主题研讨

社会风险控制抑或个人权益保护

——理解个人信息保护法的两个维度

梅夏英

内容提要:个人信息在《民法典》中被确认为一种人格法益,在理论和立法上确立了我国个人信息的私法保护面向。个人权益保护成为构建和理解个人信息保护的重要维度和线索。由于个人信息保护的公共目标和功能可能被个人私益保护的进路所覆盖或消解,因此有必要将社会风险控制作为个人信息保护的重要维度来对待。社会风险控制一直是电子化时代个人数据保护的基础性目的,它对于个人信息保护的相关理论和制度具有很强的解释力和动态构建作用。社会风险控制和个人权益保护两种进路在相关基础问题上出现分歧,如个人信息与隐私的基础关系、一般性保护与场景化保护以及本权与保护权的关系等。在《个人信息保护法》实施过程中,社会风险控制进路有助于合理解读和执行法律,把握风险大小与控制措施的合理匹配,以及在平衡相关立法价值的前提下,释放信息的流动性。

关键词:社会风险控制　个人信息权益　知情同意　场景化　基本权利

梅夏英,对外经济贸易大学法学院教授。

环球法律评论 GLOBAL LAW REVIEW

《中华人民共和国个人信息保护法》于2021年颁布并实施,昭示了我国在个人信息保护领域的基本态度和立法选择。这部立法是在借鉴和综合了国内外既有立法体例和经验的基础上,结合我国数字经济的发展实践和传统法律价值观念制订而成的,可谓我国在该领域立法的一大进步。在该法实施和适用的过程中,如何理解和领会个人信息保护的立法意向和旨趣便成为此一阶段的重要任务,其中以何种立法目标和理论线索来解读整部法律是重点内容。从立法形式和结构上解读这部法律,“个人信息权益保护”无疑是理解这部法律的基本线索和重要维度,从国内外的主流理论以及立法实践来看,个人私益保护一直是个人信息保护理论和立法的重要结构支撑点。尽管在理论发展过程中亦出现了诸如信息公共性理论、场景化保护和公法优位保护等不同的理论观点,但个人权益保护还

是占据了不可动摇的主导地位。尽管个人信息保护与个人自身存在紧密相关性,但并不能完全从个人权益角度得到合理解释,且这种个人化的视角会流失掉对其中“非个人化”的理论和制度的合理关注,如已公开信息的保护、一般同意与单独同意相区别的原因、私法救济的局限以及个人信息的合理流动等,都不能从个人私权中推导或生发出来。基于此种情境,有必要重视从公共性的维度来达致对个人信息保护的完整理解,即“社会风险控制”在个人信息保护中的基础性作用。社会风险控制常常在论述个人权益保护的必要性时被充分重视,但在构建个人信息法律结构体系时又被选择性遗忘。本文将从个人权益保护和社会风险控制两个维度进行分析和比较,系统探讨个人信息保护的立法目的和实现方式,并通过这种公私维度的相互拆解,达成对个人信息保护的完整理解,以期对该法的适用有所助益。

一 个人信息权益私法保护进路的反思

(一)个人信息私法保护的立法与理论

从个人信息保护问题开始提出到相关国家开始尝试立法,该问题主要针对的是国家或政府对于个人信息的滥用及其可能带来的大规模社会风险的防范,但事实上个人信息在理论上还是与“隐私”或“人格”范畴紧密联系在一起,被视为隐私权在信息时代所发展出的新维度。

从早期欧洲国家的立法选择来看,该时期立法都倾向于将个人信息与人格、自由等关联在一起,甚至将其纳入私法体系。如 1976 年德国《联邦数据保护法》(*Bundesdatenschutzgesetz*)、1978 年法国《信息、档案与自由法》(*La loi n° 78 – 17 du 6 janvier 1978 relative a l' information, aux fichers et aux libertés*)以及 1992 年瑞士《联邦数据保护法》(*Federal Data Protection Act*)等,都是通过单独立法来宣称保护个人人格不受侵犯。在此基础上发展出来的国际条约或指令也将个人信息与隐私或人格自由直接关联,如欧盟于 1995 年通过的第 95/46 号《个人数据保护指令》(*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*),2000 年《欧盟基本权利宪章》(*Charter of Fundamental Rights of The European Union*)第 8 条在隐私权(第 7 条)之外,单独将个人信息受保护确认为一项“基本权利”。总体而言,早期有关个人信息保护的国内外立法是在宪法与人权保护的语境中产生的,主要针对的是公共机关对于个人基本权利侵犯的防范和国家保护义务的确认问题,但基于个人信息、隐私与个体的天然联系,在立法上又不自觉地滑入以隐私保护为重点的一个相对狭小的领域里。

个人信息保护在理论、立法和司法上始终在公法和私法、基本权利和个人私权、个人人格权和法益保护之间游移,其中充斥着大量似是而非、模棱两可的观点与论述。但私法对于个人信息保护的影响却并未消退,反而得到一定的强化,其中的一个重要契机是,信息电子化处理者由公共机关扩大到私人平台等现实中大量存在的私主体,私主体之间就个人信息利用所产生的法律关系,很容易会被纳入私法规则体系中予以调整。

环球法律评论 GLOBAL LAW REVIEW

我国立法对于个人信息保护的关注起步稍晚，主要是由民法和行政法学者贡献理论资源。民法学界基于民法学科的特点，自始即将个人信息保护置于人格权范畴下进行讨论，行政法学者则更强调国家的保护义务以及公共秩序的构建，同时与宪法和基本权利相关的理论资源都被各方援用来佐证自身观点。但民法学界的观点占据了一定的优势，并很大程度上主导了理论导向和立法选择。在2012年工信部等行业主管部门制定有关电信和互联网用户个人信息保护的相关规定时，民法学界便坚持个人信息利益的私权属性，并且在私法领域形成了纷繁复杂的观点，如人格利益说、个人信息权说、个人信息财产权说、个人信息自决权说以及上述各种观点的组合等。〔1〕私权观点对立法影响的标志性事件即是《民法典》对于个人信息保护的规定，《民法典》将个人信息保护置于第四编“人格权编”第六章“隐私权和个人信息保护”部分进行规定，个人信息因此作为一项人格利益被《民法典》确立下来。由于法典并没有采用“个人信息权”的表述，故通说认为个人信息利益没有正式被类型化为一种人格权，而应当被认定为一种“人格法益”。《民法典》对于个人信息的规定，决定了个人信息利益在私法上的基础地位，这种定位对《个人信息保护法》具有直接影响，由此民法学者倾向于认为，《民法典》与《个人信息保护法》的私法规范之间构成一般法与特别法的关系。〔2〕与此同时，公法学者并没有完全接受个人信息受私法保护的正当性或必然性，他们强调个人信息保护的国家义务及其预防功能，并看重个人信息保护与所保护的基本权利之间的区分，在《民法典》与《个人信息保护法》的关系上，有学者明确提出两者是相互平行而非交叉适用的关系。〔3〕

