法商研究 Studies in Law and Business
Vol. 37 No. 2 (2020)

网络与信息法

超越私权属性的个人信息共享

——基于《欧盟一般数据保护条例》正当利益条款的分析

商 希 雪*

摘 要:在获取、处理、使用和转移个人信息的过程中,各方主体之间存在信息权益冲突,迫切需要规范层面提供协调机制。关于信息权益的主体划分和保护层级、信息正当利益的法律内涵、各方主体利用信息的范围和界限等问题,学界尚未提出明确的解决思路。为推动社会治理和产业经济的数字化进程,个人对信息的绝对控制需要让位于信息正当利益的维护和实现。《欧盟一般数据保护条例》规定在某些情形下应该优先保护信息的正当利益,体现出欧盟调节各方信息权益时的权衡和取舍。借鉴《欧盟一般数据保护条例》的规制路径并结合我国的现实问题,我国立法应构建信息主体、其他自然人、国家机关、企业四方主体共享的个人信息权益体系,以妥善解决各方主体之间的权益冲突。

关键词:个人信息 正当利益 权利共享 《欧盟一般数据保护条例》

个人信息共享的正当性表现在三个方面:首先,公民的个人信息属于公民人身权和财产权的一部分,兼具人格权和财产权的双重权利属性;其次,公民个人信息是高效社会管理系统的运作工具,“互联网+政务”模式下的个人信息早已溢出私人法益的范畴,具备公共性权利属性;最后,个人信息是企业开发和运营数据产业的生产原料,通过深度挖掘个人信息的功能,信息产品和服务不断推陈出新,数字经济的市场竞争呈白热化状态。由此,个人信息的多元利益属性和多方权属主体为信息共享权利体系提供了现实基础。在构建个人信息权益多方共享机制中,立法工作的前提任务是厘清各类共享主体以及界定各自的权益范围。然而,一方面,国内当前的理论研究侧重关注个人的信息权益保护,忽视其他主体利用和共享信息的权益诉求;另一方面,在私法规制体系之外,公法部门对个人信息的规制仍然着力于信息权益的个体保护而非公共利用。鉴于世界各国正在数字政务和数字经济中进行大刀阔斧的改革,为实现“数字中国”的宏伟蓝图,设置新型个人信息共享模式的法律体系,实现各

* 中国政法大学刑事司法学院讲师、网络法学研究院研究人员
基金项目:国家社会科学基金项目(17CFX023)、中国政法大学网络法学青年教师学术创新团队支持计划

方主体在信息利用中共享合作、互利共赢的局面,我国数据立法工作面临刻不容缓的任务。

一、信息共享权机制的体系化构建

《中华人民共和国网络安全法》(以下简称《网络安全法》)第22条、第41条、第42条将“主体同意”作为合法处理个人数据的唯一条件。然而,从《欧盟一般数据保护条例》(以下简称《条例》)前言第39～41段以及第6(1)条来看,与个人数据权利存在保护冲突的正当利益,涵盖公共利益、数据控制者法定职责、其他自然人重大人身权利、数据控制者合法利益、科学或历史研究、统计、法律诉求目的等多方面利益。文中“正当利益”概念是拟制的总括性称呼,本质是信息主体之外利益相关者的数据处理利益。相对于个体信息权利,优先保护正当利益源于对更高位阶法益价值的追求。

(一)“正当利益”的法律内涵

在探讨数据共享问题时,界定“正当利益”是利益博弈中平衡的关键,范围过宽可能侵犯数据主体的信息自由,范围过窄则不利于社会管理或数字经济的发展。《条例》前言和正文设置了诸多正当利益条款,以下剖析其内涵和外延。

1.公共利益

《条例》前言第45段和第6(1)(e)条涉及公共利益。《条例》在对“公共健康”进行界定时参照了2008年《欧洲议会和欧盟理事会关于公共卫生、工作时健康与安全的社区统计1338/2008号条例》第3(C)条的规定,但《条例》并未对“公共利益”提出具体的法律参照,公共利益的外延也不统一。例如,《条例》前言第65段就将公共卫生事业中的公共利益与所有领域中的公共利益并列叙述。可见,《条例》表述的“公共利益”较为概括,只有对公共利益条款做附场景或附目的的解读,才能提炼出其蕴含的核心要素。《条例》中的公共利益并不涵盖大部分国家机关的职能范围,只包含公共存档等少数政务职能。由此推知,此处的公共利益是指公权力职能目的之外的公共或社会利益,公权力机关处理个人数据的职能行为不属于该公共利益的范畴。值得注意的是,为维护公共利益处理数据的数据控制者不仅包括公权力机构,也包括私营组织。《条例》中公共利益优先保护条款分布较为分散,综合分析所有涉及保护公共利益的条款,可以提炼出6类公共利益:(1)科学或历史研究、统计目的。在界定“科学研究目的”的范畴时,综合考虑《欧洲联盟运作条约》第179(1)条规定的增强科研目的,以最广泛的含义解释科学研究,包括技术发展和示范、基础研究、应用研究和私人资助的研究(《条例》前言第159段)。(2)医疗健康、公共卫生事项。为分析传染病及预警目的、监测流行病及传播趋势,即使未经数据主体同意,出于公共利益目的亦可处理有关个人敏感数据(《条例》前言第45段、第52段和第159段)。(3)保存和披露公共存档资料。主要包括:1)持有涉及公共利益信息记录的公共或私人机构,根据成员国法律有义务获取、保存、评估、交流、促进、传播和提供符合一般公共利益且具持久价值的信息记录;2)成员国被允许进一步加工个人数据以供存档;3)如果数据披露行为符合国内法对该机构的职责规定,则公共机构所保存的官方文件中的个人信息可被该机构公开披露,并被视为符合公共利益目的(《条例》前言第158段、第154段和第86条)。(4)国际法义务。对于因人身或法律限制而无法做出同意的数据主体,任何将其个人数据转移到国际人道组织的行为,若符合《日内瓦公约》或其他国际人权法的立法宗旨,可纳入公共利益的考量范围(《条例》前言第112段);另外,“基于宪法、国际公法、被官方认可宗教协会的设立目的,公权力机构处理个人数据视为符合公共利益”(《条例》前言第55段)。(5)人道主义目的。对于紧急事件,尤其在自然灾害或人为灾难发生时,处理个人数据视为符合公共利益(《条例》前言第46段)。(6)政治选举目的:基于国家政体特征,政治选举活动中各

