法商研究 Studies in Law and Business
Vol. 38 No. 6(2021)

个人数据权利刑法保护的立场选择及实现路径

李 凤 梅*

摘 要:个人数据权利不仅关涉公民的人格权和财产权,而且与国家安全、公共安全密切相关。基于数据个人私有而构建的个人控制论既存在逻辑偏差,也无法有效防控滥用数据权力(利)的风险。我国刑法应基于社会控制论的立场,注重数据的整体安全与动态保护,明确基于公共利益需要的个人数据利用原则及"以国家数据论"的个人数据的范围;引入以场景为导向的、动态的情境完整性理论,寻求数据权利与数据技术发展之间的平衡;以修改、解释刑法与增设附属刑法相结合的方式,明确数据跨境流动过程中所涉及的刑事责任问题,重择个人数据权利刑法保护的路径。

关键词:个人数据权利 刑法保护 个人控制论 社会控制论 情境完整性理论

随着物联网、云计算以及人工智能等新技术的出现,人类进入了大数据时代,数据成为国家的重要战略资源。在海量数据中,能够识别出特定自然人身份的数据被称为个人数据。① 基于对个人数据的占有、控制与使用而形成的个人数据权利不仅事关个人的利益得失,而且事关国家安全和公共安全。如何在明确保护立场的前提下,兼顾个人数据权利与国家数据权力以及数据技术发展之间的平衡,探讨、完善个人数据权利的保护路径就成为我国刑法回应社会关切的重要议题。

一、个人数据权利基本属性观点介评

由于数据权利的属性问题"不仅关系到公众个人隐私权的保护,也是明确数据收集、分析、运

* 沈阳师范大学法学院教授

基金项目:司法部国家法治与法学理论研究项目(18SFB2016)、辽宁省社科规划办项目(L18BFX002)

① 一般而言,欧盟的立法多采用"个人数据"的概念,美国的立法多采用"个人信息"的概念。我国的立法虽然采用了"个人信息"的概念,但是学界对"数据"与"信息"的理解存在差异,因而多根据研究需要交叉使用。有学者认为,"信息是数据的内容,数据是信息的形式"。程啸:《论大数据时代的个人权利》,《中国社会科学》2018 年第 3 期。数据关注的是原始性,旨在呈现客观事实,而信息多是处理后的数据,强调的是主体认知。本文除相关引文外,均采用"个人数据"的概念。

用主体行为边界的基础性命题”,[①]因此厘定数据权利的基本属性就成为明确数据权利刑法保护的立场选择、保护范围及救济路径的基础。

(一)个人数据权利基本属性的域外理论

数据权利与数据技术的发展程度密切相关,两者之间呈正相关关系。基于数据技术发展优势形成的美国隐私权理论与欧盟人格权理论,一直被认为是域外数据权利研究的基本理论,除此之外的其他理论,则被认为是上述两种理论的分支或延伸。

1. 隐私权理论。隐私权理论发轫于美国,是自由主义思想的产物。最初的隐私权理论持有者认为,人应当享有不被政府、媒体或其他机构、个人无正当理由干涉的独处权,有权决定自己的思想、观点和情感与他人分享的程度,以及在任何情况下“决定关于他的一切,是否公之于众的权利”。[②] 该理论曾被美国判例广泛接受,但由于“独处”的内涵过于模糊且缺乏可操作性而不断受到质疑,其中仅关于肯定个人对其具体事务具有决定权这一理论内核因切中隐私权实质而得以保留。[③]

隐私权的实质是政治或者宪政意义上个人自由在法律上的表述,其基本理念是对个人自由的坚守。[④] 自 20 世纪 60 年代以来,随着计算机技术的开发应用,个人数据海量出现,在数据流转的各个环节,这些数据都面临被泄露、盗用的风险。为了有效防范风险,认为“隐私权是个人、团体、机构决定关于自己的信息在何时、如何传递给其他人及传递到什么程度的权利”的个人信息控制论得以流行。[⑤] 1995 年,美国信息基础设施特别工作组进一步将个人隐私权定义为“个人对控制自身信息扩散范围的自决权”,[⑥]由此确立了个人信息控制论在个人数据隐私保护方面的理论地位。

2. 人格权理论。较之美国基于个人自由建立的隐私权理论,欧盟则基于人的尊严,认为个人数据权属于公民的人格保护权。1953 年《欧洲人权公约》第 8 条规定,尊重私人和家庭生活的权利。[⑦] 2000 年《欧盟基本人权宪章》第 8 条第 1 款将个人数据保护作为一项独立的基本权利加以规定。[⑧] 2012 年《个人数据自动化处理中的个人保护公约》的出台表明欧洲国家在将个人数据保护作为人权保护方面达成了基本共识。欧盟关于个人数据保护的立法受到欧洲各国的积极响应。德国联邦法院于 1983 年通过判决的方式首次确认了“个人数据自决权”,并由此推动欧洲其他国家将个人数据自决权作为一项基本人权的立法活动,如法国、葡萄牙、西班牙、比利时等国家,都分别在其宪法中将个人数据权作为一项基本权利予以确认。[⑨] 2018 年《欧盟一般数据保护

① 邓刚宏:《大数据权利属性的法律逻辑分析——兼论个人数据权的保护路径》,《江海学刊》2018 年第 6 期。

② See Warren S D. Brandeis L D, The Right to Privacy, Harvard Law Review, 5 (1980).

③ See Bok S, Secrets: On the Ethics of Concealment and Revelation, Vintage,1(1989).

④ 参见高富平:《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

⑤ See Westin A, Privacy and Freedom, Athenacum, 7(1967).

⑥ 参见屠振宇:《宪法隐私权研究》,法律出版社 2008 年版,第 68 页。

⑦ See European Convention on Human Rights, http://www.echr.coe.int/Dicuments/Cinvention_ENG.pdf, 2019-02-08.