（二）《个人信息保护法》中的私法脉络

个人信息保护的私法面向主要体现在《个人信息保护法》的立法理念和结构体系中，成为理解该法的一条清晰线索，这主要体现在如下方面：

首先，《个人信息保护法》总则部分明确规定了立法目的和个人信息的法律界定。该法第1条和第2条明确了立法的首要目的在于“保护个人信息权益”，以防止个人信息权益被任何组织或个人非法侵害。由此个人在个人信息上存在的私法权益被法律明确承认，并成为该法的保护对象和立法基础，这与《民法典》的规定一脉相承。在个人信息的范围界定上，该法第4条明确采取“识别说”，将个人信息界定为“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个人信息”。个人信息如何界定一直是个人信息保护领域的理论难题，因为个人信息与非个人信息的划分始终没有明确标准，“可识别”标准随着技术的发展有可能会使个人信息无限扩大，故理论上还存在“关联说”“废除静态概念说”和“新识别说”等观点和方法，以应对变动不居的个人信息保护范围。〔4〕显然，通过采纳“识别说”，我国采取了传统的、静态的个人信息界定方法，与《民法典》保持

〔1〕 具体观点及相关评析参见梅夏英：《在分享与控制之间——数据保护的私法局限与公共秩序构建》，《中外法学》2019年第4期，第845－870页。

〔2〕 参见王利明：《论〈个人信息保护法〉与〈民法典〉的适用关系》，《湖湘法律评论》2021年第1期，第25－35页。

〔3〕 参见周汉华：《平行还是交叉——个人信息保护与隐私权的关系》，《中外法学》2021年第5期，第1167－1187页。

〔4〕 参见高秦伟：《个人信息概论之反思与重塑——立法与实践的理论起点》，《人大法律评论》2019年卷第1辑，第214－219页。

了一致,同时采用了“敏感信息”和“非敏感信息”的区分,其意图是参照隐私信息,为个人信息权益建立一个相对静态的、固定的空间,并对敏感信息予以重点保护。这种做法的重点是,只有个人信息与个人建立直接联系,并围绕个人形成一个大致的私域空间,个人信息权益才能获得一个相对稳定的基础。《个人信息保护法》的上述立法选择为个人信息保护奠定了一个私法保护进路的基调。

其次,《个人信息保护法》系统规定了个人在个人信息处理活动中的诸项权利。该法第 44 条至第 49 条分别规定了个人信息主体的知情同意权、查阅权、异议更正权、拒绝权、删除权等,这成为法定的个人信息权益的具体内容,与《民法典》相关内容也保持了一致。学者对于上述诸项“权利”具有工具性或技术性的色彩并不持异议,民法学者倾向于认为上述诸项“权利”乃由个人信息作为一项“人格法益”所生发,可以解读为个人信息权益的“权能”集合,而不应理解为缺乏私益基础的“权利束”。〔5〕 公法学者则普遍认为上述“权利”并不是基于民事权益而被赋予的,而只能理解为公法保护义务在具体领域的工具性手段的体现。〔6〕

《个人信息保护法》从整体理念上将个人信息与人格利益、隐私联系在一起,并大致比照隐私保护构建了相关制度:如在义务人的确定上,该法比照隐私权为个人信息保护设定的义务人为“组织和个人”,这与个人信息处理者主要体现为平台机构或政府机关、而个人一般情况下难以成为被规制对象存在一定出入;又如该法第 13 条第 5 项情形为公共利益实施新闻报道、舆论监督的行为留出合法性空间,第 6 项规定了公开信息的处理问题,这也与隐私保护的相关规则类同;再如该法第 49 条规定的近亲属对于死者个人信息权利的行使规则以及第 69 条规定的过错推定规则,也都体现出人格权或隐私权保护的基本理念。总之,《个人信息保护法》为了体现个人信息利益的私益性以及私法保护理念,在很大程度上比照借鉴了人格权或隐私权保护的相关制度,设定了个人信息保护的相关规则,以此将个人信息权益保护融于传统人格保护体系。

最后,《个人信息保护法》设定了个人信息权益保护的私法救济路径。该法第 50 条第 2 款规定“个人信息处理者拒绝个人行使权利的请求的,个人可以依法向人民法院提起诉讼”,明确将个人信息和相关权能作为私权予以诉讼救济。对于侵害个人信息的民事赔偿责任,该法第 69 条规定了过错推定规则。这两条规定都是借鉴传统人格权的私法救济而制定的。《个人信息保护法》明确了个人信息利益的私法属性,并努力采用现有的人格保护方式予以救济,这成为贯穿整部法律的一条线索,使私法理念和方法在个人信息保护领域最大程度地得以彰显。

就上面存在的问题而言,仅规定新闻报道、舆论监督合法使用个人信息,范围又过于狭窄,基于促进信息流动的需要,通常个人信息合理使用的范围应当比隐私相应的范围更广;对于已公开信息而言,其也并非必然可以被任意处理或使用,该法第 27 条对此即有限制性规定;同时,上述关于诉讼救济以及过错推定规则,也在学界存在很大争议。就第 50

〔5〕 参见申卫星:《论个人信息权的构建及其体系化》,《比较法研究》2021 年第 5 期,第 3 - 4 页。

〔6〕 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,第 159 页。

条规定而言,争议的焦点在于个人信息保护中的个人相关权能是属于民事权利,还是民事权利实现或保护过程中的技术性或工具性权利;是属于公法保护执行机制还是私法权利行使机制的一部分;且这类诉讼是否会导致滥诉、判决是否具有私权救济上的可行性和执行力等。对于第69条规定的过错推定和赔偿范围确定的规则,则又存在个人信息保护中的违法性要件可否被过错要件吸收,以及个人损失是否实际存在的理论质疑。除了上述两条规定的救济方式外,对于个人信息权益可否适用《民法典》第995条、第997条规定的人格权请求权,主流的观点持肯定态度,但也有相关学者持保留态度,认为在个人信息保护上一般性地适用人格权请求权,会使司法权前移,且造成司法权与行政权的重叠。〔7〕

