多元治理的规制体系。总体而言，应当以个人数据分类分级为基础，采取公法与私法协调规制的路径，建立多元

① See Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers, University of Michigan Press, 1971, p. 320.

② See M. Poster, The Mode of Information, University of Chicago Press, 1990, p. 30.

③ See F. Jameson, Postmodernism, or the Cultural Logic of Late Capitalism, 146 New Left Review, 55－75(1984).

④ See generally Joel R. Reidenberg, E－Commerce and Trans－Atlantic Privacy, 38 Houston Law Review, 717, 730－732 (2001).

⑤ See Daniel J. Solove, Privacy Self－Management and the Consent Dilemma, 126 Harvard Law Review, 1880 (2013).

⑥ 参见史际春：《政府与市场关系的法治思考》，《中共中央党校学报》2014 年第 6 期。

主体参与的规制体系。

(一)实施个人数据分级分类规制

不同个体的个人数据以及同一个体不同方面的个人数据,可能具有不同的价值。完全按照统一的模式进行保护难以适应数据差异性的现实,也容易耗费法律资源。因此,个人数据分级分类保护制度或更适合实践需求。

就保护主体这一问题,从上文美国行业分治模式可以看出,针对不同的人群如儿童、病人、政客的个人数据,具有不同的保护标准。不同数据主体之间对数据保护的个人预期是存在差距的,有学者曾称"为确保民主,法律保护公职人员外的个人的隐私"。① 理论上个人数据背后蕴含的人格尊严等法益不应有三六九等之分,但从道德伦理和现实需要等角度考虑,有些人的数据应当受到重点、特殊的保护,如儿童数据、病人数据等,对此类主体在个人数据保护层面应当予以强力关注。而有些人的个人数据则因其享有的社会地位或职业属性,应当在一定程度上让渡给社会公共利益或社会大众,如政府工作人员或社会公众人物等。

个人数据分级保护的具体内容涉及对个人数据如何进行分类的问题。一般而言,可以根据数据性质划分为敏感数据与非敏感数据,敏感数据不同于匿名数据等去标识化数据,也区别于一些与人身相关但并不够私密、敏感的数据,具体如姓名、性别、民族、种族、宗教信仰等。② 决定信息敏感程度的最重要因素之一是个人的隐私感知和个人羞耻心理,③这应结合本国文化及国民认知水平来判断。

非敏感数据又可分为私密性较弱的个人数据以及匿名数据,此类数据属于基数最为庞大的数据类型,种类繁杂且数量繁多,因此可以通过合理预期原则的应用将数据保护场景具体化。当个人数据难以通过分类方式得到保护,可将数据进行个案化的讨论。当以社会一般人的理性标准判断个人数据的使用、处分、收益、流转等行为超出个人合理预期范围时,个人有权被及时通知并作出判断,否则即构成侵权。④ 但众多的非敏感数据的聚合和积累仍有可能造成个人数据的泄露或遭受侵犯。因此,从长远来看,孤立的个人数据分级保护制度仍存在不足,需要进一步完善。简单有效的办法便是将被遗忘权和个人数据便携性结合,赋予个人以删除个人信息的权利,⑤即对敏感数据网络经营者应承担保密、适时删除以及在收到用户要求时及时删除的义务,而对非敏感数据,则可设置一个恰当期间,即在此期间内除非用户要求,否则网络经营者有权使用该数据,但在此期间经过后网络经营者则必须删除该数据,且无须数据主体提出要求。

(二)公私法协调保护个人数据

目前,我国个人数据保护问题的讨论多聚焦于私法领域,将个人数据规定在《民法总则》民事权利章、《民法典》人格权编,这与欧盟及美国等国家将个人数据保护和隐私权密切相连进而采取私法保护

① Clifford G. Christians, The Ethics of Privacy, G. Whitehouse, Journalism Ethics: A Philosophical Approach, Oxford University Press, 2010, p. 203.

② See A. Etzioni, A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational, 80 Brooklyn Law Review, 277 (2015).

③ See Sabah Al-Fedaghi, How Sensitive is Your Personal Information? 2007 ACM Symposium on Applied Computing, 2007, pp. 165-169.

④ 参见丁晓东:《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。

⑤ 参见罗勇:《论我国个人信息保护立法中"被遗忘权"制度的构建》,《暨南学报》(哲学社会科学版)2018年第12期。

模式相一致。然而就域外个人数据保护的经验来看，无论是欧盟还是美国均未将个人数据保护完全归属为私法领域。一方面，欧盟与美国均对公权力侵犯个人数据的情形进行了防范，它们倾向于将数据权利的保护趋向靠拢至基本权利模式乃至人权话语；另一方面，在私主体侵犯个人数据的领域，美国针对特定行业领域的立法分散，而且这些立法并没有赋予个人针对不特定第三人的权利，尤其对普通民事主体收集与处理个人信息的行为，这些法案更加难以适用。因此欧美对个人数据的规制带有明显的消费者法保护或公法规制的特征。