党派收集和处理公众政治观点的行为可视为服务于公共利益而被允许(《条例》前言第56段)。

2. 数据控制者的法定职责[①]

当数据控制者为国家机关时,若数据处理旨在行使法定职权,即使未经数据主体同意,行为仍然合法,[②]这是国家机关履行法定职能的内在需要。根据《条例》前言第45段,国家机关处理个人数据的职能行为的法律依据是法定职责,认定标准为:(1)法律明文规定,参照国家机关设置和职能分工的相关立法,如宪法、国家机关组织法和行政立法等;(2)职权行为,执行主体必须为国家机关且数据处理目的确为执行公务必要。我国现行法律侧重规制获取和披露信息的行为,对个人信息的利用尤其是公法意义上的公共使用尚缺乏足够法律支持。相对于企业难以获取个人敏感信息的情况,国家机关有强制权力获取如社保身份信息、病史记录等个人信息。对于国家机关,数据主体行使数据权利的空间非常有限。同时,随着大数据资源和信息技术在政务管理中被广泛应用,尤其在社会风险治理领域(如反恐任务下对可疑人员的监视和预警、犯罪侦查、公共事件应急决策、网络舆情管理等),个人信息在公共使用过程中呈现出个体信息权益与执行公共职能的冲突。如何解决政府利用个人信息时公、私利益之间的冲突是目前我国公法领域所面临的难题,也是构建信息共享机制的障碍之一。根据《条例》第6(1)(e)条的规定,当数据控制者为企业时,如其处理数据的行为系为公共利益执行职务或受托行使公权力所必需则属合法。如此一来,公权力机关为维护公共利益有权访问企业的数据库,而公权力机关授权企业处理数据亦被视为企业的合法职务行为。在2018年"8·24乐清女孩乘车遇害案"[③]中,受害人就因公安机关要求滴滴平台披露车主及车辆相关信息被拒而未获得及时救助。若通过设立信息共享机制明确企业在数据处理目的上的法定义务,则该案中公安机关要求平台披露信息时,平台即有义务配合公安机关履行其公权力职责。

3. 数据控制者或第三方的合法利益[④]

《条例》前言第47～50段列举了"合法利益"的范畴,包括市场营销、诈骗预防、国家机关间数据传输、网络与信息安全保障、向主管部门报告可能的犯罪行为或对公共安全的威胁。此前,《欧洲数据保护指令》第7(f)条亦有设置合法利益条款,《条例》在《欧盟数据保护指令》的基础上新增直接市场营销为合法利益。数据控制者利用数据的市场营销行为主要包括基于数据画像做出的决策、与数据主体关于数据处理违规行为的沟通等,这些均为最常见的个人数据商业应用场景。《条例》单列直接市场营销为合法利益之一,意在为企业的商业利益留出空间。欧盟委员会在《关于欧洲企业间数据共享的研究》[⑤]中也表示,为发展欧洲数据产业,将在严格数据保护规定之外制定软政策,为数据共享建设中的企业提供政策指导。由此来看,欧盟对数据的商业利用和共享持允许和鼓励态度,呼应了《条例》第1条的规定。此外,因公共安全事项中存在基于"网络与信息安全保障""诈骗预防""向主管部门报告可能的犯罪行为或对公共安全的威胁"的合法利益目的,故企业处理信息的公共利益与合法利益目的可能存在叠加,或者公共利益目的是合法利益正当性的来源。例如,根据《条例》前言第50段,在法律明文规定情况下,基于公共利益,在遵守法定、职业性及其他有约束力的保密义务前提下,即使违背

① See GDPR, Rec. 45; Art. 6(1)(c), Art. 6(3).

② See GDPR, Art. 4(7).

③ 参见《8·24乐清女孩乘车遇害案》,https://baike.baidu.com/item/8·24乐清女孩乘车遇害案/22835678,2019－05－30。

④ See GDPR, Rec.47－48; Art. 6(1)(f).

⑤ See European Commission, Study on Data Sharing Between Companies in Europe, European Union, 2018.

数据主体的目的兼容性,数据控制者仍有权进一步处理个人数据,并将其视为符合数据控制者的合法利益。由此推断,数据控制者担负的数据公共安全责任也被纳入合法利益的范畴。例如,社交类应用程序(APP)出于安全校验需要在用户登录和注册环节会申请获取用户的电话权限和收集用户的国际移动设备识别码(IMEI),从而达到排除机器人批量注册、虚假注册、非法使用他人账号等违法犯罪活动的目的。在《条例》体系下审视该场景,一方面,电话权限和国际移动设备识别码属于个人信息自决权或个人自由的范畴;另一方面,企业通过获得并处理上述数据实现防范用户批量或虚假注册、非法使用帐号的目的,该审核旨在维护所有用户正常的数字生活秩序。在"互联网+"的社会运行模式下,笔者认为上述三类数据的公共安全目的均可被纳入企业的合法利益范畴。值得注意的是,基于数据公共安全目的而进行的数据处理依然需要遵循必要性和适当性等数据处理原则和标准。

4. 数据主体或其他自然人的重大利益①

生命健康权是公民其他一切权利的基础,因此其法律保护价值高于个人信息法益价值。《条例》保护自然人重大利益条款遵循不同法益价值的保护顺序,如《条例》前言第 112 段规定:"在数据主体无法做出同意表示的情况下,为了保护数据主体或其他自然人至关重要的人身权利诸如生命权和健康权等,转移个人信息可被视为合法",同时第 6(1)(d)条亦明确规定在个人数据转移中尤其是在事关自然人生命和健康权利时,存在数据主体"同意的例外"。从数据共享角度看,这意味着数据主体外的其他自然人亦是数据权益共享主体之一。尽管其他自然人出于维护自身重大人身权益需要处理或利用他人个人信息,但其他自然人只是启动数据处理的申请者,由数据控制者决定数据处理的现实执行。由此来看,作为利益相关者的其他自然人,存在信息权利享有与行使的分离。

(二)信息共享体系中的各方权属

"正当利益"的法律内涵决定了各方的信息利用界限,由此组成信息共享权体系的基本架构。《条例》的制度设计为二元规制路径:一方面,《条例》第 23 条规定,成员国法律可通过立法限制第 12~22 条和第 34 条中个人信息权利和义务的范围;另一方面,在某些特定情形下,数据控制者的保护义务可获得不同形式和不同程度的豁免。

1. 信息共享体系的整体架构

划分同一客体承载法益的不同归属主体是构建共享权机制的前提。首先,确定利益相关方的范围。《条例》描述的主体包括数据主体、数据控制者、数据处理者及其他自然人,涉及数据归属、处理环节、利益相关等因素。由于数据处理者只是所处环节与控制者不同,因此笔者不对数据处理者与控制者的共享地位做出区分。② 鉴于公权力机关与私营企业追求的信息正当利益有着性质区别,笔者将数据控制者分为两类即国家机关和企业。其次,区分不同主体对个人信息的利益诉求。国家机关控制信息的利益表现在社会管理效益方面。企业控制信息的利益表现在追求商业利益方面。至于数据主体,控制信息的利益主要是保护隐私或其他人身和财产利益。其他自然人并不直接控制信息,间接控制信息的利益主要基于重大人身利益,如生命权和健康权等。最后,厘清各方主体处理数据的合法

① See GDPR, Rec. 46; Art. 6(1)(d).