通过借鉴私法上的人格保护制度来安排个人信息保护的基本理念和规则,可以有效地保护与隐私相关的信息,同时也可以弥补公共执法机关效率与能力的不足,这种立法尝试和创新是值得肯定的。但将具有浓厚公共性的个人信息完全作为一项私人法益甚至人格法益予以定位和调整,客观上会过滤掉具有结构性价值的其他维度的有益理论资源,并会积淀一些短期无法绕过且无法解决的理论症结:比如,个人信息法益的真实利益形态和内容迄今为止并未完全明晰,抽象的"人格法益"概念并不能解释已公开的或者非敏感的个人信息是否一定与人格有关,换言之,为何非电子化时代的个人信息不能进入人格权法的视野?又比如,《民法典》将个人信息和隐私一起作为人格利益予以规定,同时又将两者区分为独立的人格利益类型,会导致私密信息同时符合隐私和个人信息两种人格利益的奇怪现象。《民法典》虽然规定个人信息中的私密信息适用有关隐私权的规定,但在法律上仍然没有解决何以一项私密信息构成两种平行的、相异的人格利益,这种存在于同一领域的权利的重复和冲突在逻辑上无法被合理解释。再比如,个人信息保护肇始于电子数据库的出现,其初始目的是为了规制公共机关的信息处理活动,调整的领域属于规范公共权力行使的公法关系;其后虽然随着商业平台数据处理活动的大量出现,私主体亦一并被纳入个人信息保护视野,但是法律对公私主体个人信息保护的规制应服务于相同目的,同时也不应完全过滤掉上述公法背景而成为纯粹的私法关系。除此之外,理论上尚有个人信息保护的预防性与所保护的基本权利之间的关系如何理解等问题。〔8〕这些类似问题充斥着整个个人信息保护的各个领域,对多维度的法律理解和解释提出了现实要求。

二 社会风险控制对于个人信息保护的基础性意义

(一)社会风险控制作为个人信息保护的基础性目的

从私益角度来理解个人信息保护只是理论上的一种进路,依上文分析,这种进路会导致个人信息保护中涉及的诸多非私法因素的流失,从而使个人信息保护的理论口径

〔7〕 参见周汉华:《平行还是交叉——个人信息保护与隐私权的关系》,《中外法学》2021年第5期,第1185页。

〔8〕 参见张新宝:《论个人信息权益的构造》,《中外法学》2021年第5期,第1154页。

过于狭窄,经常面临与实际需求不符甚至“失真”的情形。对此学界往往通过公共维度的话语体系予以中和,如部分学者提出的“社会控制”或“国家保护义务”等论述。〔9〕这些论点都有很强的解释力,但很少与私法进路形成直接的交锋,即都有意无意地忽视了对一个最基础问题的回答:为何要在电子时代保护个人信息?在电子数据库形成以前,个人信息无处不在,但并没有产生任何从法律上予以保护的需求,个人信息除了隐私之外,实际上一直被置于公共领域自由流通。这是理解个人信息保护的一个前提性的事实因素,因为计算机和网络技术的出现,并不能自然地产生将传统社会非人格性的个人信息变成人格利益的对象这一如此大的飞跃。另外,西方国家保护义务理论也没有系统地论述个人信息保护的具体社会功能,如上文所介绍的欧洲关于个人信息的公约或指令等,都一再重复个人尊严、人格或自由的保护等类似表述,这实际上也成为个人信息被置于人格保护领域的另一个理论背景。但在理论上可以确定的是,个人信息保护的进一步强化与电子计算技术的出现紧密相关,且其功能也必然与电子计算机普及后产生的不利后果相关,由此对于计算机普及后产生的新型社会风险的控制便应成为个人信息保护的重要理论支点。

早期欧洲各国如瑞典、德国、法国和瑞士等制定的个人数据保护法律,主要针对的是政府机关和大型企业大规模收集电子信息可能造成的滥用或泄露等风险的防范。美国早期关于保护个人信息的措施或立法也都集中于某些风险较大的领域,规制的对象是政府、学校、医院等大型机构,以及企业的大规模个人信息收集行为,并强调个人信息的收集、披露和使用都必须遵循所谓的“合理信息实践”原则。〔10〕这些法律针对的是个人数据的收集者或处理者,而不是日常生活中的一般个体,且都是在公法领域或消费者保护范畴下来规制的。虽然随着电子平台的普及,个人信息保护的适用范围逐渐扩大,但并没有脱离原有的公法语境,个人信息保护的目的和手段也没有根本改变。

对于美国现有理论将个人信息作为“数据隐私”来保护,美国学者迈尔-舍恩伯格教授(Viktor Mayer-Schönberger)认为,20 世纪 70 年代美国数据隐私监管来自当时的数据隐私专家经过深思熟虑后提出的两个原则:一是使用数据的主体应当承担相应的风险防范责任和义务,即使用数据的组织需要对数据的使用和产生的潜在危害负责;二是避免电子数据过于集中,把数据集中在少数人手里是危险的。他认为,我们遗忘了这两个基本原则,而把数据交由个人来决定,并由个人来规避所有的风险。〔11〕事实上,社会风险防范的确是早期个人信息保护立法的实际目的,它并没有抽象地对个人信息的权利归属进行认定,而是针对电子数据大规模使用可能给社会带来的风险,而这些风险的防范责任主要应由信息处理者来承担。在风险防范前提下赋予个人信息以私权保护,事实上并不能很好地完成相应任务,可能出现的情况是,要么是通过私权行使过分控制了信息的流动,要么

〔9〕 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;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。

〔10〕 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,第 198 页。

〔11〕 参见《讲座回顾:舍恩伯格教授“人工智能的数据隐私”讲座顺利举办》,https://mp.weixin.qq.com/s/rIhnVN-TaiGZeeMIj3dYVgQ,最近访问时间[2021-11-15]。

是这种私权行使并不能有效规避信息处理者不当处理行为造成的不利后果。

在理论上将个人信息与隐私保护联系起来的一个通常理由是，个人信息的不当使用主要侵犯的是个人隐私，但这与个人信息滥用或泄露所制造的多种风险并不契合。实际上，个人信息滥用或泄露造成的风险会伤及诸多个人权利或社会公共利益。