⑧ 参见高富平:《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

⑨ 参见 [德]Christopher Kuner:《欧洲数据保护法——公司遵守与管制》,旷野、杨会水、李晓娴等译,法律出版社 2008 年版,第 20 页。

条例》在建立信息泄露通知机制、信息保护影响评价机制等个人数据保护机制的同时,新增了旨在强化公民个人信息控制权的被遗忘权的规定。①

综上所述,美国提倡的隐私权理论关注的是个人不愿意公开的各种私生活信息或者生活秘密,但对于不涉及隐私的个人信息,隐私权理论就难以涵摄。② 欧盟主张的人格权理论偏重于人格权的保护,但因其摒弃了数据的财产属性而难以很好地诠释数据权利的法律属性。③ 两者的共同之处在于,隐私权理论强调人的自由价值包含人格尊严和人格独立的内容,而人格权理论在强调人格尊严的同时也对人的自由给予肯定。另外,两种理论都基于个人控制论的视角,认为个人数据应当由数据主体掌控和支配,保障个人数据的自主、自治和自决。

(二)我国个人数据权利基本属性研究现状

我国关于数据权利属性的研究一直深受域外的影响,多从人格权或隐私权方面展开。2020 年 5 月 28 日通过的《中华人民共和国民法典》(以下简称《民法典》)将个人数据权利纳入“人格权”编,就表明了在私法领域立法者对个人数据权利属性的态度。然而,不可否认的是,随着国内数据技术的迅猛发展及因此而引发的社会结构的重大变革,数据权利已经被赋予更多的属性意义。将个人信息保护纳入人格权编与隐私权并列在一起,其实质是将一项新型公法权利简单归入传统民事权利范畴。这种错配既会使得个人信息保护在民事立法中定位困难、逻辑混乱,也会导致立法的各种反复与纠结,未来适用时将面临巨大的不确定性。④ 司法实践的经验表明,1997 年《中华人民共和国刑法》(以下简称《刑法》)第 253 条之一规定侵犯公民个人信息罪的目的从来就不仅仅限于保护公民的人格权,而更在于对因个人数据泄露可能受到侵害的个人财产权的保护。因为行为人侵犯他人的个人数据,其目的多表现为将数据非法提供给他人以获取经济利益,或者通过非法手段获取他人数据后,用于市场分析或者向数据主体定向推销商品或服务,甚至实施电信诈骗、敲诈勒索等行为。侵犯他人数据的行为并不必然会侵害他人的人格权,而往往意指他人的财产权,在非法获取他人数据的场合,这一特征表现得更为明显。所以,数据权利不应被局限于隐私权或人格权范围进行“是或否”的片面论证,而应当对其做多元化的分析与解读。

从现有的研究成果看,我国关于数据权利基本属性的定位,还包括“知识产权说”“商业秘密说”“数据财产权说”等多种学说,但都颇可质疑。“知识产权说”的缺陷在于,虽然应用了独创性加工方法的衍生数据具有知识产权保护的可能性,但缺乏独创性加工方法的衍生数据则很难达到知识产权保护的基本要求;⑤“商业秘密说”肯定了数据的隐私性,但数据权利作为个人的一项权利,其属性意义并非仅限于商业价值,同时也具有“人的权利”的侧面;“数据财产权说”赋予数

① 欧盟在“数据遗忘”的权利化道路上长期处于领先地位,引领着全球数据遗忘问题的探索进程。根据 2018 年《欧盟一般数据保护条例》第 17 条第 2 款的规定,如果数据控制者将符合该条第 1 款规定的个人数据(即用户依法撤回同意或者数据控制者不再有合理理由继续处理的数据)进行公开传播,那么其应该采取所有合理的方式予以删除。换言之,数据控制者不仅要删除自己所控制的数据,而且还必须就其公开传播的数据通知其他第三方停止利用并删除。参见孙道萃:《数据遗忘权的刑法学观察与协同保护》,《西部法学评论》2016 年第 4 期。

② 参见史卫民:《大数据时代个人信息保护的现实困境与路径选择》,《情报杂志》2013 年第 12 期。

③ 参见肖冬梅、文禹衡:《数据权谱系论纲》,《湘潭大学学报》(哲学社会科学版)2015 年第 6 期。

④ 参见周汉华:《个人信息保护的法律定位》,《法商研究》2020 年第 3 期。

⑤ 参见王融:《关于大数据交易核心法律问题——数据所有权的探讨》,《大数据》2015 年第 2 期。

据主体无偿占有其个人信息的权利，在逻辑上存在瑕疵，[①]无法解释为何国家拥有对特定个人数据的无偿占有与使用权。

基于对数据权利单一属性局限性的认识，学界也有人提出数据权利独立化的观点，认为数据权应当被认定为一种新型的民事权利。例如，有学者认为，厘清数据权属，有必要脱离我国学界主流以“财产权说”为逻辑起点的数据权属定位，克服其无法解决在数据采集过程中必须征得数据权利主体同意并因而导致大数据在社会治理应用中存在重大理论障碍的问题，直接将大数据权利定位为具有独立属性的数据权。这种新型的数据权应兼具财产权、人格权及国家主权于一体的混合属性。[②]

数据权利混合属性观点的提出表明，学界已从单一的隐私权、人格权等理论研究，发展到既关注其人格权属性又关注其财产权属性的混合属性研究，注意到在数据权利纠纷中人身权益与财产权益交织混杂的复杂形态。在关注数据权利个体属性的同时，也基于数据本身在大数据时代的特殊作用而对其公共属性予以特别关注，契合基于数据技术发展而引发的关于数据权利法律关系重大变革的时代要求。较之将数据权利属性界定为某单一传统属性的观点，这种基于数据技术发展客观情势而将数据权利抽象化为独立新型权利的观点不失其合理性和可行性，同时也为大数据背景下个人数据权利刑法保护的立场选择提供了全新的视角。

二、数据权利保护个人控制论及其检讨

如上所述，数据（信息）个人控制论肇始于美国，其最终目的在于实现公民对其个人数据的有效控制。我国关于数据权利保护是否采用基于私权视角的个人控制论立场，我国刑法未作明确的回应，但作为刑法前置法的相关法律法规则大都坚持基于“同意权”的个人控制论。例如，2017年施行的《中华人民共和国网络安全法》（以下简称《网络安全法》）第41条关于个人数据使用须经数据主体同意的规定；2013年修订的《中华人民共和国消费者权益保护法》（以下简称《消费者权益保护法》）第29条对作为数据主体的消费者的“同意权”的确认；《民法典》第1035条“处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：（1）征得该自然人或者其监护人同意……”以及2018年8月20日通过的《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》）第13条“符合下列情形之一的，个人信息处理者方可处理个人信息：（1）取得个人的同意；……”的规定等。这些立法规定暗合了域外关于数据个人控制论的保护精神，体现了立法者对于个人数据个人控制论的肯定和支持。然而，在大数据时代，基于个人控制的数据权利理论及立法是否真能对个人数据权利提供有效的保障，值得商榷。

1.个人控制论的立论基础值得质疑。个人控制论立基于权利的个人私有，认为数据权利是公民个人权利的一部分，其实质是个人自决权，具体包括对个人数据进行支配、控制并排除他人侵害等权利。[③] 由于个人数据本身具有一定的标识性，诸如基因、家庭住址、手机号码等更是具

