

新科技时代个人信息保护法的适用出路

冯 恺

(中国政法大学比较法学研究院,北京 100088)

摘要:在新科技发展背景下,如何保持我国《个保法》的适用活力是一个重要命题。场景化应用和领域化方案为《个保法》的适用提出了新的思路。然而,尽管场景化应用以其适用上的张力迎合了《个保法》的特定需求,其与成文法规范之间存在内在冲突,不宜成为普适性方案。领域法方案具有特定的法律价值,但其难以实现自身的独立性和体系性,与部门法及相关领域法之间的关系不易协调,无法塑成统一的行为范畴,客观上面临一系列实践障碍。借由现有的两种适用路径,《个保法》仍能有效地应对诸多新生问题:一是基于法释义学的方法,结合特定立法目的对《个保法》中的一些基本范畴作出扩展性解释;二是通过司法适用技术将新规则嵌入既有制度框架,并重视法官自由裁量权的行使。

关键词:个人信息保护法;场景化应用;领域法;法释义学;司法适用技术

中图分类号:D923.8 **文献标志码:**A **文章编号:**1009-1505(2023)06-0056-10

DOI:10.14134/j.cnki.cn33-1337/c.2023.06.006

我国《个人信息保护法》(以下简称《个保法》)的出台是数字科技迅猛发展背景下对“百年未有之大变局”的制度应对,也是对近十年来相关学术研究及司法实践问题的全面回应。然而,尽管立法上可以因一部法律的通过而实现从无到有的快速跨越,但是司法实践上仍需要一个循序渐进的消化和吸收过程,以最终实现《个保法》与现实问题的衔接。与此同时,数字科技的发展超乎想象,从互联网、大数据到更为精细的人脸识别、算法、区块链,又快速迈进到元宇宙、机器学习和自主型人工智能时代。新科技作为一种“替代性”和“超能型”力量,不仅意味着以数据和算法为表征的技术力量的宰制,而且意味着对人类社会活动之规范性意义的重新理解和价值实践的挑战^[1]。那么,如何在既有法律框架内通过更具灵活性的适用方案,使《个保法》得以应对更为复杂的科技衍生问题,仍有待理论上作出进一步探究。

此外,《个保法》的立法目的是为个人信息处理相关问题提供法律依据,增强适用上的确定性。然而,该法的出台并未完全消除此前的所有问题,例如,公私法之争尚未偃旗息鼓,关于个人信息权利属性之论辩仍在持续。尤其是,借由何种适用路径方能使得既有规则有效应对新科技背景下不断涌现的新问题,对新出台的《个保法》亦构成挑战。从目前研究来看,多数学者坚持法释义学的方法,通过对

收稿日期:2023-05-12

基金项目:国家社会科学基金一般项目“未成年人个人信息保护立法研究”(19BFX151)

作者简介:冯恺,女,中国政法大学比较法学研究院教授,博士生导师,法学博士,主要从事民商法研究。

《个保法》规则的扩展解释以应对新的问题。也有部分学者提出了更具跃进性的方案,其中包括场景化应用及领域法理论。相关方案在特定方面与《个保法》的属性相契合,在理论上亦具有一定自洽性,然而,其对《个保法》适用的效果如何?有无必要打破既有制度安排作出大幅度的调整?本文拟对场景化应用与领域化方案之优劣予以探究,进而审视《个保法》既有适用路径的合理性,以期在制度的守成与求新中获得良性平衡。

一、《个保法》场景化应用之优劣

场景理论的提出为《个保法》应对新问题提供了一个开放性方案。学者认为,个人信息本身即具有高度的场景依附性,个人信息与非个人信息的界分“经常是场景化”的^[2]。因此,数据的个人性“不应被视为数据的属性,而应被视为数据所处场景的属性”^[3]。此种场景化观念为欧盟法所认可,例如,欧盟第29条数据保护工作组发布的“关于个人数据概念的意见”指出,某些标识符是否“实现识别,这取决于特定情况的场景”。^①场景理论近年来也日渐成为我国个人信息保护理论研究成果中较具影响力的学说之一,并呈现一定扩张之势。

(一) 场景化应用的入口

早在构建个人信息保护法律体系的过程中,一些学者便已意识到相关制度的法律适用困境,并进行了一系列场景化应用的尝试,从引入场景理论到提出更为具体的动态同意及个人信息概念的场景化等方案,意图为《个保法》的制度适用提供一个更具弹性的路径。