具体而言，个人权利被侵害的风险包括：一是隐私权被侵害的风险。这是个人信息滥用或泄露最可能产生的风险，也是个人信息经常与隐私相提并论的原因。二是人格尊严或人格自由被侵犯的风险。如通过个人信息收集和挖掘整理，平台的个性化服务为追求精准营销，会引导、强化或操纵个人的偏好选择，并形成“信息茧房”，从而减少个人做出自主选择的可能性；在此基础上也存在大量的针对个人的“用户画像”，并导致对用户进行监视、操控和歧视等侵害人格尊严和人格自由的风险。三是通信自由和通信秘密被侵害的风险。在个人信息处理活动中，个人的通信自由与通信秘密可能以多种形式遭受其他主体的非法侵害。例如，处理者以个人不同意处理其个人信息或者撤回同意为由拒绝提供通信服务，则可能构成对通信自由的侵害；手机 App 等互联网应用擅自收集用户通讯录、短信内容、通话记录等信息，也可能构成对通信秘密的侵害。〔12〕四是生命健康权被侵害的风险。个人信息在网络上的泛滥大大降低了对他人进行人身伤害的成本，犯罪分子通过精准地掌握特定用户的地址、行踪、社会关系等相关信息，实施针对个人生命和健康的犯罪行为的可能性显著增加；五是财产权被侵害的风险。个人信息的泄露会导致精准诈骗、账号盗窃和敲诈勒索等侵害财产行为的大量发生，个人的财产在网络时代面临着前所未有的安全问题。

公共利益被侵害的风险则包括：一是公共安全问题。个人信息的大规模滥用或泄露会引起社会的不安、焦虑，并导致各种舆情频发。二是公共秩序问题。个人信息的不当利用会影响一个国家的基本秩序，如选民被操纵、国家秘密被泄露以及群体歧视的加剧等。三是超级平台的数据垄断问题。超级平台对于个人信息的垄断会使其利用优势地位攫取垄断租金，并且难以被社会监督和控制，其既定优势地位也会压制新创企业的成长和发展，导致经济结构失衡。

从风险防范角度分析，个人信息保护的底色应为比较纯粹的公法关系，风险防范的预防性质也决定了个人信息保护制度具有浓厚的信息管制色彩，它的目的是防止个人的基本权利或公共利益被侵害。但个人信息保护自身体现的基本价值理念，应当是个人和社会的“安全”价值，而与人格尊严和自由等基本权利本身并没有结构上和形式上的直接连结。有学者注意到个人信息保护并非保护个人信息本身，而是保护其背后的可能被侵害个人的基本权利，继而提出以背后存在的基本权利作为“本权”和以保护方式作为“本权的外部保护”，来解释个人信息权益的内部和外部结构。〔13〕这种分析的理论意义是值得肯定的，它将个人信息保护方式及其目的进行了区分，但可否基于个人信息保护的目的在于避免基本权利被侵害，而将基本权利归入个人信息权益的内在结构，则需要综合考虑。

〔12〕 参见张新宝：《个人信息收集：告知同意原则适用的限制》，《比较法研究》2019 年第 6 期，第 5 页。

〔13〕 参见张新宝：《论个人信息权益的构造》，《中外法学》2021 年第 5 期，第 1144 – 1166 页。

民法上的本权和救济权在逻辑上是权利本体和本体被保护的关系,权利本体本身应具有特定的私益内容和形式,而个人信息保护法同时防范个人的基本权利和社会公共秩序被侵害,这些公私基本利益的安全保护是否可以被置于个人信息权益的私法关系中,或者说个人信息权益能否容纳如此众多的基本权利和公共秩序等利益形态,则需要进一步观察。正是基于社会风险防范对于个人信息保护的基础性意义,个人信息受保护并不一定意味着个人对个人信息自然享有一项确定的权利,个人信息受保护也不代表个人信息一定受个人支配,而不能为社会合理分享。

(二)社会风险控制维度对解读个人信息保护基本规则的意义

如果说社会风险控制作为个人信息保护法的基础功能这一说法成立的话,那么它就一定对于个人信息保护的基础规则具有解释性和建构性意义。事实上,即使各国从隐私或人格尊严角度来论证个人信息保护,也同时都将风险防范纳入其立法考量。典型的如欧盟《一般数据保护条例》(*General Data Protection Regulation*)就体现为鲜明的"以风险为路径"(risk-based)的特征。该条例第 24 条规定:"考虑到数据处理的性质、范围、情境、目的,以及对自然人权利和自由的不同程度和大小的风险,数据控制者应采取合适的技术和组织方面的措施,以保证数据处理符合《一般数据保护条例》的规定",以及"上述措施应与数据处理的风险合乎比例,应包括在内部建立合适的数据保护政策"。这一条规定了数据控制者处理数据的风险及总体保护的一般原则,这项原则贯穿了整个条例的结构体系。又如美国联邦贸易委员会(FTC)则对于个人信息保护提出设计原则、选择原则和透明原则,在强化对数据收集和利用风险评估的基础上,采取全方位的控制,甚至对企业内部的例行工作和日常事项也提出了严格的要求。[14] 事实上,个人信息保护基于电子化时代的风险防范而生,就天然带有风险防范的基因;目前从私权角度对个人信息主要规则所做的分析和解读,也可以从风险路径得到新的解释,以下择要述之。

首先,个人信息的概念和分类带有一定的风险防范面向。从风险路径角度来理解,"可识别"标准的目的在于抑制因电子技术对巨量个人数据的过度识别,而可能造成对个人和社会安全的不必要威胁。即使如此,"可识别"标准仍然被认为不敷使用,关联说、废除静态概念说和新识别说等观点应运而生,这些观点都指向以动态的、情境化的判断来把握个人信息保护范围。个人信息由此成为变动不居、难以提前设定的概念,与自然人人格渐行渐远,但却愈加呈现出个人信息界定的根本目的,即在数据处理活动动态的、具体的场景中评估、规避和控制个人信息利用的风险。另外,个人信息的分类如私密信息、敏感信息、已公开信息或匿名信息等,也不必然是根据信息距离人格利益的远近而作出的,如敏感信息(如人脸)并不一定与隐私有多大关系,但在风险防范上却处于较高位阶;又如已公开信息大多不受人格权法的保护,但仍被纳入个人信息保护的视野,也是因为相关风险的存在。