因此，单一私法规制模式已难以满足当下需要。公法规制也应成为我国个人数据保护的重要一环。个人在面对强大的数据企业时始终处于弱势，尤其是在“知情－同意”规则大范围使用时，仅以私法模式保障个人数据权利存在着举证难、保护力度弱等问题。如果国家能对相关风险进行有效的预防管理，个体防范相关风险的压力便可以降低很多，个人信息的收集、使用和流通也会变得更为安全。[①] 因此，将立法赋权模式和行为规制模式[②]相结合是较为适合我国现实的数据规制模式。

就公法与私法混合治理模式的构想而言，知识产权模式给予了较好的参考框架。首先，个人数据的生成过程与文学创作相类似。文学作品是作者个人创造的带有明显个人痕迹的知识财产，而个人数据也是个人部分的生活痕迹，且因个人生活细节的不同而各有差异，因此就数据承载信息本身而言其具有创造性，即每个人都是自己生活的作者，而数据是对生活这一作品的部分承载。其次，个人数据既具有财产价值也具有人格价值。个人数据一旦生成便脱离主体而独立存在，不以主体的意志为转移。个人数据所蕴含的信息具有收集、利用的价值，即具有财产价值。同时，因其承载内容的特殊性，决定了个人数据与公民人格利益相关联。因此，个人数据兼具财产性和人格性的特点与艺术作品相类似。最后，未经数据主体同意或授权的个人数据的流动、传播与艺术作品信息网络传播权和复制权被侵犯相类似。个人数据的人格性使得个人对自身数据的传播抱有可有效控制传播范围的期望，这与艺术作品的传播应获得作者授权的原理十分相似。综上，个人数据的公私法混合治理模式可类比适用知识产权的相关规定，从而兼顾个人数据的财产价值和人格利益。但同时不应放弃对新模式的探索和新法律的创设，因为艺术作品和个人数据还是有本质区别的，个人数据的数量规模和更新速度是艺术作品无法比拟的，而艺术作品的社会价值也不是普通的个人数据可以达到的。我国未来的个人数据立法应当建立一套风险管理制度。例如，针对收集、储存与处理个人敏感信息或海量个人信息的网络与信息设备，比照《网络安全法》第 31 条的规定，要求企业等采取严格的安全保护义务。对一般企业和机构的个人信息收集与利用，则可以借鉴采用风险评估与风险预防制度来有效管理相关的风险。[③]

（三）形塑多元主体参与的规制格局

我国对个人数据的治理，不能脱离当下社会制度背景。数据化浪潮下，传统立法规制中要求被管理者不得或者必须为某些行为的命令控制方式已经不能完全适应个人数据治理与数据保护的需求。借鉴欧盟 GDPR 坚持既保护个人数据控制权利又促进个人数据自由流动的双重价值，以及美国在分

① 参见丁晓东：《个人信息私法保护的困境与出路》，《法学研究》2018 年第 6 期。

② 参见宁立志、傅显扬：《论数据的法律规制模式选择》，《知识产权》2019 年第 12 期。

③ 参见丁晓东：《个人信息私法保护的困境与出路》，《法学研究》2018 年第 6 期。

行业针对性治理个人数据的同时施以强有力的外部执法震慑的经验,[①]结合中国实际情况和数据流动的动态发展趋势,我国应当构建个人数据的多元化规制体系,具体可以从以下方面着手:

1.制定客观、统一、操作性强的数据安全评估办法,评估办法应当包含评估内容和评估程序两部分。首先,确立数据评估内容便可在海量的数据中有选择性的对有价值的数据进行抓取,进而对数据传输和利用进行有针对性的监控和管理,这样既可加强监督力度又可提高执法效率降低管理成本。简单来说就是在海量数据流动的过程中设置无数道滤网,每一道滤网都有针对性地筛选、抓取部分数据,如针对个人身份证编码的抓取、针对个人病例的抓取等。其次,确立数据评估程序有利于行政机关严格依法办事、提高行政透明度,有助于通过科学合理的评估程序维护公民个人数据安全、促进资源优化配置。最后,要兼顾评估和执法的灵活性。在某些特殊情况下,在个人数据遭受侵扰的范围可得到有效控制的前提下,个人数据安全让位给国家或社会公共利益。对公共利益的定义应平衡未来利益和现实利益、评价对象和评价程序之间的关系,切实遵循预防性原则和损害最小原则。

2.强化"元规制"策略,将指导性规范与行业自律相结合。元规制又被称为强制性自我规制,是外部规制者有意促使规制对象本身针对公共问题作出内部式的、自我规制性质的回应,而不是外部规制者的无意而为,元规制既注重外部规制,也整合了自我规制的洞见。外部规制者既可以通过威慑制裁也可以通过奖励,以实现对规制对象采取自我规制措施的目的。[②] 英国学者费恩和赖特认为,个人数据安全问题在很大程度上是一个道德问题。[③] 意大利学者曼特列罗认为,面对硬性的法律规范,市场私主体更愿意支持市场的自我调节,采用行业自律与国家标准相结合的模式,能够确保所有利益相关者的参与。[④] 这种行业自律或者说市场的自我调节,与美国当下的数据财产权化理论相近,即都承认数据的财产价值并愿意通过一定的规则来激励企业参与数据流动。因为只有让企业自身主动参加"比赛",才能用赛场规则促使其自主地发现问题、解决问题,才会形成根深蒂固的传统和责任意识。因此,我国应当强化元规制策略,在政府的指导性规范之下,鼓励行业或部门积极发挥自律作用,由市场解决其能够自我调节的问题。