场景理论最初是作为对个人信息保护问题的整体应对而“一揽子”引入的。依据海伦·尼森鲍姆提出的隐私场景公正理论,教育、政治、消费、社交、面试、医疗等生活领域皆发生在由信息构成的场景中,在不同场景中的信息处理应该受到不同的约束^[4]。因此,对于个人信息并非要进行统一与标准化保护,而是要寻求与“具体场景相关的信息规范”(Context-relative Informational Norms),维护具体信息关系与生活秩序的公正性或融贯性(Integrity)^[5]。在立法层面上,欧盟2018年颁布的《通用数据保护条例》以场景为导向,重视风险评估,引入了数据泄露通知、隐私评估、第三方认证等新机制。2015年美国《消费者隐私权利法案》亦引入了“场景”的范畴,规定仅在信息处理场景不一致的情形下,消费者才享有同意权,同意从一般适用走向例外适用^[6]。在一定意义上,场景理论因其更具灵动性而在个人信息保护法的若干核心规则中得以阐释和适用,其中较具代表性的为动态同意主张与个人信息概念的场景化。

将场景理论应用于同意制度的基本动因是:传统的知情同意制度在个人信息领域的适用遭遇一定困境;同意作为个人信息处理的合法性基础之一,其规则并非不可动摇。20世纪90年代至今,从分布式计算机时代进入大数据时代,科技革命带来信息处理模式的根本变化,导致原有的强同意模式已不再适宜^[7]。为了克服同意制度既有的僵化性,研究者试图从场景化的视角提出改良性方案。有学者认为,诸如行为、环境、时空、设备的场景要素都会影响数据处理的敏感程度,社会习俗、法律责任、风险控制能力等规则遵循情况也在形塑着数据主体的隐私期待和对数据处理风险的容忍度。因此,应基于场景变化适用同意规则,在涉及敏感信息处理、自动化决策等特定场景时须征得信息主体明确同意,但在符合情境合理测试的情形下允许适用拟制同意^[7]。有学者提出的有限告知同意论中亦蕴含着场景化应用的理念,其认为,应遵循情境完整性理论采用客观化的确定标准进行类型化展开,在不同情境中实行择入式或择出式同意,同时考虑到合法公开的个人信息的双重属性,衍生利用风险系数高于

^①Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data, 01248/07/EN. WP 136.

未公开的个人信息^[8]。儿童个人信息的处理即是动态同意适用的一个范例:当服务出于内部目的使用儿童数据时,允许采用较为宽松的同意机制;但如果服务是向第三方披露个人数据并使得儿童信息被公开的高风险服务,则必须遵守更为严格的同意机制,父母须通过邮寄、传真或扫描等更正式的方式填写和返回同意表、提供信用卡号码、通过电话或视频会议联系服务提供商及核实身份^[9]。

在更为新近的研究中,有学者进一步提出了个人信息概念场景化的主张,认为应在符合社会场景目的的情形下处理个人信息^[10]。有学者主张将某一信息还原到具体的信息关系与信息实践中,而相关信息的属性如何界定,往往取决于这一信息是被用于何种用途、被谁识别、多大概率被识别、被识别的风险等场景性因素,例如,对符合识别目标的信息作更广的界定,对不符合识别目标的信息作更窄界定;分析识别的可能主体,根据较为可能识别的主体而判断个人信息的可识别性;分析个人信息被识别的概率,结合非技术人员预期与技术人员预期而判断信息被识别的可能性^[11]。相关主张进一步丰富了《个保法》的场景化应用。

(二) 场景化应用的特定价值

一定程度上,场景化应用方案以其适用上特有的张力迎合了个人信息保护的特定需求,有利于平衡不同信息主体之间的利益诉求,从而能够更好地应对科技发展带来的新问题。其法律价值主要表现为如下几个方面。

首先,场景化应用强调结合具体的场景进行针对性保护,有助于防控具体的而非抽象的风险,避免笼统泛化个人信息的保护^[12]。以动态同意在儿童个人信息处理中的适用为例,若是基于信息处理者的服务目的及风险大小来区分保护的强度,避免针对所有处理儿童个人信息的情形一概采取严苛的同意机制,则能够在保护儿童这一特定主体的同时兼顾个人信息处理者的合理商业利益。