其次,《个人信息保护法》中对个人信息权能的规定也带有显著的风险控制考量因

〔14〕 参见谢琳、祝林华:《我国个人信息保护的政府监管模式探析》,载张志安主编《互联网与国家治理发展报告(2017)》,社会科学文献出版社 2018 年版,第 104 - 118 页。

素。就个人同意规则而言,主流理论将其视为个人信息自决的核心内容,以此来正当化个人信息的私益性,但同意规则在传统个人信息领域并不存在,早期个人数据保护法中的同意规则并非私权的行使形式,而是将风险告知个人,并由个人决定是否将其个人数据置于电子和网络系统中流转利用。故"同意"并非一项对个人确定有益的权能或行为,反而是对风险的认知和主动选择,"同意"在此也就不能被理解为私法上的授权行为。在此基础上,一般同意和单独同意的区分也不完全具有私法上的意义,两种同意方式是依据个人信息利用中的风险大小来设定的。除此之外,个人信息的更正、删除和同意撤回等都具有类似的性质,即尽可能规避个人数据被扭曲或无限利用。但必须承认的是,个人信息保护权能中的查阅权和争议颇大的可携带权则并不一定与风险路径相关。查阅权尚可解释为个人对其信息的"监管",但确实与风险防范关系不大,而可携带权则更是与风险防范没有直接联系,它课以原平台更多额外义务,学界倡导可携带权的原因至今尚不明确。在数据获取权和可携带权的解释上,显示出个人信息权益的复杂性,也许个人对其数据的确享有某种特殊的新型权益,但这尚有待进一步研究。

再次,个人信息保护法确立了整体的个人数据处理规则以及数据控制主体的义务来规避风险。从个人信息权益的角度出发会提高同意制度的核心地位,但在整个风险的防范体系中,个人同意仅仅是风险控制的第一步,它只是正式开启了网络个人数据的"风险源"。真正的风险在于数据控制主体对个人数据的处理和利用上,由于建立在算法基础上的数据流通具有隐匿性和随意性的特点,难以为用户知晓和追踪,故法律在规定个人信息处理一般规则的基础上,为数据处理主体(包括国家机关)设定了多种保护义务。这些义务与网络安全法、数据安全法中的相关法律制度相互配合,尽可能减少个人信息被滥用或泄露的风险,这些原则和制度并不能由个人信息权益生发而来。个人的诸项技术性权利虽然能有效地配合相关制度降低风险发生的机率,但对于日新月异的数据处理形式如用户画像技术、算法推荐技术和人工智能学习等而言,个人控制风险的能力会越来越弱,但相关风险发生的机率却成倍增大,这客观上要求法律建立强制性的义务体系和制度来履行国家对社会公共安全的保护义务。

最后,个人信息保护领域的救济方式目前仍应以公法责任的追究为主。尽管我国立法目前规定了个人信息的私法救济和侵权损害赔偿归责规则,但在司法实践中会遇到巨大障碍。就个人信息保护中技术性权利的可诉性规则而言,其会面临司法权与行政权的职能交错问题,案由的确定和判决的执行都与传统私权救济原理相左。对于侵权损害赔偿而言,面临的实际难题是在大多数情况下,个人信息的非法利用并没有产生实际的损害,故司法上倾向于强调精神损害的存在,且有学者提出有条件地承认个人信息的"预期侵权"制度来对"损害"进行评估确认。[15] 这些做法都是在承认个人对个人信息享有私益的基础上,在逻辑上完善私法救济的理论努力,但在强调若有若无的"损害"的同时,却忽略了个人信息保护的风险防范目的。在目前的司法实践中,私法救济效果不彰,并不能

〔15〕 参见谢鸿飞:《个人信息泄露侵权责任构成中的"损害"——兼论风险社会中损害的观念化》,《国家检察官学院学报》2021 年第 5 期,第 35 页。

很好起到规避风险的作用。公法责任的追究是个人信息保护的主要方式,而强调通过行政执法并课以巨额罚款来阻吓数据处理者的违规行为。法律对个人信息保护的力度甚至强于对隐私的保护,这种结果有悖于民法上的个人信息和隐私对人格重要性的梯度递进,在人格权法上令人费解。究言之,这种保护上的差别实则归因于风险控制因素,即个人信息大规模不当利用造成的风险远远超过个人隐私被不法侵害的后果,前者须通过对违法行为的严厉惩罚来预防风险,后者通过正当的民事责任追究即可得到保护。

三 风险路径与个人权益路径在主要问题上的不同态度

从个人权益和风险防范路径来解释个人信息保护的目的和规则体系,都有各自的合理性,甚至风险路径的解释力有时更直截了当,这就在理论上提出了如何理解两者的关系这一问题。实际上也可以理解为,个人信息保护法主要体现的是信息管制法还是个人权益保护法,对此公法学者和私法学者之间的观点差异较大。鉴于两种路径都是从自身可解释的领域来正当化自身主张,故有必要通过揭示两种路径在主要理论问题上的分歧来进行综合判断。

(一)个人信息与隐私的基础关系

个人信息与隐私的关系是个人信息保护的基本问题。从概念分析,隐私信息属于个人信息,且隐私信息的保护适用传统人格权法的保护方式。对于隐私信息之外的个人信息是否属于人格利益所及范围的问题,我国《民法典》明确认定其依然属于人格权法保护范围,换言之,隐私之外的个人信息构成人格利益的一种新类型。但民法上的这种划分和认定并未体现在个人信息保护的相关法律中,比如 2016 年通过的欧盟《一般数据保护条例》修正了 1995 年《个人数据保护指令》的做法,将个人信息与隐私分开,不再相互参照。我国《个人信息保护法》和《消费者权益保护法》等亦采取类似做法,不再在相应法律中使用隐私概念,亦即隐私信息作为个人信息可以受相关保护性法律保护,亦不影响其同时受人格权法保护,有学者据此称之为个人信息和隐私的“平行保护”。但《民法典》又将个人信息置于人格权保护范围,由此产生了个人信息和隐私保护的交错,故又形成了“交叉保护”的态势。〔16〕 由此,平行或交叉保护成为个人信息和隐私关系的争议焦点,这就又回到非隐私性的个人信息是否有必要纳入私法保护范围这一问题。

主张平行保护的观点认为,交叉保护将隐私和个人信息都作为人格利益对待,且分属不同的人格利益类型,将会导致隐私同时归属于人格权法中两种不同人格类型的对象,却又只适用隐私权保护方法这一矛盾结果,使人格权的结构和规则适用产生混乱和矛盾,同时还会导致人格权保护规则系统性地影响个人信息保护,因为很多人格权法规则(如人格权请求权)与公法调整的逻辑并不相符。〔17〕 主张交叉保护的观点则认为,个人信息通