② 在《欧盟一般数据保护条例》中,数据控制者(data controller)与数据处理者(data processor)在界定上有所区分,面对不同的义务设定,相较而言,数据控制者需承担更多的责任,如保证数据处理合规以及承担相应的证明责任。See Burri Mira, Rahel Schär, The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy, 6 Journal of Information Policy, 479-511 (2014).

依据。根据《条例》的规定,国家机关基于公共利益或法定职责可处理数据、企业基于合法利益要求可处理数据、数据主体则基于各项法定的数据权利和人身权利可处理数据、其他自然人则基于法定的人身权利可处理数据。

接下来,信息共享权属问题的解决需要厘清各方利益相关人对信息的权利性质和权能种类。信息主体对个人信息虽然享有所有权,但不享有绝对的控制权,其各项权能被不同程度限缩。这是因为,为享受个性化信息产品或服务带来的便利,个人必须让渡部分或全部信息使用权。传统所有权制度的绝对控制性在大数据时代已然不存在生存土壤。在此前提下,其他主体对信息的使用、处理和收益的权利源于信息主体对信息所有权部分权能的让渡,体现了个人所有权向社会共用权的转化,从而形成企业与信息主体、国家机关与信息主体、企业与国家机关之间的权益制衡关系。概言之,个人信息权的产生、行使、管理和保护实则取决于四方主体在信息使用和收益中的制度分配,也就是共享权模式下三类权利的优先关系和平衡规则。在制度设计上,应采纳个人信息权益的双重规制模式。对于信息主体侧重设立保护机制,其在私权领域中被赋予一系列信息权利;对于数据控制者则重在设置管理义务,对应一套行为规范。① 个体信息权利让位于正当利益时,一方面数据控制者存在信息保护义务的豁免,另一方面信息主体行使个人信息权时存在某些限制。

2.数据控制者的信息利用边界

一方面,数据控制者在信息使用中享有优先权。原则上,数据处理应基于数据主体的意思自治,但《条例》还提供了数据处理的其他法律依据。在个人的信息处理意愿与信息的正当利益发生冲突的场合中,优先保护正当利益一般是基于数据控制者的法定职责、数据控制者出于公共利益或官方授权执行工作任务或者数据控制者或第三方的正当利益。例如,在数据自动化处理时,原则上需经主体同意或为履行合同目的,但主体行使数据权时不应与控制者所担负的公共职责或法定义务相违背。因此,《条例》前言第68段指出上述原则性规定不适用于:(1)为履行数据控制者承担的法定义务;(2)维护公共利益;(3)数据控制者的职务行为。另一方面,数据控制者的一般保护义务可获例外豁免。在行业规范下,数据控制者担负特定数据保护义务,如保密、匿名处理、不超越授权范围等。同时,在个体数据权保护义务之外,数据控制者亦承担保护公共利益、他人核心利益、法定职责等社会责任性质的义务,甚至也可合法追求经营利益等。因此,当个体权利与上述利益冲突时,若正当利益保护价值超越个体数据权益,数据控制者原本的保护义务可被豁免。根据不同的数据处理环节,义务豁免情形主要有:(1)数据转移中保护义务的豁免。若数据转移是为重大公共利益,即使在转移中没有充分采取《条例》要求的保护措施,该转移也视为合法[《条例》第49(1)(d)条]。但是,数据控制者维护的公共利益应由欧盟法或国内法明确规定[《条例》第49(3)条]。(2)数据处理中通知和说明义务的豁免。该豁免条款分别针对数据控制者和数据处理者,涉及以下情形:1)数据控制者与数据主体之间。当获取的个人数据并非直接来自数据主体时,数据控制者应向数据主体关于处理细节做出说明[《条例》第14(1)～(4)条]。但是,当该通知信息被证明是不可能或者需要付出过度努力时,尤其当数据处理是为了公共利益、科学或历史研究、统计目的而进行的存档行为时,可以不必说明[《条例》第14(5)(b)条]。2)数据处理者与数据控制者之间。一般来说,处理个人数据只能根据数据控制者的书面指示,包括数据向第三国或国际组织转移等情形;除非欧盟法或处理者所属国的国内法另有规定,允许数据

① 参见中国社会科学院民法典工作项目组:《大数据时代下个人信息保护的立法模式变革》,https://mp.weixin.qq.com/s/4KVobF26Yb0Ay0kz0ceoaw,2018－05－20。

处理者不必告知控制者即可处理数据;即使在这种情况下,数据处理者在处理之前也应告知数据控制者该法律规定,除非基于重大公共利益法律禁止提供这样的通知信息[《条例》第 28(3)(a)条]。(3)数据保护影响评估中咨询义务的豁免。在不影响商业或公共利益以及操作安全的情况下,数据控制者在恰当时候应寻求数据主体或其代表人对预期处理的意见[《条例》第 35(9)条]。如果涉及保护上述正当利益,数据控制者不必履行通知义务。