① 参见邓刚宏：《大数据权利属性的法律逻辑分析——兼论个人数据权的保护路径》，《江海学刊》2018年第6期。

② 参见李爱君：《数据权利属性与法律特征》，《东方法学》2018年第3期。

③ 参见齐爱民：《论个人信息的法律保护》，《苏州大学学报》（哲学社会科学版）2005年第2期。

有直接的指向性,因此任何侵犯个人数据的行为都有可能危及公民的人身安全和财产安全。就此而言,个人控制论将数据作为个人私有、由个人支配的立论具有一定的合理性,但是如果认为“基于自己意思自主地决定个人信息能否被他人收集、储存并利用”就能充分实现数据确权,[①]那么该立论就值得怀疑。其理由是:(1)就规范逻辑而言,不同于传统的人身权、财产权等个人权利,数据权利是融合了外在技术因素的一种混合性权利。在大数据时代,个人只要参与社会活动,就会留下痕迹,形成个人数据,数据权利的边界因数据技术发展而处于不断扩张的态势中,要求个人对海量的数据进行实际控制,使数据权利成为排他性权利的个人控制论,既忽视大数据时代个人数据的动态性特征,又忽视个人数据权利与数据收集者、分析者、使用者之间的权利规范冲突,容易造成权利体系的混乱。(2)就制度功能而言,基于意思自治、主体平等等私权观念形成的个人控制论体系无法实现对受侵害的数据权利的有效救济。“无救济则无权利”,只有在受到侵害之后能够获得及时、充分的救济,权利才能成为真正法律意义上的权利。虽然基于个人控制论设计的数据权利保护体系确实能够在一定程度上实现对权利的积极控制,但是这种形式主义的保护模式并未充分注意到数据权力因技术优势而可能进行的、未经过或未及时经过数据主体同意的数据流向操控。在数据主体不可能对数据进行全链条追踪与全方位监控、甚至对数据已被采集的事实都无法知晓的情况下,权利救济也就成为空谈。那种认为“无论国家机关处理自然人的个人信息,还是非国家机关处理自然人的个人信息,也无论处理者处理自然人个人信息的目的是行政管理、公共服务还是营利目的,处理者与自然人都属于平等的民事主体”[②]的观点,忽视了个人与信息处理者之间明显不平衡的关系,[③]建立于该种理论基础之上的数据权利保护体系,自始即存在立论偏差。

2.数据的价值属性决定了个人控制论不具有完备性。大数据时代的数据具有重要的经济和战略价值已成共识。具体而言,前者表现为利用大数据获取经济收益,如通过分析数据实现对市场走向、消费趋势等的研判,以明确企业的发展方向与营销策略等;后者表现为国家在对内进行社会治理与对外享有数据主权方面的数据控制权和利用权。然而,并非所有的收集与使用数据行为都要经过数据主体的同意,在涉及公共利益及国家安全等场合,对个人数据的收集与使用就无需经过个人的同意,就此而言,个人控制论下的数据权利可能成为“纸面上的权利”。[④]

基于对数据价值属性的充分认知及对个人控制论的深刻反省,为个人控制论下的数据权利保护寻求变通性方案或者替代性思路,已日益受到重视。例如,有学者试图从行为主义与场景主义的立场出发,探求个人数据收集与使用行为的合理边界;[⑤]也有学者提出,应当强化公法意义上的数据权利,并以此作为对抗信息控制者侵害个人信息的前提性设定。[⑥] 上述观点或许能够解决数据企业基于数据经济利益而在数据收集与使用过程中与数据权利之间存在的冲突问题,而对于基于重大公共利益涉及的国家机构的数据收集与使用行为,则未必能提供合理的依据。就立法层面而言,无论是 1997 年《刑法》第 253 条之一还是其他前置法,都没有就国家未经个人

① 参见程啸:《论大数据时代的个人数据权利》,《中国社会科学》2018 年第 3 期。

② 程啸:《我国〈民法典〉个人信息保护制度的创新与发展》,《财经法学》2020 年第 4 期。

③ 参见王锡锌:《个人信息国家保护义务及展开》,《中国法学》2021 年第 1 期。

④ 参见张新宝:《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。

⑤ 参见丁晓东:《个人信息的双重属性与行为主义规制》,《法学家》2020 年第 1 期。

⑥ 参见周汉华:《个人信息保护的法律定位》,《法商研究》2020 年第 3 期。

同意而获得或者使用个人数据的行为作出入罪的规定，个人控制论明显存在立论上的缺陷。

3.作为个人控制论核心的同意原则并不必然具有客观合理性。(1)“同意”本身的真实性值得商榷。在实践中，数据企业为了合法取得对用户数据的收集权和使用权，往往会在服务终端页面设置“同意”条款，用户只有在确定“同意”后方可获得服务。然而，基于参与网络生活的必要性及享受网络产品和服务的便捷性考虑，数据主体往往并不真正具有作出同意决定的自由，也并非实质性地认同用户协议、服务条款及隐私权政策规定的内容。另外，受自身专业知识的限制，大多数数据主体往往会受限于“获得性启发”[①]而忽略“同意”后的风险。在很多情况下，数据主体甚至在根本没有对“同意”的内容进行阅读的情况下就进行了确认。部分数据企业为了规避责任而有意设置具有倾向性模糊条款的做法，也使得同意的真实性大打折扣。(2)同意原则本身存在逻辑方面的缺陷。根据同意原则，数据主体有权决定个人数据能否被他人使用以及如何使用，但这种理论设定不可避免地带有理想主义的色彩。其原因在于，既然数据主体有权决定让他人使用其数据，那么当然也就有权决定不让他人使用其数据或者删除已使用的数据，即享有删除权。但删除权的行使是建立在数据主体有证据证明他人不是或者不再是使用自己数据的适格主体的基础上，尤其是在面对处于优势技术地位的互联网企业时，数据主体更会因举证困难而难以有效行使删除权。另外，在面对国家机构的数据使用问题时，数据主体会面临无权行使删除权的问题，如无权要求金融机构删除其不良信用记录、无权要求司法部门删除其犯罪记录等。(3)同意原则并未获得立法层面的经验性认同。作为个人数据控制权起源地的美国，目前并未以立法的方式对数据主体的“同意权”进行确认；欧盟也仅将“同意”作为个人数据收集的合法性基础之一，而并非使用个人数据的必要条件；我国《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》(以下简称《规定》)，对网络用户或者网络服务提供者未经数据主体同意公开其个人数据并造成损害情况下的侵权责任的规定，[②]以及2020年10月1日实施的《信息安全技术　个人信息安全规范》(GB/T35273—2020)对同意原则例外情形的规定，都表明立法者对个人控制论下的同意原则持谨慎的态度。[③] 基于法统一性原理及刑法的“二次法”特征，行为人的行为在不构成民事侵权的情况下，刑法当然也不得认定其为犯罪。[④] 立法是公民权利得以实现的保障，任何立法犹豫或者立法限定都表明，立法者在将立法原理或者立法精神内化为实在的法条规范的过程中，对隐藏其后的法学理论持一种有限接受的态度。也正是认识到个人不可能通过“同意”的方式对其数据进行控制与支配，立法者最终选择了留有余地的立法方式，

① “获得性启发”也称“可行性启发”，由美国学者丹尼尔·卡尼曼提出，是指人们在形成判断的过程中，往往会根据常见的例子或证据作出经验性判断，而对其他必须考虑的信息则选择性地“视而不见”。See Amos Tversky & Daniel Kahneman, Availability: A Heuristic for Judging Frequency and Probability, 5 Cognitive Psychology, 208 (1973).