〔16〕 参见周汉华:《平行还是交叉——个人信息保护与隐私权的关系》,《中外法学》2021 年第 5 期,第 1175 – 1186 页。

〔17〕 参见周汉华:《平行还是交叉——个人信息保护与隐私权的关系》,《中外法学》2021 年第 5 期,第 1174 – 1175 页。

过人格利益受私法保护具有正当性,且《个人信息保护法》作为特别法应与作为基本法的《民法典》保持一致,另外个人信息的私法保护和公法保护并不冲突。[18] 上述两种观点都有其论证上的合理性,但一定程度上忽视了风险防范对于个人信息保护的影响。依上文分析,这些风险并不一定与隐私或其他人格利益相关,也可能与经济利益有关,故个人信息是否一定要与隐私相提并论仍然值得研究,另外个人信息是否成为私益标的或人格利益类型,也要在这种权益是否有利于消除个人电子数据利用产生的社会风险这一基础背景下进行充分说明。

(二)一般性保护与场景化保护

将个人信息权益作为人格法益来定位,客观上会倾向于强调个人信息的一般性保护,如保护对象同时包括电子化信息和非电子信息,义务对象既包括公共机关、企业,也包括个人。《个人信息保护法》第2条、第4条对此予以确认。但就个人信息保护规制的主体而言,世界各国的立法倾向于只适用于特定领域和特定对象。如美国的个人信息保护措施和相关立法带有明显的消费者法保护或公法规制的特征。再如,1977年德国《联邦数据保护法》针对的也是个人数据的收集者或处理者,而不是日常生活中的一般个体;[19] 欧盟《一般数据保护条例》将规制对象定位于"数据控制者",在此之前的新加坡2012年《个人数据保护法》(*Personal Data Protection Act*)也仅仅涉及"组织机构"的行为,对于个人或家庭行为、员工的职务行为以及政府部门行为中涉及的"个人数据"不予干涉。

将个人信息保护限于特殊的数据处理者和电子数据的场景,说明个人信息保护的目的并非针对抽象的个人信息,而是特殊主体对特殊信息形式的处理行为,其目的仍然与风险控制直接相关。风险源于何处,便应止于何处,这也是有学者反复提及的"场景主义",即个人信息保护应是通过对不平等信息关系的干预来体现合理信息实践原则,通过信息处理的公开、告知和预防,在具体场景中实现个体和国家的有效参与,以最大程度地降低电子技术造成的社会风险。[20] 这种场景化保护图景与一般性保护的最大区别在于,后者从普遍化和形式化的个人信息权益出发,以个人信息内容为锚,将所有主体对所有形式的个人信息利用纳入抽象的私权行使和保护领域,这种平等关系的横向调整与前者基于公共风险防范的纵向调节形成鲜明的纵横交错的关系。

(三)私法救济中损害的有无与确定

个人信息公私法救济在目前的主流理论中是相互共存、互不矛盾的。类似于民事权利的公法和私法保护,公法通过刑事责任和行政责任、私法通过民事责任来共同对个人信息民事侵权行为进行制裁。但在个人信息侵权的民事救济尤其是损害赔偿责任上,侵害个人信息权益是否存在法律上的"损害"一直是司法实践上的难题。在绝大多数情况下法院无法确定经济损失,事实上,个人信息的不当利用只是增加了个人受实际侵害的风险

〔18〕 参见王利明、丁晓东:《论〈个人信息保护法〉的亮点、特色与适用》,《法学家》2021年第6期,第15页。
〔19〕 参见丁晓东:《个人信息保护私法困境与出路》,《法学研究》2018年第6期,第200页。
〔20〕 参见丁晓东:《个人信息保护私法困境与出路》,《法学研究》2018年第6期,第204页。

和机率,信息处理本身并没有造成实际损失。至于以信息处理者所获利益来确定损失,也存在很大的争议,它需要充足且直接的因果关系基础,也与数据处理者利益获得的多要素性和个人信息对收益获取的或然性并不完全契合。

从风险防范路径角度来观察,个人信息侵害实则体现为数据处理者因处置失当而制造了相应的风险,风险本身并不必然体现为现实损失,甚至与隐私权被侵害时精神上的痛苦或焦虑亦无直接关系。非私密性的个人信息与隐私不同,它本身可以进入共享领域,只是可能产生不当风险,故个人数据本身不应被视为直接保护对象,数据处理行为才应是关注的重点。在这一问题上,学界注意到西方国家隐私侵权中“合理期待”(reasonable expectations)理论的发展,并期待这一理论能在个人信息保护中发挥作用。合理期待理论的核心是,在信息主体与信息处理者之间设定权利义务关系时,需考虑信息主体在特定场景下所可以合法享有的期待。〔21〕 但隐私保护与非私密个人信息保护的一个显著区别是,隐私的合理期待体现为确定相应信息或空间成为隐私范围,个人信息的合理期待则体现为对于何种信息处置行为制造何种风险的判断,其法律后果也会有较大不同。在此前提下,风险防范导向下的责任追究倾向于关注信息处置行为的非法性认定,并通过刑事责任和行政执法来遏制风险的产生和蔓延。基于此,公法上行为的违法认定与私法上过错的认定产生了交错,《个人信息保护法》第 69 条规定的“过错推定”规则并非严格意义上的损害赔偿规则,在公法保护义务作为个人信息保护主要背景的前提下,过错吸收“违法性”的做法在风险防范意义上并不能完全适用,相反强调违法行为的存在且以“过错推定”来增强违法性的认定,才符合个人信息保护中风险防范的宗旨。

除了上述三方面的根本分歧外,风险路径和个人权益路径在个人信息权益与个人信息保护权的确定上也持完全不同态度。在理论上究竟是因为个人信息人格利益的前提性存在衍生出个人信息保护问题,还是因个人电子数据利用中外部性的发生促使“个人信息保护权”的产生,都具有理论上进一步探究的余地。另外,在个人信息人格利益模糊且大多可以通过风险路径或外部性理论解释的前提下,个人信息权益的核心内容究竟如何认定或表述,它与隐私性人格权或其他人格权的区别如何,甚或这种权益具有何种独立的人格意义,都需要在理论上进一步明晰。