3.数据主体的权利行使限制

一般保护原则的例外规定普遍适用于各项个人数据权利。同时,基于各项数据权利的特性,除数据访问权和更正权外,《条例》在每一项数据权利下重申了各数据权利行使时对其他正当利益的考量,并设定了具体限制条款以作特别提示。例如,数据主体行使限制处理权后,原则上除了储存行为,数据处理者只有经数据主体同意方可继续处理。但是,基于法律诉求的执行或辩护、保护第三方权利或维护成员国重大公共利益的目的,[①]需要处理已被限制处理的个人数据时,对数据主体限制处理权的执行可被终止。也就意味着,即使个人信息已经处于限制处理状态,但若需要在上述情形中使用,仍然可以被处理。是否可将该限制情形前移至数据主体行使限制处理权当时?从现实效果来看,前推适用是合理的。在各项数据权利中,被遗忘权的限制情形最多,这是因为,行使被遗忘权时关涉的公共利益范围最广。被遗忘权对个人数据的公开产生根本限制作用,使得被遗忘权与言论自由、信息公开所蕴含的公共价值之间存在利益冲突。2014 年,欧盟法院在首个关于被遗忘权的判决中认定,不相关的和过时的个人信息经请求后应被删除。[②] 由此推断,可被"遗忘"的个人数据需满足以下要素:(1)不相关性。即个人数据与《条例》第 17(3)条规定的正当利益不具有关联性。(2)过时性。即该个人数据已无信息公开必要,也可看作是对相关性的反向重申,也即该个人数据对维护正当利益不存在参考作用或影响。此解读思路体现在英格兰—威尔士高等法院的两起被遗忘权案[③]中,两位原告(各自匿名为 NT1 和 NT2)[④]曾要求谷歌(Google)删除关于多年前他们犯罪报道的链接,以消除对其生活和工作的不良影响,但谷歌以个人职业生涯中的犯罪信息属公共利益范畴为由拒绝删除。该高等法院支持了 NT2 的诉求却驳回了 NT1 的请求。对于案情相似的两个案件,之所以出现不同的判决,审理该案的法官沃比认为是因为:(1)NT2 之前的犯罪行为并非针对"消费者、客户或投资者"等群体的行为而是侵犯他人隐私的违法行为。该犯罪行为与 NT2 正从事的职业无任何明显关联性,对于他人对 NT2 的职业评估不存在影响,因此没有必要保存犯罪报道作为警告。(2)谷歌搜索服务的用户没有支持该犯罪报道继续存在的合法权利。而对于 NT1,法官认为,NT1 并没有表现出对以往罪行的懊悔,并且 NT1 仍然在商界活动,曾经的犯罪行为与目前从事的职业有关联性。因此,保留 NT1 的犯罪报道是为公众提供警告,以尽量降低 NT1 对他人可能再次造成损害的风险。反之,即使删除 NT1 的犯罪报道也并不会抹除官方犯罪记录,反而会导致该犯罪信息难以被察觉,无法起到警示作

① See GDPR, Art. 18(2).

② See Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. C—131/12, 13 May 2014.

③ See Charlie Nash, Google Loses "Right to be Forgotten" Case Appeal in UK, http://www.breitbart.com/tech/2018/04/13/google—loses—right—to—be—forgotten—case—appeal—in—uk/, 2018—04—13; Jamie Grierson, Ben Quinn, Google Loses Landmark "Right to be Forgotten" Case, https://www.theguardian.com/technology/2018/apr/13/google—loses—right—to—be—forgotten—case, 2018—04—13.

④ NT1 曾被判为假账罪的共犯,处以 4 年有期徒刑;NT2 曾被判为拦截通讯罪的共犯,处以 6 个月监禁。

用。从与正当利益冲突的角度看,一方面,被遗忘权与言论自由、信息公开、公众知情等公共价值存在冲突;另一方面,作为横跨在数据主体和企业间的防御屏障,过度行使被遗忘权会影响企业的市场竞争力。

(三)各方信息权益保护的位阶

《条例》第6(1)(f)条原则性地规定,为实现数据控制者或第三方合法利益的数据处理应视为合法,但是在该情形下,如果为了保障数据主体的基本自由和权利,并且该保护利益高于数据控制者或第三方追求的合法利益时,则处理行为不合法,除非是公权力机关执行工作任务。可见,在《条例》的框架下,信息权益保护的位价为:数据控制者或第三方的合法利益让位于数据主体的基本权利和自由,但保护数据主体基本权利和自由的考量要让位于公权力机关的职责履行。由此可知,在数据处理的利益博弈中,公权力机关的职责处于最高保护位阶。在解读合法利益的官方文件中,公权力机关行使公共职权时不能以合法利益作为处理数据的理由。[①] 由此推断,公权力机关只能出于维护公共利益和履行法定职责而处理个人数据。因此,即使公权力机关存在合法利益的目的,也不能超越数据主体基本的权益和自由。前面提到,企业合法利益的范畴包括数据公共安全目的,那么该类安全目的可否超越个人数据权利获得优先保护呢?由此来看,答案必然是否定的。数据经济市场中很重要的产业环节是数据转移,对于转移过程中正当利益与个体利益之间的冲突,《条例》设定的优先保护规则大多是侧重维护公共性利益而非企业的合法利益。同时,数据控制者的合法利益不得超出数据主体基本的数据权益和自由。可见,数据权益保护的位阶为:国家或社会的公共性利益(公共利益或法定职责)大于个体基本数据权益和自由,后者又大于企业数据利益(合法利益)。然而,对于信息主体非基本的数据权益和自由与企业合法利益(主要指市场营销目的)冲突的权衡路径,《条例》没有提供清晰的判断依据,有必要对企业的合法信息权益予以探讨。

二、非基于公共职责的企业信息权益

出于公共利益或法定职责,数据控制者使用个人信息是履行国家职能的合理方式,职能权限包括信息使用权限。在商业使用中,确立非公共职责的正当利益范畴是建立个人信息共享权的前提。

(一)企业信息权益的厘定

公权力机关使用个人数据时一般不具营利目的,立法保护个人信息商业利益的目的是推动数字经济的发展。推动方式表现为两方面:一是积极作为,二是消极保护。《条例》保护企业合法利益主要采取后一种方式。尽管《条例》前言第47段明确规定,直接市场营销目的可被视为数据控制者的合法利益,但这并不意味着企业可以未经用户同意就将其个人数据用于市场营销。合法利益条款本身尚不足以作为获取信息商业利益的完整依据,还需要确定合理的数据使用范围和使用方式。

1.企业可利用的数据范围

① See UK Information Commissioner's Office, What is the "Legitimate Interests"Basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/, 2018—05—20.