② 参见2014年6月通过的《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。

③ 参见2020年10月1日实施的《信息安全技术　个人信息安全规范》第5.6条。

④ 需要说明的是，虽然《中华人民共和国消费者权益保护法》及《中华人民共和国网络安全法》规定了同意原则，其规定也具有较之《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》而言具有更高的法律效力，但《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条关于在对数据主体不构成侵害的前提下容许数据权力优先于数据权利的立法态度，则表明司法机关在“同意原则”的适用问题上所持的谨慎存疑及务实的态度。

或者暂缓立法以维护法律的稳定性和权威性。(4)同意原则的实现面临数据技术发展带来的挑战。个人控制论下的同意原则是在传统历史条件下进行的理论创制,前大数据时代不仅不具有大规模采集数据的能力,而且缺少通过大数据分析获得目的性收益的可能。随着海量数据的产生,注重数据分析与利用已成为产业通例,且基于数据的可重复利用性,数据价值更多地体现在二次利用即对数据的深入挖掘和处理过程中,不仅如此,处理目的也可能在二次利用中发生改变。① 虽然欧盟、美国以及我国等相关国家和组织均在法律中设立了“目的限制原则”,试图通过严格禁止非约定目的的数据使用来防止数据被滥用,但是适用情况并不理想。如果遵从同意原则的要求,那么数据企业必须在二次利用数据之前取得数据主体的同意,而这显然面临因二次利用模式的多元性及可能的多重流转性所导致的、在追溯原数据主体时的现实困境,而要求数据主体在不仅没有任何收益而且可能会因此给自己的人身或者财产造成损害的情况下同意数据企业的二次使用要求,也不具有操作层面的可行性。

三、数据权利保护社会控制论立场之提倡与证立

社会控制理论为美国社会心理学家 E.A. 罗斯所构建。罗斯在《社会控制》一书中指出,社会控制“是一种社会行为,即社会通过各种手段,运用各种方式,使个人和团体的行为能有效地遵从社会规范,以达到维持社会秩序、保障社会整体协调、促进社会正常发展之目的”,②并详细阐释了包括法律在内的 10 多种控制工具的运行机理。时至今日,社会控制论已成为社会科学领域的显学之一,为日益匿名化、陌生化的社会提供了相对稳定、权威的行为规范。提倡个人数据的社会控制,更有利于个人数据保护目标的实现。因为面对数据平台和国家机关所拥有的强大“数据权力”,个人控制论下的数据权利保护模式很难为个人信息提供充分、全面和有效的保护。③

(一)个人数据的公共属性决定了数据权利保护的社会性

个人数据依其来源不同可分为自然性数据与社会性数据两种。④ 前者指基于自然出生而形成的、不可更改的数据,如指纹、血型、基因等;后者则指基于社会交往及相应活动而产生的数据,如姓名、电子信箱、电话号码、行动轨迹等。在互联网出现之前,虽然社会性个人数据具有一定的公共属性,但是自然性个人数据则具有天然的私权属性。自进入大数据时代以来,全息化、海量化的个人数据在维护国家安全与社会发展过程中的作用日益凸显,包括自然性个人数据在内的数据的公共价值逐渐受到重视,为实现数据权利社会保护的目标提供了可能。

1.个人数据与国家安全的密切相关性决定了对个人数据动用国家公权力进行保护的必要性。如果以数据主体身份和数据内容的敏感程度为标准进行分类,那么个人数据可以分为涉密人员敏感数据、涉密人员一般数据、非涉密人员敏感数据与非涉密人员一般数据 4 种类型,⑤其中前 3 种类型的数据直接关涉国家安全,需要动用国家公权力进行保护。其理由如下:(1)涉密

① 参见任龙龙:《论同意不是个人信息处理的正当性基础》,《政治与法律》2016 年第 1 期。

② 转引自吴刚、张敏杰:《转型时期的社会控制论纲》,《浙江社会科学》1994 年第 6 期。

③ 参见王锡锌:《个人信息国家保护义务及展开》,《中国法学》2021 年第 1 期。

④ 参见刘迎霜:《大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角》,《社会科学》2019 年第 3 期。

⑤ 参见姚斌:《总体国家安全观视角下个人信息保护机制研究》,《保密科学技术》2019 年第 8 期。

人员的个人敏感信息如一国领导人的健康信息、行动轨迹等可能成为国家的秘密数据而需要进行特别保护，在国家面临政治动荡、国家间发生战争等情况下，更是如此；(2)涉密人员的一般个人数据也可能直接威胁到国家安全，而通过对涉密人员一般数据进行分析，定位其所用互联网电脑并进而发动针对国家安全的网络攻击在近年来也屡见不鲜；(3)非涉密人员的敏感数据也与国家安全的相关性越来越高，如海量非涉密人员的基因数据会影响到国家的生物安全，在政治事件中网络用户评论区域的数据可能被用来作为倾向性地投放诱导性新闻以引导事件的政治走向等。[①] 没有国家权力，公民权利就难以得到有效的保障，[②]在作为公民数据权利客体的个人数据同时兼为国家数据时，这一特点表现得尤为突出。基于国家立场对数据权利进行体系性的社会化保护，是国家数据安全的应有之义，也是个人数据权利实现的有效保障。