四 风险防范维度与《个人信息保护法》的实施

对《个人信息保护法》的两个分析维度进行的比较探讨,有助于我们在整体上从多重视角来理解该法的立法背景、意旨和目的,也有助于该法的科学实施。基本而言,判断一部个人信息保护法是否成功,在于该法是否能够实现三个基本目的,即:充分保护个人信息权益、有效规避各类风险以及合理促进信息利用,这三者既相互支撑亦相互制约,立法

〔21〕 参见石佳友:《隐私权与个人信息关系的再思考——兼论私密信息的法律适用》,《上海政法学院学报》2021 年第 5 期,第 8 页。

上最好的结果是三者达到最优组合,以实现社会效益的最大化。在个人权益保护占据优势地位的前提下,就有可能对个人信息施以较强的控制,而忽视其他两个目的的合理实现。《个人信息保护法》设置了许多涉及信息处理的相关义务,但除了个人信息权益保护这一目的以外,这些义务却并没有形成与风险预防或信息利用之间的直接联系,同时违反该义务的责任亦缺乏足够的衡量标准,这样从形式上就无法将个人信息权益打造成一个向上与基本权利或人格尊严联结、向下与数据技术处理贯通,对信息内容和形式同时进行保护的"超级权利",这便是从单一维度理解个人信息保护的结果。上文就两种维度所做的分析涉及到各种层面,个人权益保护的路径虽然对于个人信息权益的定性和保护价值有一种指引作用,但是与个人信息保护的层次和预防力度并不能形成逻辑对应的关系。基于此,在法律的实施中,有效地将风险路径纳入法律理解和执法衡量视野,是合理实施该法的必要举措。对于我国《个人信息保护法》而言,这种视角和态度能够在两个方面作出有益的贡献,即在风险大小与数据控制程度之间的合理匹配上进行细化衡量,以及在风险防范相对充分的情形下,合理释放信息的流动性。

(一)风险评估与数据控制力度的合理匹配

我国《个人信息保护法》借鉴了欧盟《一般数据保护条例》的大量规则,总体上遵循了风险与控制力度相一致的做法,但鉴于立法理念和导向的不同,风险防范与数据控制之间的匹配尚有解释和调整的空间。具体而言,法律实施中会存在对较高风险施以较低防范措施,以及对较低风险予以较高防范措施等两种情形。就前者而言,我国《个人信息保护法》中存在诸多情形,在此列举几例:

一是关于数据安全事件,该法第 57 条仅规定,发生或可能发生个人信息泄露、篡改、丢失时应当通知相关部门,原则上不通知个人。这种处置方式和力度与风险程度相比略有不足。在数据安全事件已然发生时,高风险的应对防范甚为必要,此时应将风险扩大到该条规定的情形之外的其他风险,同时应对信息处理者确定一个较短的通知时间,责令其将采取措施的过程和预期效果等内容报告监管机构,并对例外情形予以设定。

二是《个人信息保护法》第 45 条对于数据迁移的规定,赋予了个人行使可携带权,且无相关限制。但数据迁移会带来的一系列风险,如第三方隐私保护、数据安全和市场竞争的失序等,这要求执法监管机关对其合法性基础和限制性情形作出实践性应对。

三是《个人信息保护法》第 26 条对图像采集和个人身份识别作出了限制性规定,与在此之前最高人民法院有关人脸识别的规定相呼应。人脸识别涉及的并不完全是人格权的问题,它属于敏感信息,且具有唯一性、易收集和无感知性等特点,一旦被他人非法利用,就有可能对个人的隐私、财产或公共安全造成极大风险,故法律应对其使用进行严格限制。欧盟 2021 年 10 月对于公共场所人脸识别全面禁止,实际上将《一般数据保护条例》的相关规定缩紧了。尽管《个人信息保护法》第 26 条作了相关限制性规定,且以"单独同意"作为公共目的之外使用的前提条件,但与此种高风险相匹配的限制条件仍然不足,对于人脸识别的利用原则上应当更加慎重。

就对较低风险课以较高防范措施而言,在《个人信息保护法》之中也不乏其例,需要

环球法律评论 GLOBAL LAW REVIEW

在司法和执法过程中予以关注:一是对于死者个人信息的保护失之过严。《个人信息保护法》第 49 条允许近亲属对死者的相关个人信息行使相关权利,在世界立法上少有先例。比如,欧盟《一般数据保护条例》不适用于死者的个人数据,成员国可以对死者个人数据处理自行作出相关规定。欧盟各成员国的立法均未明确死者的个人信息保护问题,或明确规定不适用于死者的个人信息;加州隐私法也未对死者的个人信息保护作任何规定。有些国家虽然对死者的个人信息保护作出了相关规定,但也存在一定的限制。例如,2018 年的《丹麦数据保护法》(*Data Protection Act*)第 2 条第 5 款规定,该法与欧盟《一般数据保护条例》适用于死者死后十年内的个人数据的保护。死者个人信息上的人格性较弱,其上存在的社会风险不大,但他人行使相关权利造成的风险却不容忽视,即近亲属行使权利时有可能涉及第三人隐私,并从事相关背俗行为或违法行为。二是关于"去标识化信息"的界定范围失之过宽。《个人信息保护法》第 4 条将匿名化信息排除在外当无疑义,去标识化信息仍应属于个人信息保护的对象。我国的去标识化信息保护内容过宽,其中一部分信息因经有效技术处理,虽可以复原但仍然具有相应的保密性,在欧美国家被认为风险可控,故被排除在保护之列,此种做法亦值得我国借鉴。三是关于《个人信息保护法》中规定的特殊情形下用户的"单独同意"制度。应当肯定"单独同意"规则针对的是风险较大的领域,如敏感信息的使用、向他人提供信息等场合,该规则有利于有效控制风险。但在数据控制者和用户的利益格局既定的情形下,单独同意规则在电子化领域并不能明显增加用户的自主性,且会导致实际操作的困难和成本的提升。另外,在需要用户明确同意的高风险数据利用场合,用户的单独或书面同意只是风险防范的第一步,真正控制风险的主要领域在于数据处理者的合规体系和行政监管体系,在风险尚未实际开启的起始阶段使用单独同意规则,可能会影响信息的收集和流通。除了上述相关情形外,尚有其他值得探讨的事例,在此不赘述。