《条例》规制的数据类型有:(1)可获取和可循环利用的公共机关数据;[①](2)可共享的科研数据;(3)在企业与企业之间或者企业与政府的私营部门之间可共享的数据;[②](4)公民医疗健康数据。欧盟委员会认为,某些特殊领域的数据具有巨大的共享价值,包括交通、气候、能源、卫生等领域。[③] 对于公共事业领域的个人数据,公权力机关和私营企业可在收集和使用方面展开合作。在欧洲医疗健康领域中,移动医疗和电子健康行业正积极通过标准化和共同协作的方式为投资生命科学的企业(包括医疗设备公司、在线销售药品的制药公司等)提供商业机会。因此,公民医疗健康数据不仅限于公共事业管理中的使用,也可能用于商业医疗产品和服务的市场研发。该类数据明显具有双重使用价值,包括社会管理价值和市场经济价值。因此,对于该类个人数据的正当使用,可以是公权力机关出于法定职责或公共利益,也可以是企业出于合法利益或法定职责。

在运营中需使用个人数据的企业主要是提供产品或服务的网络平台企业。欧盟委员会曾在欧洲31个国家发起企业间数据共享研究,共对129家公司做了调查访问,主要涉及7类数据行业:数字驾驶、智能制造、智能农业、电信运营、智能生活、智能电网、计量设备等。上述行业中,最常见的两类可共享的数据是:(1)内部业务资讯系统产生的数据(约占56%);(2)物联网产生的数据(约占54%)。商业和工业市场中目前可共享和利用的数据主要有两类:一类是针对消费者或需求商的科技服务或产品中涉及的个人数据;另一类是工业或农业生产物联网产生的个人数据。再从数据产生方式看,机器自动生成数据在产业领域中的应用十分广泛,具有极高的共享必要性,欧盟目前有关数字经济的文件也主要涉及该类数据。根据2018年《欧盟非个人数据自由流动条例》前言第9段,非个人数据主要包括机器生成的和商业经营中产生的数据。由此,在限制性和共享性上,机器生成数据和商业运营数据处于同等地位。因此,机器自动生成数据属于企业之间可共享以及可商业利用的数据范围。可见,依据生成方式和适用领域归纳出可商业使用的个人数据范围,对其的商业化利用属于企业合法利益。

2.企业利用数据的正当方式

企业利用和处理个人数据主要有两个合法依据:用户同意和合法利益。合法利益条款是用户同意条款之外的补充条款,用户同意适用于大部分个人数据商业使用情形,并且应被企业优先适用。[④]具体分析来看:(1)在用户同意制度下审视企业的信息使用方式,个人信息商业利益的法律保护价值并不高于自然人人身和财产权的保护价值,两者在法律保护上处于同等地位。实践中,企业往往通过广泛挖掘和使用个人信息获得商业利益,如通过提升用户的使用体验来吸引更多用户。因此,企业与信息主体间的利益权衡关系可归结为用户自身对效率获取与隐私披露间的取舍选择,通过赋予主体充分自主的选择权并相应地细化用户与企业间服务协议,可妥善解决双方的利益冲突。在具体制度

① 2013年6月,经修订后的《欧盟公共部门信息再利用指令》涵盖公共事业部门在交通和公用事业部门所拥有的数据,规定了允许公共机构收取数据传播的边际成本费用以循环使用其数据的例外情况,促进公开研究数据的可循环利用性。See Directive 2013/37 / EU of the European Parliament and of the Council of 26 June 2013 Amending Directive 2003/98 / EC on the Re-use of Public Sector Information Text with EEA relevance, Official Journal of the European Union, L 175, 27 June 2013, pp. 1-8.

② See European Commission, Towards a Common European Data Space, SWD(2018) 125 Final. 该通讯旨在为欧盟运营企业提供数据共享协作的法律与技术指导。

③ See European Commission, Building a European Data Economy, COM(2017) 9 final, 1 October 2017.

④ Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC (844/14/EN WP 217), 9 April 2014, pp. 10-11, p. 25.

设计上,有学者指出:要同时强化个人敏感信息的保护和个人一般信息的利用,企业在普遍免费服务模式的基础上提供用户可选择的个别付费模式;在免费模式下提供基础性和统一性的数据保护措施,而在付费模式下基于合同约定,用户享有个性化定制和高保护标准的数据安全措施;此外,通过筛选用户倾向,对个人信息迟钝者和个人信息敏感者作区分保护(分别为标准化与个性化保护)。① 笔者认同区分性保护敏感信息和一般信息,因为两者在法律内涵上存在确定的区分。但是,用户分类筛选的制度设计尚需进一步探讨。这是因为,对用户"迟钝"或"敏感"特性的判断过于主观与随机,会增加法律适用的不确定性。在发生信息权益纠纷时,监管机关或司法机关难以做出令公众信服的决定。(2)考虑到在某些情况下企业取得用户同意可能极为困难或者成本过高,再加上对用户同意表达有着严格要求,如书面形式、内容清晰、自由意志等,在特殊情况下,企业可适用合法利益条款作为数据处理的法律依据。② 根据《条例》第5~6条中的相关规定,企业利用个人数据时应明确知晓正在收集哪些数据以及将用于何种目的,尤其在未经主体同意的特殊处理过程中,对企业行为的限制非常严格。

(二)企业与公共机关之间的数据共享

除企业间数据共享外,私营主体与公权力机关之间的数据双向流动也是目前数据共享的趋势。欧盟的数据共享有两类模式:政府与企业间共享模式(B2G)和企业与企业间共享模式(B2B)。

1.企业数据的公共利用

2017年,欧盟委员会就《重复使用公共部门信息的指示》做公众问询调查。调查显示,为科研或政府管理目的访问私营组织的数据值得支持和推广。基于此背景,2018年4月25日,在发展单一数字市场的策略下,欧盟委员会发布《修改〈重复使用公共部门信息的指示〉的建议》。电信运营商、在线平台、汽车制造商与零售商、社交媒体等平台的数据具有高度的公共利用性。该类数据的公共使用可使公共部门更有针对性地应对流行病、更合理地规划城市、更有序地管理交通系统及保障道路安全、更好地保护环境、更有效地监测市场与保护消费者等。③ 企业与国家机关的数据共享合作是指企业将其所收集数据的分析成果服务于公共利益和照顾其他利益相关方,彰显了企业的社会责任。在我国,中国人民银行于2015年允许8家商业机构对个人征信业务做准备工作,互联网征信体系已迅速发展起来。在第三方个人信息源接入政务系统的应用举措中,公共事业单位如公交系统、电信企业、保险公司等与征信服务企业在个人信息共享上已展开深入合作,体现出国家将集合性个人信息作为公共资产进行宏观调控和重复利用的态度。我国目前的数据共享立法工作主要侧重于国家机关之间的数据共享,④反映了国家机关间积极建设信息共享平台的发展趋势。对于私营企业与国家机关之间的数据共享合作,我国也在进行制度探索。例如,《国务院关于印发政务信息资源共享管理暂行办法的通知》第2条规定,政务信息的收集方式扩至第三方信息源。

2.公共部门数据的商业利用

欧盟数字经济市场的数据原料不仅限于企业自身收集和加工的数据,也包括公共部门的数据。

---

① 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。

② See Legitimate Interest, https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/, 2018-04-13.