2.个人数据已成为公共资源的一部分，需要提供多元化的社会保护。数据技术的发展不仅给数据主体带来享受高品质服务、快速迭代创新等各种便利，[③]而且使得数据成为信息控制者的生产要素和行动指引，[④]直接与公共生活相关。具体而言：(1)在引发社会安全忧虑的群体性事件以及各种刑事、暴恐事件中，对个人数据的掌控和使用可能直接影响舆论及控制事件的走向；(2)随着互联网经济的发展，通过网络购物已成为常态，对海量个人消费数据进行分析的结果可以成为制定经济政策的重要参考指标，甚至会改变相关领域的经济格局；(3)数据已成为深入分析各类群体社会活动乃至个体活动的重要指标，在公共政策制定、疫情防控、社会保障与维稳等领域的作用不可替代。个人数据在公共事务中的立体化嵌入已成为大数据时代的常态特征，保护个人数据已成为全社会的共同责任，需要与之相关的国家机构以及其他数据控制者、使用者共同协作，形成多元化、多层阶的社会保护体系。

(二)社会基础的改变为个人数据社会控制论提供了现实支撑

在前互联网时代，个人数据无论是由数据主体提供给政府、企业或者他人，还是由对方主动收集，其种类、流通范围和流通渠道都相对受限，数据主体可以通过同意数据被收集或使用、要求更正或删除等方式，要求数据占有者按照预定的方式和用途占有、使用数据，数据被滥用的风险相对可控，因而“在大数据时代来临之前，个人数据实际处于未被利用的沉睡状态”。[⑤] 随着信息技术的发展，数据成为知识，[⑥]数据需求呈几何级数增长。而日益严密的监控系统、人脸识别系统则较好地满足了社会对数据的需求，并因此形成庞大的动态数据库，由个人提供的诸如姓名、性别、联系方式等基础数据只占据其中的一小部分，新技术的出现彻底改变了前互联网时代数据各方基于信用而建立起来的规则体系，数据被滥用的风险陡增。与此同时，数据本身具有的随时

① 参见胡雅萍、洪方：《社交媒体情报研究》，《情报杂志》2018年第3期。

② 参见张晓琴：《论国家权力对公民权利的保障》，《宁夏大学学报》(人文社会科学版)2009年第2期。

③ See D.Daniel Sokol & Roisin E.Cimerford, Antitrust and Regulating Big Data, 23 George Mason Law Review, 119(2016).

④ 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。

⑤ 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。

⑥ See Martin Hilbert, Big Data for Development: A Review of Promises and Challenges, 34 Development Policy Review, 139(2016).

产生、多点存储、多次开发、跨场景应用、多人经手、收集与处理分离等特点,[①]也使得个人数据自产生时起即进入大数据系统并呈现与数据主体加速脱离的趋势,数据主体据以控制其个人数据的客观基础被不断削弱,对数据的控制愈来愈体现出强烈的社会化倾向。

在持社会控制论者看来,对具有异质性的社会结构进行不同的功能控制,是社会有序发展的客观要求。[②] 个人数据的有序流通与使用是大数据时代数据资源利用的重要保障,任何有损数据效能发挥的行为都有悖社会发展的客观要求,除了其他个人对数据主体权利可能造成侵害外,个人数据权利与企业数据权利之间也存在此消彼长的冲突。要避免数据权利免受侵害,就必须发挥法律法规、行业规则等手段的不同社会控制功能,对偏离和违背规范、具有社会异质性的犯罪行为及越轨行为等进行防范、纠正与惩罚。[③] 需要说明的是,法律作为一种高度专业化的社会控制形式与主要手段,[④]理当成为满足社会结构调整与变革控制需求的理想选择。

(三)坚持社会控制论有利于实现数据权利与数据权力之间的平衡

"在检讨域外个人信息保护的法律文件时,我们发现几乎所有的国际性和国家性法律文件均将个人信息流动或流通使用作为最终的目标。"[⑤] 数据流动的最终目的就是希望通过数据利用来实现数据效益,而数据企业与国家在利用数据过程中难免会对个人数据权利的实现构成威胁:(1)数据产业的发展离不开数据流通,单纯强调数据保护将因阻碍企业数据权利的行使而限制数据产业的发展,而数据产业的发展受阻会反噬数据保护的能力;(2)对数据权利保护过度会导致国家数据权力受限,甚至有可能导致国家数据安全面临风险,而一旦国家数据安全面临风险,那么个人数据权利的保护也就成为空谈。

坚持社会控制论的理由在于,个人数据权利要求的数据保护与数据利用所需要的数据共享之间的冲突能够得以缓解:(1)社会控制论不仅关注个人数据权利的实现,而且强调数据的社会价值,提倡在数据流动过程中个人权利保护与数据有效利用的相对均衡。"忽略个人数据的社会价值"被认为是美国个人数据保护模式存在的严重缺陷,[⑥]而在设计个人数据保护制度时应当充分关注各方利益之均衡,[⑦]则被认为是数据经济的重要内涵。基于社会控制论建立起来的数据权利保护体系,不再局限于单纯的个人数据保护,而是着眼于社会经济发展与个人权利保护的相对均衡,以动态保护为出发点,对数据权利的保护范围及保护限度作出适时调整,建立包括法律保护在内的数据权利社会保护体系,避免因对个人数据保护过度而可能导致的数据产业发展不彰,以及因此可能引发的对数据权利保护的反噬。(2)社会控制论有利于企业数据收集与利用的规范化。在数据流动的整个生命周期,数据主体并不能有效控制数据的流向和用途,即便是在个

① See Martin Hilbert, Big Data for Development: A Review of Promises and Challenges, 34 Development Policy Review, 139(2016).

② 参见何怀远、田佑中:《社会哲学视野中的社会控制——兼就"社会系统的自在控制"问题与杨桂华先生商榷》,《哲学研究》2000 年第 1 期。

③ 参见蒋传光:《论社会控制与和谐社会的构建》,《江海学刊》2006 年第 4 期。

④ 参见[美]罗斯科·庞德:《通过法律的社会控制 法律的任务》,沈宗灵、董世忠译,商务印书馆 1984 年版,第 12 页。

⑤ 高富平:《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

⑥ See Sdhwartz P.M, An Economic Theory of Clubs, 32 Economica, 125(1965).