环球法律评论 GLOBAL LAW REVIEW

(二)风险可控前提下的信息流动性释放

总体来看,我国《个人信息保护法》对社会风险采取了强监管的立法态度,更接近欧盟《一般数据保护条例》的立法理念,但同时又强调个人信息权益为该法的基础,对个人信息保护赋予了双重任务,加强对个人数据的各种控制便成为通行做法。但数据控制并非个人信息保护的根本性目的,在数据处理风险可控且用户权益能得到有效保护的前提下,可以采取相对宽松的做法来释放信息的流动性。试述几例说明。

首先,关于个人信息保护的适用范围和排除适用规则,《个人信息保护法》第 4 条规定:"个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等";第 72 条则将"自然人因个人或者家庭事务处理个人信息"排除在该法保护之外。该法对适用其保护的数据活动范围规定得很广,而排除适应的情形则相对较窄。事实上,个人信息保护的适用范围并非越宽越好,个人权利保护和风险控制也只能接近最优水平,不可能面面俱到。在法律实施过程中,应将企业的数据处理放在重点领域予以监管,适度放宽对新创中小企业的相关要求,同时在特定信息领域发挥部门法的作用。

其次,关于数据处理的合法性基础,《个人信息保护法》第 13 条进行了列举式规定,

分列了七种情形，相较其他国家立法偏于严格。美国对于数据处理规定择出（opt-out）机制作为合法性基础，也并未限制其他方式，是最宽松的保护方式。欧盟规定的内容则与我国类似，但在具体表述和范围界定上有所不同。比如《个人信息保护法》第13条相比于欧盟《一般数据保护条例》的相关内容而言，所列举的范围较后者的一般性规定更狭窄。实则涉及公共利益的情形甚多，诸如科学研究、社会统计、法律程序以及信息表达自由等都应属合法情形之列；另外，对于合法侦测数据安全事故、修正信息预期功能的错误等均应纳入合法利用情形。

最后，《个人信息保护法》第47条规定了用户享有删除权的情形，并将“法律、行政法规规定的保存期限未届满”和“删除个人信息从技术上难以实现”作为该条的例外情形。比较欧盟《一般数据保护条例》和《加州消费者隐私法案》（*California Consumer Privacy Act*）、《加州隐私权法案》（*California Privacy Rights Act*），我国立法规定的例外情形较少。前述条例与法案中规定了言论自由、法律程序、公共健康、科学研究和履行法定职责等作为删除权行使的例外情形，《加州消费者隐私法案》和《加州隐私权法案》还将履行合同所必需、侦测安全事故、调试以识别和修复损害现有预期功能的错误、符合消费者预期的内部使用等都作为删除权行使的例外情形。这些例外情形在《个人信息保护法》中并未列入排除规定，致使实践中相关的信息资源因被删除而无法被有效利用，上述域外立法对我们在实践中有效地平衡个人和企业的利益具有参考意义。

环球法律评论 GLOBAL LAW REVIEW

五 结语

本文关于风险评估与防范措施相匹配的分析，及其对信息流动优化的积极意义，只是从风险维度对个人信息保护法实施提出的局部分析和建议，并非本文的初衷和落脚点。个人信息权益与风险防范作为理解个人信息保护法两个不可或缺的维度，有利于我们科学解读个人信息保护的相关制度和规则，并对个人权益保护路径的优点和不足予以合理判断。世界范围内的个人信息保护法都从不同维度探寻完善个人信息保护的路径，这些路径之间并不是非此即彼或彼此排斥，都是在立足一个主要的价值面向或出发点进而统摄与涵盖所有可能的方式方法。从目前来看，为更好实现个人信息保护的公共目标和功能，风险控制维度的价值选择或许更优。就我国情况而言，鉴于《个人信息保护法》已经生效，在实施该法的过程中，尚有可能通过制定实施细则或司法解释对相关规定予以细化调整，以从风险控制的维度充分实现个人信息保护的价值目标。随着网络技术和应用业态的发展，新的风险会陆续出现，也同样会随着技术发展而迭代更新，给人类带来新的挑战。因此，风险维度的思考和建构方式将会在此领域发挥越来越重要的作用。申言之，对于个人信息权益存在与否，法律一次性予以确认即可，而且对于成文法国家而言，法律具有稳定性的同时也可能相反意味着一种固定不变或者较为机械，而未来个人信息利用所面临的风险，却可能是无法预测甚至是无穷的。是以，风险维度的思维与制度建构就更具有重要意义，殊值重视。

［**Abstract**］ Chinese Civil Code recognizes personal information as a kind of personality legal interests, thereby establishing the private law protection orientation of personal information in theory and legislation and making the protection of personal rights and interests an important dimension of and a clue to the construction and understanding of personal information protection. Personal information protection laws around the world have sought to improve the path of personal information protection from different dimensions, and these paths are not mutually exclusive, but are all based on a major value orientation or starting point, which in turn covers all possible ways and means. At present, the public objectives and functions based on personal information protection cannot be covered or eliminated by the approach of personal private interest protection, so it is necessary to recognize social risk control as an important dimension of personal information protection. Social risk control has always been the basic objective of personal data protection in the electronic era. It has a strong explanatory power and plays the role of dynamic construction in the relevant theories and systems of personal information protection. There are contradictions between the social risk control approach and the personal rights protection approach on some basic issues, such as the basic relations between personal information and privacy, between general protection and scenarized protection, and between the right itself and the protective right. In the future implementation of the Personal Information Protection Law, the social risk control approach is conducive to reasonably interpreting and implementing the law, achieving the reasonable matching between the scale of risk and control measures, such as the matchings of different risk dimensions and corresponding restrictions for data security, data migration and facial recognition. In the meantime, the mobility of information should be released on the premise of balancing the relevant legislative values. For example, for the application scope and exclusion rules of personal information protection, the right to deletion of personal information subjects and the legitimacy basis of personal information processing, the corresponding application scopes and exclusions should be balanced according to the corresponding risk matching degrees. In short, with the development of cyber technology and its application, new risks continue to emerge, are iteratively updated along with technological development, and bring new challenges to humanity. The method of thinking and construction of risk dimension is very important in the field of personal information protection, because the law can only confirm and regulate the existence of personal information rights and interests once, and for the states of continental law system, the stability of law may conversely imply a rigidity, but the risks in the use of personal information are unpredictable or even infinite. Therefore, the thinking and institutional construction in the risk dimension i s more important and worthy of attention.

环球法律评论 GLOBAL LAW REVIEW

（责任编辑：姚 佳）