③ See European Commission, Towards a Common European Data Space, SWD(2018) 125 Final.

④ 参见《关于建立和完善执行联动机制若干问题的意见》(法发〔2010〕15号),《关于建立实名制信息快速查询协作执法机制的实施意见》(公通字〔2011〕3号),《关于加强信用信息共享及司法协助机制建设的通知》(法〔2014〕312号),《关于建立快速查询信息共享及网络执行查控协作工作机制的意见》(法〔2016〕41号)。

在欧盟层面看,公共事业领域的个人数据属于可商业利用的数据范围。大规模且高质量的个人数据资源掌握在政府部门手中,[①]但原始数据被加工为可利用的数据产品或服务需要大量的资金、技术、人员和设备支持,政府部门却缺乏相应的资源,因此有必要开展政企合作。[②] 由此,公共部门数据库的商业共享需要在立法层面做出谨慎的规范设置。在政府与企业间共享模式中,由于同时涉及公法和私法规制,数据共享主体的法律地位通常不明晰。政府与企业间共享模式主要面临数据处理的合规性挑战,主要表现在:(1)必要时保持信息的机密性;(2)获取信息时企业的额外保护义务不能妨碍共享。[③] 对此,笔者认为,一方面,企业利用公共部门数据时要有目的上的限制,应主要用于开发公共事务有关的数据产品或服务,如金融、医疗、通信、交通、电力、环境、自然资源等事项相关的数据成果;另一方面,对企业的数据使用权限要有限制,企业的数据利用权限来自政府部门的授权,本质是公共部门信息使用权的转移,不能超越公共部门的信息使用权限和信息主体的数据权益,数据共享权体系本质上是各方信息使用权限的内部流转关系。考虑到公权力机关收集个人数据的难度较低,而企业收集信息则需付出一定的市场成本并承担更严格的数据保护义务,因此政府数据向企业的流动需要严格限制,避免企业变相逃避市场责任和数据安全义务。

(三)我国企业开展数据共享策略的障碍与出路

在数据共享的合法化问题上,我国企业目前面临的法律顾虑有:数据权属的模糊性、侵犯公民个人信息罪适用的扩张化、《网络安全法》第 41～44 条安全保障义务的概括性。我国面临互联网企业失信与公众缺乏信息安全感的现实困境,无论企业还是政府,对于数据的披露和利用几乎如履薄冰,数据共享合法化的道路艰难。相比而言,欧盟企业间数据共享已呈规模化态势,意味着欧洲商界与公众之间已建立一定程度的信任。欧盟在数据共享领域开展了系统性的立法政策咨询、技术支持储备和社会信任建设等工作,逐渐形成"数据共享—更好的产品和服务—数据主体获得更好的产品与服务"良性循环的产业系统。[④] 有鉴于此,恰当照顾数据主体权利的信息保护机制为企业与企业、企业与政府部门之间开展数据共享奠定了制度基础,有利于树立用户相信数据控制者会合理利用其个人数据的社会氛围,这样不仅有利于高效获得用户的授权同意,也推动数据共享的运作机制更加臻于成熟。

三、共享模式下信息主体权利的基本保障

多方主体共享和利用个人数据时,为保障信息主体的个人信息权益,最关键的制度设计是数据主体应享有贯穿始终的反对权。因此,在基于信息合法利益而做出数据处理的情形中,数据主体应一直享有反对权,只有存在法定拒绝理由时反对权才可被排除。[⑤] 在数据主体行使反对权的情况下,数据

① 例如,我国目前已建立的政府信息数据库包括人口信息管理系统、出入境/证件信息数据库、全国违法犯罪中心数据库、脱氧核糖核酸(DNA)数据库、统计数据库等。

② 美国数据共享的政企合作又称为公私合作模式,该模式下的政府主导型符合此处的共享方式描述,通过政府主动开放自身数据吸引企业投资,深化政府数据的创新应用,如开展创新应用竞赛、合作建立试点项目。参见黄如花、陈闯:《美国政府数据开放共享的合作模式》,《图书情报工作》2016 年第 19 期。

③ See Dhata Praditya, Marijn Janssen and Reni Sulastri, Determinants of Business－to－Government Information Sharing Arrangements, 1 The Electronic Journal of e－Government, 44－52 (2017).

④ 参见冯坚坚、刘晓春:《数据共享合法化:以〈关于欧洲企业间数据共享的研究〉为起点》,https://mp.weixin.qq.com/s/YxNZRDrV3－k2－P_8GaBs2Q, 2018－05－09。

⑤ See Guide to the GDPR — Legitimate Interests, https://www.twobirds.com/～/media/pdfs/gdpr－pdfs/23－－guide－to－the－gdpr－－legitimate－interests.pdf? la＝en, 2018—05—20.

控制者需证明确实存在高于个体利益且具有强制效力的法定利益,[①]如果无法证明,数据主体接下来则可行使限制处理权或被遗忘权。根据行使效果,反对权可分为绝对反对权和相对反对权。

(一)绝对的反对权

《条例》序言第70段规定当企业将个人数据用于市场营销时,数据主体有权对市场营销中被数据画像的程度、起始处理结果、处理时间及费用承担等事项表示反对,且该反对权与其他信息区分开以单独提请数据主体注意。对于直接市场营销行为,数据主体享有绝对的反对权。"绝对"意味着:(1)数据主体可在任何时候要求数据控制者停止任何与市场营销有关的数据画像[《条例》第21(2)条];(2)数据控制者必须无条件服从,不存在拒绝的理由亦无须提供证明来对抗反对权[《条例》第21(3)条],一旦收到数据主体的反对通知(口头或书面),数据控制者应立刻停止营销行为。可见,企业的直接市场营销利益需要服从数据主体的处理意愿。但是,此处的商业目的仅限于产品或服务的商业推广,在市场运营、产品开发和销售等环节中,数据控制者的其他数据处理利益是否也应绝对地让位于数据主体的个人反对意志?笔者认为,《条例》单独列出的市场营销类型是以直接方式做出的市场营销,因为直接营销方式给用户带来的影响较大,干扰了个人生活的安宁。由此,笔者认为,在限制反对权的条件设置上,既然《条例》将数据控制者或第三方的合法利益与直接市场营销目的分别规定在不同条款中,《条例》第21(1)条关于合法利益的规定就为企业直接市场营销以外的商业目的留出了合法空间,包括间接市场营销及其他商业目的。随着信息技术日新月异的发展,在直接市场营销之外,合法商业目的的外延是开放的,需结合特定信息产品和服务的应用场景作出判断。