⑦ 参见张新宝:《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。

人数据与特定服务或交易联系在一起时，也未必能有效保护数据不被滥用。社会控制论的优势在于，数据自产生时起即一直处于严密的规则体系之下。这种全方位的控制论体系使得任何僭越既有规则而滥用数据或者侵犯数据权利的行为，都能够受到自上而下的即时监督，明确国家机关、企业及网络主体等数据采集者、使用者及监督者的主体责任，确保企业数据利用的合法性。(3)社会控制论能够有效避免建立在自决权基础上的个人控制论与国家数据利益之间产生的矛盾。国家数据利益与个人数据权利之间的矛盾主要表现为，国家基于安全与发展需要而采用包括定位跟踪、监视监控等在内的各种方式收集、使用个人数据，压缩数据权利空间。但是，在国际数据技术竞争日益白热化的当下，国家数据利益是维护域内包括个人数据在内的数据安全的根本保障，因而要“在一个矛盾统一体中求得一种动态的平衡，以实现国家管理的效率”，[①]就必须充分运用国家的资源配置能力，在对各种社会要素进行充分评估的基础上，明确国家数据利益与个人数据权利之间的基本界限以及当两者发生冲突时后者的让渡规则，建立基于社会利益整体化考虑的体系性保障。

四、社会控制论视阈下我国数据权利刑法保护立法检讨

(一)我国数据权利刑法保护立法之现状

就广义而言，我国对个人数据权利的刑法保护可分为3个层面：(1)前置性法律法规，包括《个人信息保护法》《关于加强网络信息保护的决定》《消费者权益保护法》《规定》以及《民法典》等。这些法律法规都对个人信息(数据)保护作出了规定，为个人数据的刑法保护提供了前提性的法律根据。(2)附属刑法立法，如《网络安全法》第74条第2款“违反本法规定，……构成犯罪的，依法追究刑事责任”的规定，首次以附属刑法的方式明确了网络运营者、网络安全监督管理部门、其他组织及个人侵犯公民个人数据的刑事责任。(3)刑法关于个人数据保护的规定，主要体现在以下几个方面：1)直接侵犯个人数据权利类犯罪。这包括1997年《刑法》第252条规定的侵犯通信自由罪，第253条规定的私自开拆、隐匿、毁弃邮件、电报罪，第253条之一规定的侵犯公民个人信息罪。上述条款的规制对象都直接指向或者涉及个人信息(数据)。然而，随着传统通信方式的日渐式微，信件的使用率已大幅下降，电报也逐渐被互联网以及手机短讯所取代，在民用领域基本处于停滞状态。以邮件和电报作为规制对象的侵犯通信自由罪和私自开拆、隐匿、毁弃邮件、电报罪的适用范围随之变窄，对个人数据的保护效用也大为降低。[②] 2)间接侵犯个人数据权利类犯罪。这主要是指1997年《刑法》第286条之一规定的拒不履行信息网络安全管理义务罪。根据该条的规定，网络服务提供者虽然未直接侵犯个人数据，但是如果拒不履行法律法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使违法信息大量传播、用户信息泄露造成严重后果，以及具有其他严重情节的，处3年以下有期徒刑、拘役或者管制，并处或者单处罚金。3)基于国家数据立场形成的对个人数据的宏观层面的保护。出于对个

① 李文汇：《公民权利与国家权力关系之法理分析》，《社会主义研究》2000年第3期。

② 需要说明的是，随着电子商务的发展，邮件的业务量虽然规模较大且呈递增趋势，但是以包裹类为主，因而所涉罪名多为职务侵占罪或者盗窃罪，侵犯通信自由罪和私自开拆、隐匿、毁弃邮件、电报罪仅适用于邮件中所占比例较小的信件、文件等。

人数据公共性、社会性的考虑,在个人数据可能涉及国家安全的情况下,我国刑法关于国家数据保护的规定,也适用于对个人数据的保护,相关条款主要包括:1997 年《刑法》第 111 条规定的为境外窃取、刺探、收买、非法提供国家秘密、情报罪,第 219 条之一规定的为境外窃取、刺探、收买、非法提供商业秘密罪,[①]第 282 条规定的非法获取国家秘密罪、非法持有国家绝密、机密文件、资料罪,第 398 条规定的故意或者过失泄露国家秘密罪,第 308 条之一规定的泄露不应公开的案件信息罪、披露、报道不应公开的案件信息罪。[②]

(二)我国现行数据权利刑法保护立法检讨

虽然基于附属刑法规范及刑法的相关规定形成的个人数据权利保护体系,同时实现了对网络经营者等数据占有者的行为限制以及对其他单位、个人侵犯数据权利行为的刑事规制,从立法上实现了对个人数据权利的多方面保护,但是我国现行立法仍存在结构性缺陷,而导致存在这些缺陷的主要原因在于缺乏进行整体社会保护的立法意识。

1.侧重对个人数据的保护,忽视对国家数据安全的深层保护。有研究成果表明,无论是相关附属刑法规范还是刑法,都未以列举规定或者概括规定的方式明确国家数据的范围,未对作为国家数据的个人数据的类型、特征或者规模等做任何描述,导致对作为“国家秘密”须予刑法保护的个人数据的范围无从确定。这一立法缺陷导致国家权力机关在基于国家安全或者社会治理需要而使用包括关键数据、敏感数据在内的个人数据时,面临如何保障公民数据权利不被国家数据权力侵犯、如何维护刑法保护机能与保障机能之间平衡等抉择困难,从而使 1997 年《刑法》第 111 条、第 219 条之一、第 282 条、第 308 条及第 398 条之一等条款的规定形同虚设。

2.关注个人数据的境内保护,缺少对数据跨境流动中的个人权利保护。在互联网时代,个人数据几乎能够实现零成本的跨境流动,从而对主权国家基于本国国家利益或者国民利益而必然拥有的数据管辖权构成威胁。无论是美国主导的《跨太平洋伙伴关系协定》《澄清域外合法使用数据法》,还是欧盟的《安全港协议》《隐私盾协议》以及《通用数据保护条例》,都将个人数据保护作为处理国际政治与经济关系的重要内容。大数据时代的数据资源已成为重要的战略资源,我国必须注重国际背景,为刑法保护管辖权的行使提供国内法支持,但就目前的立法现状而言,我国刑法显然缺乏应对大数据时代数据管辖权行使的规范供给。

3.重视对个人数据的静态权利保护,未兼顾数据技术的动态发展需求。数据共享是数据技术发展的前提之一,而数据共享意味着数据主体必须允许数据企业根据数据技术的发展需要分析、使用数据,并适时调整数据的使用范围,以实现动态数据技术发展对数据使用的需求与数据权利保障之间的平衡。遗憾的是,我国刑法对这一问题并未给予足够的重视,刑法和相关附属刑法都未基于数据应用环境、数据的敏感程度以及数据权利让渡的限度等方面的考量,对数据流通过程中的权利保护程度作出分级规定。这就要求立法者在转变立法理念的同时,基于社会整体控制的思维,根据数据技术发展与国家数据战略的需要,在兼顾企业数据权利的情况下,重构个人数据权利保护的立法体系。

---

① 在涉国家安全的个人数据保护的场合,该罪名的适用需要具备两个条件:(1)作为行为客体的商业秘密本身是采取了保密措施的个人数据,而非技术数据或者其他经营数据等;(2)为境外窃取、刺探、收买、非法提供该商业秘密的行为不仅损害了相关企业的经济利益,而且严重危害了国家的经济安全。