其次,场景化应用有助于维护既有个人信息保护框架的确定性和统一性。从表面看来,场景化保护方法依赖于个案审查,是动态的、灵活的;究其目的,却恰恰是避免个人信息保护规则僵化所带来的恣意性,通过案例与程序化解“非规则型法”所带来的适用挑战,构建动态但相对确定统一的个人信息保护规范^[13]。就适用结果而言,场景化应用使得一些新生问题得以在既有个人信息保护法制度框架内得以解决,而无须重新设定新的规则。

最后,场景化应用意在平衡不同信息主体之间的利益关系。对信息处理参与主体的利益平衡,意味着需要动态地评估信息处理给各方带来的风险,多维度地考察各方主体在信息处理过程中的责任分配,兼顾信息参与主体的利益,增强各方主体保护个人信息的激情,将保护个人信息变成信息处理者的内在需求^[14]。场景理论极具兼容性,可以考量多元要素互动,注重信息流动规律,规范参与场景主体行为,平衡各方利益^[15]。

(三) 场景化应用的内在局限性

场景化应用得以尽可能保有既有信息制度的外观,通过评估特定场景因素(如风险评估)克服《个保法》相关制度的适用局限性,矫正其功能减损的不良趋向,有助于缓和既有制度与新生问题之间的矛盾。然而,场景化应用方案在《个保法》适用背景下展现了难以克服的内在局限性。

针对场景化应用理论的一个质疑是:场景化保护可能不符合《个保法》的成文法特征,并且导致其规则形同虚设^[13]。一方面,场景化的目的是维护既有个人信息保护框架的确定性和稳定性,但由于它依赖于个案分析,当法官在司法实践中过于强调场景化应用甚至予以滥用时,客观上会引发法律的不确定性。另一方面,鉴于场景化理论的抽象性,其实践过程中要求设立一定的“场景要素”,包括信息识别的主体或概率、信息处理的目的、风险评估标准及其他影响因素。例如,美国《儿童在线隐私保护法》(COPPA, §312.5)要求根据被处理信息的“使用目的”(是内部使用还是用于商业目的)来评估应否取得监护人同意;2011年欧盟第29条数据保护工作组提出了“浮动比例尺”方案,建议根据被处理个

人信息的“类型、处理目的以及最终风险”等多种因素来判定儿童作出同意是否有效。^①此种“场景因素”因个案的不同而存在差异,难以形成统一的标准。因此,场景化应用实践中需要另行缔造出新的规则 and 标准,事实上推动了“个别化立法”,若是不加限制,便会在客观上抵消通过场景化应用“维护既有制度外观”和“简化新问题适用”的部分努力。

场景化理论应用于《个保法》的特定制度时亦显现了一定弊端。例如,在动态同意的制度设定下,主体反复给予或撤回同意而影响信息处理效率,从而造成资源浪费和成本增加^[16]。动态同意说虽然主张信息主体可以选择个性化的偏好设置,但是对如何实现这种设置付之阙如^[17]。场景化应用本身的一系列局限性意味着:这一方案仅适用于依据某种“场景因素”作出具体评估的特定情形,虽有助于应对《个保法》适用中的特定问题,但不宜成为一个普适性方案。

二、领域化方案于《个保法》之适用可行性

为了应对数字科技的冲击,一些学者主张放弃“部门法”思维,转向“领域法”思维。此种思维以问题为导向,采“诸法合一”的姿态,运用“领域性整合”模式和“问题—经验—逻辑”一体化实用型思维以及立体化解释与应用体系,来构造一种包容性范式^[18]。此种思维表现在学科上也即“领域法学”,是以特定经济社会领域中与法律有关的现象为研究对象,融经济学、政治学和社会学等多种研究范式于一体的整合性、交叉性、开放性、应用性和协同性的新型法学理论体系、学科体系和话语体系^[19]。《个保法》是专门规制个人信息保护问题的一部法律,它兼具公民法属性,并非直接从哪个具体的部门法剥离而来,无法直接归于某个部门法的统领,在形式上满足“领域法”的要件要求。然而,领域化方案能否成为《个保法》的一个更优适用路径,其可行性仍有待检验。