(二)相对的反对权

当数据处理出于公共利益、官方授权、数据控制者或第三方的合法利益目的,且该利益未超越数据主体的基本自由和权利,数据主体可对该处理提出反对,但不一定得到数据控制者的无条件支持,因此属于相对的反对权。

1.行使限制

一方面,如果数据控制者有法定理由证明所处理的利益高于个人利益,或者数据处理是为了法律诉求的提出、执行和辩护,该处理行为就不受反对的影响。[②] 若上述三种利益属于本文所指正当利益的范畴,数据控制者提供法律依据即可。若数据处理是为了公共利益或官方任务,则数据主体的反对权无效。这意味着,当数据处理是基于公共性利益时,反对权是绝对性的无效。尽管《条例》区分了公共利益目的与官方授权行为,但在实践中很难对处理目的做出明确的定性,容易发生混淆。对此,应主要以公权力机关的明确指令作为判断和区分的依据。当数据控制者或第三方追求合法利益时,数据控制者应在其合法利益与数据主体的权利、利益、自由之间做出衡量和评估,但权衡各方利益的实践均为个案操作,并无统一的流程和标准,具体结果也因案而异。根据《条例》第6(1)(f)条,权衡因素实则由数据控制者自行决定,即使数据主体不同意数据控制者的决定,也只能诉诸数据保护署或法院寻求救济。由此看出,该权衡条款要真正落地实施尚缺乏具体的制度设计,导致反对权仍处在"字面权利"阶段。[③] 另一方面,《条例》第21(6)条规定:"(《条例》)第89(1)条中个人数据因科学或历史研

① See GDPR, Rec. 69.

② See GDPR, Art. 21(1).

③ See UK Information Commissioner's Office, Right to Object, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/, 2018—06—02.

究、统计目的被处理时,数据主体基于自身情况有权拒绝个人数据被处理,除非该处理是基于公共利益的必要”。由此判断,如果数据处理是出于科学和历史研究、数据统计目的,反对权将受到更多的限制。具体表现在:(1)数据控制者被允许的处理空间更大,对基于官方授权、数据控制者或第三方合法利益而进行的历史、科研、数据统计目的的数据处理行为,数据主体的反对可能不被支持;(2)根据《条例》第89(1)条,基于科学或历史研究或统计目的成功行使反对权时也不会触发删除权的适用,而在其他目的情形下,反对权被支持后可能引起删除权的后续行使;①(3)《条例》第21(4)条规定在隐私协议中数据控制者无须分别告知用户反对权与其他信息权利,在其他目的情形下则需单独提醒。②

2.证明责任的分配

《欧洲数据保护指令》第14(a)条规定数据主体需证明存在强制法定理由支持个人数据不被继续处理,而《条例》降低了反对权的行使门槛,将证明责任转移至数据控制者,由其证明存在强制法定理由支持继续处理。数据主体则只需说明个人数据不应被处理的理由,而不再对“强制性”与“法定理由”承担证明责任。这意味着:一方面,数据主体只需说明理由即可,不必提供法律依据。另一方面,数据控制者则需证明:(1)法律依据,即法律明文规定;(2)法定利益,即存在受法律强制保护的利益;(3)该合法利益超越个人权益或自由,或者是为了法律诉求的提出、执行和辩护,应优先被保护。此处的个人权利不仅限于数据权利,也包括其他合法权利。对“超越”的理解应遵循保护价值的位阶,在任何情况下,数据控制者或第三方的合法利益都不得超越数据主体的基本权利和自由。法律诉求的进展过程一般有诉讼法的明确指引,数据处理符合司法程序的法律要求即可。如何量化地证明信息处理利益高于个人利益是较为抽象的问题,从目前已有的解释来看,法律的明文规定是最好的证明。这是因为,确定的法律指引会降低司法审判中法官的自由裁量空间,进而保障个体权益不被任意侵犯。在《条例》中,凡涉及正当利益被优先保护的情形,一般均要求该正当利益已为法律明文规定。③ 在行使反对权的设置上,核心问题在于个人数据保护与其他利益之间的权衡。具体到最难界定的企业信息权益,《条例》第6(1)(f)条的合法利益规定和前言第70段中数据主体在此情形下的反对权条款,可视作企业利益与个体数据权利之间的制衡设置。一方面,不仅要考虑数据主体的合法权利,还要顾及其利益,无论该利益在法律上是否已被确立;另一方面,企业必须承担举证责任,证明该企业的合法利益在某些情形下高于个体信息利益。④ 实务中优先保护的判断可以考量:(1)数据主体应合理预期个人数据可能被数据控制者或第三方做进一步处理的可能,若在合理预期范围内,则企业行为合理;(2)若数据控制者所计划的处理安排超出数据主体的合理预期,即数据主体的权利和利益明显超越数据

① See Jef Ausloos, The Interaction Between the Rights to Object and to Erasure in the GDPR, https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/, 2018—04—21.

② See HIPAA Journal, The GDPR Right to Object Explained, https://www.hipaajournal.com/gdpr-right-to-object/, 2018—06—04.

③ 根据《欧盟一般数据保护条例》前言第112段和第49(5)条的规定,唯一的例外是:即使在没有充分决定的情况下,出于公共利益的考量,国内法亦可明确限制将个人敏感数据转移至第三方国家或国际组织,但欧盟成员国应将该限制条款告知欧盟委员会。提出非明文规定的公共利益主要因为公共利益的外延无法被穷尽列举,因此以“兜底式”规定为欧盟成员国留下维护突发性公共利益的法律支持的余地。

④ Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (844/14/EN WP 217), 9 April 2014, pp. 30-52.