② 参见唐稷尧:《大数据时代中国刑法对企业数据权的保护与规制论纲》,《山东警察学院学报》2019 年第 3 期。

此外，当前的立法也存在规制不全等问题。例如，对于匿名化个人信息，《网络安全法》第42条规定：“网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外”。根据该条的规定，个人数据中的人格属性被剥离后，企业即享有自由处理与转移数据的权利。然而，已被匿名化后的个人数据，完全可能通过与其他社交媒体的资料比对，还原为具体的数据主体的数据，匿名已经成为一个“破碎的隐私承诺”。[①]《网络安全法》第42条的规定只对匿名化后的纯数字化信息作出了规定，但对这些数据的可能复原却未作出进一步的规定。刑法作为事后法，在前置法未予规定的情况下，如何对精准复原后的个人数据进行保护，以及能否适用侵犯公民个人信息罪对该行为进行规制等都值得研究。

五、社会控制论视阈下我国个人数据权利刑法保护路径重择

构建社会控制论视阈下我国个人数据权利的刑法保护体系，必须在讲求刑法规范完整与体系结构合理的基础上，基于体系的、动态的社会视角，着力于具有针对性的规范构建。

（一）关注数据整体安全，防止进行片面强调个人数据权利保护的单向立法

长期以来，我国在个人数据权利保护方面的研究，基本都遵循基于私权视角寻求相应法律对策的思路。这种单一的定向化研究，形成个人数据权利应当优于其他数据权利或数据权力的表象，以致有损刑法社会保护功能的发挥。为此，我国刑法立法应基于社会控制论的立场，重构个人数据权利保护体系。

1.明确我国刑法保护的“个人数据”的范围。关于何为个人数据，我国刑法及其他刑法规范并未作出规定，因而对1997年《刑法》第253条之一关于侵犯公民个人信息罪中犯罪对象的界定，只能借鉴其他前置性法律法规的规定。根据《民法典》第1034条的规定，个人信息“是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”。另外，《信息安全技术　个人信息安全规范》第3条第1款对个人信息的界定与《民法典》第1034条的规定基本一致，并在附录A中对个人信息的判定方法与类型作出了规定，进一步补全了我国民法典关于个人信息的规定。然而，对前置法规范与刑法规范之间关系的考察表明，两者之间具有属种关系，前置法未予认可的必然会为刑法所否定，但前置法所保护的则未必会得到刑法的保护。上述法律法规关于个人信息的规定，可以为我国刑法惩处侵犯个人数据的犯罪提供基础概念的借鉴，但究竟哪些个人数据能够成为我国刑法保护的对象，仍应基于相关前置性法律法规关于个人数据的规定，在对数据种类、规模及可能的危害程度等进行类型化预估的前提下予以明确。

笔者认为，对个人数据的界定应考虑以下几个方面的内容：(1)刑法是强权法，其威慑力既源于对财产、自由乃至生命的剥夺，也源于因稳定性而带来的对法效果的可预测性以及其在民众心中所形成的权威感。考虑到附属刑法具有较强的专业性及对客观需求的适应性，立法者应尽可

① See Ohm P., Broken Promises of Privacy: Responding to Surprising Failure of Anonymization. 57 University of California Los Argeles Law Review, 1701(2010).

能采用附属刑法的方式明确个人数据的保护范围,以避免对我国刑法的频繁修正。(2)充分考虑新技术发展可能引发的个人数据范围扩大等因素,在立法中应避免采用单一列举式的立法模式,可借鉴我国民法典关于个人信息(数据)的规定,采用“列举+概括”式的立法模式。为了给立法解释与司法认定提供更为明确的指引,可以对个人数据采用类型化描述的方式加以规定,以便准确指示列举式规定中的数据特征,并据此对概括性规定部分进行合目的性解释。(3)个人数据除了敏感数据及关键数据以外,一般的单个数据价值相对有限,但在大数据背景下,规模化的个人一般数据具有重要的经济价值与安全价值,直接关涉数据主体的人身、财产利益乃至公共安全,因而立法者既要考虑在特定情况下单项数据的价值,又要考虑数据的综合价值,以明确刑法的保护范围。

2.明确“以国家数据论”的个人数据范围。刑法拟制是刑法立法基于立法目的性及便宜性考虑而采用的一种立法技术,“旨在赋予虚构事实与类型化的原事实以相同的法律效果,以契合刑事政策之需或弥补立法技术之力所不及”。① 个人作为群体的一部分,其数据在一定程度上也是个人在群体生活中的反映,通过对个人数据的分析与运用,往往能够得出一定时期内相应群体的活动状态乃至国家的相关政策走向,而这直接关系到国家的安全。我国刑法应当采用立法拟制的方式,将可能影响国家安全的个人数据拟制为国家数据,并明确“以国家数据论”的个人数据的范围,以实现对重要个人数据进行特殊保护的目的。这类数据具体包括:特定人员(尤其是涉密人员)的特定数据的认定范围,刑法拟保护的特定人员的一般数据的范围及适用条件,一般个人的敏感性数据,可能影响国家安全的规模性个人数据的认定条件等。与此同时,我国立法应当明确规定,对侵犯上述数据的行为,适用 1997 年《刑法》第 111 条、第 282 条、第 308 条以及第 398 条之一的相关规定,以侵犯国家安全的犯罪论处。

3.明确基于社会公共利益需要的数据利用原则。公共利益是公民普遍享有的基础利益,是发生冲突的利益之间进行比较的结果。② 虽然与个人利益相互依存、相互促进,但是公共利益的实现往往以个人利益的减损为代价,两者之间存在对立统一的关系。在解决公共利益与个人利益的冲突中,单纯的个人主义或者社群主义都不利于社会的健康发展,权衡受保护法益的增益程度与受损害法益的减损程度的比例原则被认为具有相对合理性。③ 刑法在保护个人数据的同时,要兼顾数据公共利益的实现,就必须权衡个人数据权利与公共利益之间的关系,着重注意以下几个方面的问题:(1)在涉及重大公共利益的场合,应当基于公共利益豁免原则,允许实施基于合法目的的个人数据利用行为,对任何阻碍个人数据利用或者通过虚构、篡改等方式改变个人数据分析结果或者用途的行为,应当追究刑事责任,并根据违法行为的严重程度规定相应的罚则。(2)对于基于一般公共利益目的需要使用个人数据的情形,我国刑法应当在充分尊重个人数据权利的前提下,合理界定犯罪的范围。根据比例原则,如果个人数据的利用将严重损害数据主体的利益,那么只有在因阻碍个人数据利用造成公共利益受到严重损失的情况下,才能考虑适用刑罚处罚。(3)在关于个人数据权利与公共利益的法益衡量中,对数据权利法益的衡量应着眼于数据的敏感程度、数据规模、数据性质等方面,预估其价值效益以及基于公共利益进行权利让渡后可