(一) 领域化方案的主要价值

领域法主张以问题领域来整合不同法学部门、学科和法律规范,而非以部门法、分支学科来拆分性地回应问题领域,其研究旨趣不仅是要拨开多元复杂的领域法律现象的“面纱”,揭示隐含于其中的规律或机理,而且是要在此基础上推动各个领域之重大法律问题的有效解决^[18]。它在一定程度上弥补了部门法学以“调整对象”或“调整方法”为划分标准的局限性,更好地应对新型交叉领域的问题^[20]。同时,领域法学强调传统与现代、历史与现实相融合的思维方式,强调对法律问题的“主体性中国”思考^[19]。因此,领域法理论的提出被视为新科技发展背景下应对《个保法》适用新问题的一个积极方案。

个人信息保护法作为一个新兴学科,是多个部门法规则的融合,难以直接将其纳入任意一个传统部门法。若是通过领域化方案赋予个人信息保护法与其他学科平等的独立学科身份和平台,客观上能够纾解其作为新兴学科的“身份认同”困境^[18]。如此,它不再受制于公法或私法之所谓部门法系属之争,而得以根据本领域自身的特点设定相关适用规则。领域法所倡导的问题化导向,亦有助于研究个人信息法制的不同部门法学者摒弃门户之见,基于所在具体学科的经验对个人信息法制这一主题作出积极回应,促进这一新兴领域问题的系统化解决。

(二) 领域化方案的适用障碍

领域化方案旨在另辟途径,较之传统部门法的适用路径具有一定优势。然而,它迄今为止仅是一个理论上的畅想,旨在厘清在方法论层面关于领域法学的若干前置性议题^[21],能否将其视为《个保法》的一个适用性方案仍存在诸多质疑。领域法学的支持者也多为法理学者,其更多地从理论而非规

^①Article 29 Data Protection Working Party. Opinion 15 /2011 on the Definition of Consent, 01197/11/EN. WP 187.

则适用层面上提出构建思路。概言之,领域化方案远未进入实践应用阶段,其理论本身依然存在一定局限性,将其作为《个保法》的适用路径仍存在明显的现实障碍。

首先,领域法学难以实现其自身的独立性和体系性。领域法学的规范对象主要是新兴领域,这些领域中对法律应予规范的主体、对象等基础要素尚未达成共识,法律制度的基本框架与具体内容仍在摸索制定的过程中,学者并无成熟、完备的法律文本和法律原则可以探讨,无法借助对实定法的规范分析形成内容完整、逻辑自洽的学科体系^[22]。而且,通过建设一个独立的领域法“拨开多元复杂的领域法律现象”之必要性也存在质疑。正如学者所言,传统部门法涉及的社会生活领域同样很复杂,但它们依然能够通过抽象的思维方法,得以建构出一套概念明确、规则完备、逻辑严密的法体系^[23]。既然部门法自身具有“化复杂为简单”的应变能力,若是非要另起炉灶,在一定意义上反倒增加适用上的复杂性。

其次,相关法律关系难以协调。若依据领域法方案在各部门法之上构建一个以个人信息保护问题为中心的综合法部门,那么,作为领域法的《个保法》法律地位如何界定?其与民法、行政法、刑法等传统部门法的法律地位是否平等,以及如何处理二者适用中的关系冲突?这些问题尚未获得充分应答。实际上,作为领域法的《个保法》和部门法的界限是模糊的,其与多个部门法相互交叉,难以作出切割。《个保法》与相近领域法之间的关系也难以协调。不同领域法仅存在局部的共性,它们既不共享同一套权利话语体系,又无法构成复合型领域法^[20]。例如,在已存在“个人信息保护”之领域法的情况下,若是再就“人工智能”这一问题确立起另外一个领域法,如何处理二者之间诸多的交叉问题,本身即是一个难题。而且,随着科技的迅猛发展,新的领域法不断产生,原有的领域法也会随时消失,结果上并不利于维护法律体系的稳定性。

再次,领域法中难以塑成统一的行为范畴。在领域法的层面,想要在制度规范中形塑统一的行为范畴十分困难,其主体的异质性更为突出,多元主体在相关领域从事的行为难以在法律层面作统一涵摄;即便真的规定了统一的“行为”,也不过是纯粹的理论抽象而实践意义有限^[23]。《个保法》作为一部实操性很强的法律,其规则的适用必然要求区分行为的性质,并据此确认不同主体的权利、义务及责任,因此,统一行为范畴的缺乏成为其走向实践的直接障碍。