3.实施适度的命令控制型规制,特定情况下选择强制义务模式。传统的规制属于命令控制型规制,由规制者制定规制规范,被规制者被动地遵守规范,既不参与规制规则的制定,对规制要求的执行也没有选择的余地,以制裁来实施规制,以实现企业行为与社会利益的一致。这种规制方式在个人数据规制领域仍有适用的余地。如前所述,以个人控制为核心的个人数据权利保护模式已经在大数据潮流面前发生变异,脱离个人控制的个人数据利用决定了事后惩处的侵权责任无法发挥作用。同样大数据的强渗透性和高发展性决定了在指导性规范与行业自律相结合模式下,若无强力加以保障,个人数据仍将处于高风险之中。因此,我国有必要在条件成熟时根据实际需求引入"隐私风险评估"。

---

① 参见周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018年第2期。

② See Cary Coglianese, Jennifer Nash, Management－Based Strategies: An Emerging Approach to Environmental Protection, Leveraging the Private Sector: Management－Based Strategies for Improving Environmental Performance, Routledge, 2006, pp. 3－30.

③ See Rachel L. Finn, David Wright, Privacy, Data Protection and Ethics for Civil Drone Practice: A Survey of Industry, Regulators and Civil Society Organizations, 32 Computer Law & Security Review, 580－586(2016).

④ See Mantelero A, The Privacy Impact Assessment in the EU Proposal of General Regulation on Data Protection, 1 Social Science Electronic Publishing, 145－153(2012).

隐私风险评估作为衡量隐私风险的有效工具，实践中已发展成为规范化操作流程，即只要满足特定条件，在数据处理会给自然人权利和自由带来风险时，数据管理者就应当对数据进行保护影响评估。①

4.积极参与国际合作。目前，美国和欧盟已基本完成了个人数据保护在国内或联盟内的立法进程，正在推广自身的数据跨境流动规则，抢占制定国际规则的主导权。由此可见，数据流动和传输并未仅限于国内，其国际间的流动同样值得关注。欧盟借助 GDPR 在其成员国的通过，已使该规则成为一项区域内的国际规则。美国则通过跨境隐私规则和自由贸易协定推广其数据跨国流动主张。当前我国正在倡导“一带一路”合作和区域全面经济伙伴关系协定战略，隐藏在其背后的是我国与其他国家公民个人的数据流动和交换。因此，如何在构建国内数据保护规则体系的同时，处理好内外数据保护体系的协调和对接是我国数据保护的又一重大议题。

五、结语

数字化时代的来临改变了社会的记忆、存储机制，变革了数据的流动方式，使得个人对自身数据的管控已经无能为力。事实上，我国个人数据的保护同西方国家一样也面临诸多困境。一方面，伴随着大数据与信息技术的发展，当前民法体系中的财产权和隐私权保护机制均难以应对现代数字社会中的新挑战，传统的侵权责任法无法适应当下纷繁复杂的社会风险。另一方面，过度依赖私法自治原则即所谓的“告知－选择”规则来保护个人数据，会给个人和企业带来难题。于个人而言，框架协议中的隐私政策专业性太强、个人识别能力有限、信息风险复杂等因素，使得个人难以对自身的权益做出精准判断。于企业而言，若要求个人信息的收集、使用都以明确授权为基础，那么社会中的数据流通将遭遇巨大阻碍。因此，为摆脱个人数据私法保护的困境，在借鉴国外有益经验的基础上，我国个人数据保护应当沿着私法救济和公法规制相结合道路稳步前行。为真正发挥私法保护个人数据的作用，国家有必要结合具体场景，将私法“消费者法化”，即个人以数据换取服务。个人数据保护的背景是现代信息社会中个体与企业等大型社会机构之间能力上的巨大差距，这与私法所强调的主体地位平等、意思自治等私法理念存在隔阂。在单一个体难以对企业进行监督对抗时，政府的介入将重新平衡天平的两端。因此，公法保护也应是我国个人数据保护的重要手段。保护个人数据的目的在于，除海量数据流蕴含的无限价值外，保障数据正常流动，避免给公民个人带来无法预见的风险。②

责任编辑　　翟中鞠

① 参见谢宗晓、董坤祥、甄杰：《隐私影响评估（PIA）的发展及 ISO/IEC29134：2017 实施探讨》，《中国质量与标准导报》2020 年第 3 期。

② 参见丁晓东：《个人信息私法保护的困境与出路》，《法学研究》2018 年第 6 期。