① 李凤梅:《刑法立法拟制研究》,《北京师范大学学报》(社会科学版)2013 年第 4 期。

② 参见刘太刚:《公共利益法治论——基于需求溢出理论的分析》,《法学家》2011 年第 6 期。

③ 参见[德]拉伦茨:《法学方法论》,陈爱娥译,台湾五南图书出版有限公司 1997 年版,第 319~320 页。

能产生的损失。对公共利益的衡量应关注其可能产生的经济价值、社会价值、受众区域、范围，以及受众成分等因素，综合评估因个人数据利用受阻可能产生的损失。

（二）兼顾数据技术发展需要，寻求个人数据权利与企业数据权利之间的平衡保护

防止企业数据权利对公民个人数据权利造成损害，既是个人数据权利保护的核心内容，也是刑事立法必须关注的重要课题。在数据权利保护中引入以场景为导向的、动态的情境完整性理论，已成为近年来学界探讨个人数据权利有效保护的新路径。该理论基于动态的分析系统而成，将数据置于交换时的情境之中，以参与人、数据类型与传输原则为参数，对数据应用进行是否具有“适当性”的判断。①

根据情境完整性理论，数据的收集人、传输者等参与主体只要基于特定情境对数据进行合规范化处理，其行为就是适当的。例如，数据企业基于技术发展目的而对相关数据进行分类收集、国家行政机关基于社会管理需要对个人数据进行收集等，都是基于特定情境的适当行为。数据的流通过程既要受流通规范的限制，也要流向特定的对象，不能超越情境限制。根据美国学者海伦·尼斯堡的观点，这里所谓的情境是指数据在流通过程中的社会情境，②是基于一般人判断的社会法则。数据企业向关联企业提供数据以进行商业情势分析，只要数据脱敏且被用于特定的目的，就是适当的；该关联企业如果将所获得的数据扩散，那么就超越了社会一般人的认识，即超越了特定情境，就存在侵犯个人数据权利的风险，因而不具有适当性。

情境完整性理论的核心在于其是基于动态的判断系统而构建的，破除了传统理论在关于是否侵犯个人数据权利时的静态认定标准，合理兼顾了企业数据权利与个人数据权利之间的平衡而具有相当的合理性。对于追求稳定性、可预测性及抽象化的刑法立法而言，要有效解决现行立法在个人数据权利保护过程中可能涉及的侵权问题，情境完整性理论不失为一种可以借鉴的理论。司法机关在认定数据企业是否侵犯个人数据权利的过程中，基于系统的社会论原理，从数据流通过程中的参与人、流通数据的类型及保护限度、流通原则及流通对象限定等方面，就企业数据权利与个人数据权利的动态平衡进行社会情境的一般性判断，在企业数据权利是否构成侵害个人数据权利犯罪的认定过程中，既关注个人数据权利的正当性和保护的重要性，也赋予数据企业一定的权利空间，防止因过度强调个人数据权利保护而阻碍数据技术的发展，尤其是对于数据企业基于国家安全、公共安全等需要而形成的针对个人数据的侵害行为，我国刑法应基于社会治理的观念予以从宽处理。

（三）完善附属刑法立法，明确跨境数据流动过程中的相关刑事责任

随着全球经贸交易、技术交流、资源共享等跨国合作的日益频繁，包括个人数据在内的数据流动规模不断扩大，数据跨境流动成为国际社会普遍关注的问题。因此，包括美国、欧盟在内的多个国家和地区都在积极制定数据跨境流动规则，《网络安全法》第37条也对数据跨境流动作出了规定，要求关键信息基础设施的运营者因业务需要，确需向境外提供个人信息和重要数据的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。作为对该条法律规定的回应，《网络安全法》第66条规定，对于关键信息基础设施运营者违反该法第37条之规定，在境

① 参见倪蕴帷：《隐私权在美国法中的理论演进与概念重构——基于情境脉络完整性理论的分析及其对中国法的启示》，《政治与法律》2019年第10期。

② See Helen Nissenbaum, Privacy as Contextual Integrity, 79 Washington Law Review, 119－157(2004).

外存储网络数据或者向境外提供网络数据的,分别规定了针对企业及相关责任人员的责令改正、给予警告、没收违法所得等行政处罚及行政处分。

通过对《网络安全法》第 66 条规定的解读不难得出如下结论:对于实施违反该法第 37 条规定的行为,无论其情节及后果如何,都只涉及行政法层面的处罚。这实际上是直接否定了对实施违反该法第 37 条规定的行为适用刑罚的可能性。在数据被作为国家重要战略资源的当下,这一规定无疑是值得商榷的。另外,对于作为非关键信息的一般信息基础设施的运营者、网络服务商以及跨国企业等在生产经营中确需向境外提供个人数据的,相关个人数据的种类、范围及程序规则等,我国网络安全法均未作出规定,对由此可能引发的不利后果自然也缺乏相应的法律救济手段。

刑罚权的发动必须以所处罚的行为违反前置法为前提。我国网络安全法的相关规定,既未对实施关键数据违法跨境流动行为情节严重或者结果严重情况下的刑事责任作出规定,也未对实施一般数据违法跨境流动行为可能引发实质性刑事责任的情况作出类型化的规定。因此,一方面,包括我国网络安全法在内的相关前置性法律规范应当充分认识到跨境数据流动的重要性及其可能导致的国家安全、社会安全以及个人数据安全问题,在对可能引发数据安全的类型化行为作出尽可能详细规定的情况下,也要完善责任体系,在对相关行为的民事责任、行政责任予以明确的基础上,以附属刑法的形式对其刑事责任作出规定。另一方面,我国刑法应当与附属刑法相衔接,从以下两个方面入手完善应对体系:(1)立基于我国现行刑法的规定,根据跨境数据流动中违法行为的类型,分别以危害国家安全、危害公共安全、扰乱社会秩序以及侵犯公民个人权利等罪责规范加以规制;(2)根据情势发展需要,在我国现行刑法规范无法涵摄前置性法律法规规定的违法跨境数据流动的行为类型时,通过增设或者修改相关刑法立法的方式予以回应。与此同时,我国未来的刑法立法应当尽可能与相关立法规范涉及的技术性规定相协调,以实现刑法立法与其他法规范体系相统一的目标,满足我国刑法对社会治理的回应性需求。

责任编辑 田国宝