控制者的利益，则企业行为不合理。①

（三）反对权的制度保障

《条例》中的某些制度安排也为反对权适用提供了执行指导，如在主体同意原则适用场景中，数据主体可随时撤回先前同意而不必做出反对表示。因此，同意制度下数据主体的撤销权本质上是另一种形式的反对权，并且撤销权的行使更加自由。《条例》第17(1)(c)条明确将反对权与删除权、被遗忘权关联，规定数据主体的反对权被支持后即可行使删除权。此外，根据《条例》第77条的申诉规定，如果数据主体认为数据控制者或处理者在数据处理过程中违反《条例》侵害了个人权利，其可寻求司法救济，并且有权要求数据控制者对其造成的直接损害负责。由此推断，当个人数据转移至第三方数据处理者时，数据控制者负有保障个人数据安全的责任。② 这也就意味着，数据控制者应就恰当照顾了数据主体的基本权利和自由进行评估。评估应具体涵盖以下事项：(1)采取必要且适当的措施以保护数据主体最基本的权利和自由，如数据假名化处理；(2)保证处理过程中不违背公共利益责任和官方授权职责，且处理利益符合公共性利益；(3)在技术和组织措施上严格遵守目的限制和数据最小化原则；③(4)已经评估了在不允许和不再允许识别数据主体的情况下处理该个人数据以实现上述目的的可行性。④ 反推来看，在基于正当利益进行的数据处理中，原则上不允许识别数据主体。

四、我国信息共享权系统化的制度准备

（一）信息共享法律规范的体系设置

《网络安全法》规制的网络运营者不包含国家机关。国家机关作为收集和使用大规模个人数据的共享主体，立法是否应将其纳入规制范畴？笔者认为答案是肯定的。《条例》将公权力性质的国家机关和私营性质的企业统一纳入规制，统称为数据控制者且在权利和义务设置上一视同仁。这是因为，《条例》的出发点和落脚点在于保护个体的信息权益，因此在各方主体划分上，与个体相对的其他使用主体被划分为同一类。欧盟委员会在其解释文件中也认为，相对于企业来说，包括政府部门在内的国家机关在数据收集、保存和处理的行为标准应有“豁免”，尤其基于行政目的或在诸如公共安全和公众健康等特殊领域中。⑤ 因此，《条例》中不同类型数据控制者的信息正当利益的范畴和界限存在某些差异。跨越公法与私法边界的二元立法模式是个人信息法律的立法特征，我国当前关于个人信息保护、利用和共享的法律体系呈现以下特征：(1)在信息处理环节上，主要针对收集和披露行为，对使用和共享行为较少涉及；(2)在规范目的上，侧重个体保护（主要关注隐私），而对其他主体关于信息利用、公开和共享的权益无清晰界定；(3)部门法规范呈现“刑先民(行)后”“民法模糊”“行政法滞后”的立法局面；(4)规范层面没有明确规定个人信息权益的权属定位和权利结构。学理阐释大多是关联性

① Legitimate Interest, https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/, 2018—04—13.

② See Alan Calder, EU GDPR: A Pocket Guide, Ely : IT Governance Publishing, 2016, p. 42.

③ 《欧盟一般数据保护条例》第5(1)(c)条规定：“充分、相关且以处理目的所必需的为限(“数据最少化”)。”这意味着网站运营者只能在必需的时间内，采取必要的技术设置，以尽可能少地储存数据。

④ See GDPR, Rec. 156; Art. 89(1).

⑤ See Balancing Security and Public Interest: The GDPR and the Public Sector, https://www.trendmicro.com/vinfo/us/security/news/online-privacy/balancing-security-and-public-interest-gdpr-and-public-sector, 2018—04—09.

地分析各类规范文件中的单独规定,并以此推断立法的态度和趋势。然而,各类规范文件的制定部门和法律效力不尽相同,统一解读混淆了不同规范体系的效力位阶,该解读方式并不可取。考虑到我国的立法现实,国家机关与企业在处理和使用个人信息时的利益考量存在本质区别,公、私权利的立法体系依旧界限分明。因此,针对不同类型的正当利益,各方主体信息权益的规范设置应在不同部门法体系下分别探讨。例如,政府部门对个人信息的公开和使用属行政法律和法规的规制范畴,司法机关处理和使用个人信息则属诉讼法的规范领域。个人信息保护法和数据安全法具有公、私法兼容性质,难以划归到某一法律部门中,宜采取综合立法方式,但可对某些关键条款做性质明确的界定,如法律参照、监管机构、救济部门、责任主体、责任模式等事项。

(二)"正当利益"的立法界定

《条例》第 23(1)条以列举方式对正当利益做了最全面的描述。虽然《网络安全法》将主体同意作为合法处理数据的唯一条件,但《个人信息安全规范》(以下简称《安全规范》)在主体同意之外列举了 11 项情形作为数据处理的合法依据。对比《条例》,《安全规范》中正当利益的范畴更加广泛,额外提及新闻报道和信息公开目的。尽管《安全规范》自身无强制性法律效力,但作为国家标准仍可为信息立法提供参照。此外,界定个人信息正当利益的立法技术可参照《中华人民共和国行政诉讼法》第 12 条关于行政案件受案范围的界定,采取概括、列举及排除的方式为各方信息共享主体设定权益范围。

(三)构建信息共享法律体系的整体思路

整体上,《条例》体现了公、私利益平衡兼顾的立法思路,除数据主体自由意志外,特定情形下为优先保护特定正当利益处理个人数据的行为也被视为合法。《条例》中数据主体个人权益让位于正当利益的条款主要体现在:对一般保护原则的限制、个人行使数据权利的限制、公共利益或公共安全的维护、数据控制者的职责行为或合法利益等。由此,在个体数据权利与公共正当利益之间,《条例》内在形成了一套权衡标准和配置体系,为数据权益的多方共享体系奠定了法益划分的基础。借鉴《条例》的规制路径,立足于我国以往的立法传统和实践,我国信息权共享体系的建设工作可从 3 个方面构建:(1)以行政法、诉讼法为主的公法领域,侧重规范个人信息的开放和共享,对个人信息权益和行政或司法职能目的中的正当利益冲突做出平衡设置;(2)涉及网络交易、消费者权益保护、个人信息安全等事项的相关法律文件需要对企业商业利益与个体信息权益间的协商关系做出具体规定,既为个人数据提供充分的法律保护,也要避免数据保护过度增加企业的合规成本而对数据产业发展造成压制。(3)公、私法部门需对企业与公权力机关之间的数据流动和共享做出前瞻性的衔接布局,以打通公、私机构之间的数据控制壁垒和垄断地位,实现数据资源的互补和整合。

责任编辑 何 艳