最后,领域法方案与实践相脱节。在领域法支持者的理想目标中,相关的新兴、交叉学科依据其理论成果发挥各自的作用,而不必经由部门法学的“加持”或“升级”,来争取相应的学术地位或话语权^[18]。然而,如何将这一理想目标转化为司法实践尚未可知。领域法方案若要成为《个保法》的适用路径,就必须具有现实可行性,经得起实践检验,避免理论和实践脱节。领域法学虽然也关注个案和具体问题的分析,但更加偏向于对相关问题的理论归纳,提炼具有共性的知识部分。同时,这一模式与目前的司法适用框架也不尽契合。单是从司法部门的构成来看,各审判庭长期以来基于部门法的类分而设置,审判人员(硕士研究生学位以上)的知识体系也通常基于相关学科类分而塑成。在这一现实框架内,法官先要基于部门法的属性不同对《个保法》的目标规则作出类分,再依据相关部门法的规范要求将其应用于个案。换言之,《个保法》相关规则的适用最终仍需要回归于各自所属的部门法之中。由此视角,领域法方案不仅偏于理论,与既有司法体制也缺乏协调性,其实践化进程不可能一蹴而就。

除此以外,当一个理论方案具有颠覆性,试图以一种形式覆盖或替代原有整体方案时,尤其需要科学评估其是否存在引发原有制度价值遭受破坏的风险。有学者即认为,领域法方案适用过程中容易过度强调基于领域本体性特征的特定价值而忽视以自由价值为核心的私法赋权作用^[20]。而且,若将《个保法》整体纳入一个新的法律体系,不对相关法律作切割处理,虽然利于从整体上把握整部法律的目的和精神,客观上反倒会冲击既有的法律部门划分标准,使得整个法律体系的结构设计失去科学性和严谨性^[1]。综上,领域化方案于《个保法》是否具有适用可行性远未形成定论。

三、《个保法》适用的守成与求新

场景化应用、领域化等方案的提出,在一定程度上映射了学者对于既有法律制度能否有效应对新技术发展问题的担忧。然而,既有法律体系是否真的如此不堪一击?答案是否定的。纵观法律制度的发展史,立法者和司法者无时无刻不在准备应对新问题的挑战,在长期的实践中不断积累经验并将其融入既有法律体系之中。换言之,在新科技发展背景下,既有法律体系并非如同一些学者所想象的那样脆弱。借助一些有益的法律适用方法和工具,我们仍能得以在制度守成和制度求新中实现平衡。

从欧盟和美国的法律发展来看,其关于个人信息保护的立法已经完成了一个代际性转换:欧盟法以95指令为基础,进而发展到《通用数据保护条例》;美国法推行专门立法的同时,通过判例法的灵活适用,在遵循传统信息隐私法的前提下逐步引入新的规则。域外个人信息保护法相关理论的发展亦呈现一定的代际性,即前沿理论的提出仍然牢牢根基于传统法律制度框架,在承袭的基础上不断创新。与之相较,我国相关理论研究存在一个短板:鉴于传统法中个人信息保护法律制度的缺失,学界对于新理论及新规则的构建投注了过多的热情,一定程度上忽视了本国法固有的传承性及法律的代际性。然而,超越法律实践的理论创新观点往往难以获得有效执行,学界在关注理论创新的同时须注重对既有制度的衔接。为了应对新科技发展引发的社会变动,法学理论和司法实践中有待进一步检讨如何做到“在规则更迭中守成,在制度咬合中求新”。本文认为,法释义学和司法适用技术作为《个保法》的两大适用工具,仍然具有强大的应变力。

(一) 法释义学的实践意义:从法律范畴的可扩展视角

《个保法》出台后,学界对相关制度的适用性研究总体上延续了法释义学的技术路线。其中较为突出的一个努力是:对既有的法律范畴作出扩展性解释,令其具有更大的适用空间。正如学者所言:就部分法学基本范畴而言,新科技虽然对它们造成一定冲击,但未形成根本性的撼动;而且,这些基本范畴通常关联着被广泛承认且不可轻易动摇的基本理念和价值预设^[1]。因此,对法律范畴作出扩展性解释成为一个无须改变既有制度安排便可应对新技术冲击的有益手段。当然,此种扩展性解释方法并非适用于所有的法律范畴:一个法律范畴的内涵可能是固化的,缺乏可扩展的空间;当一个法律范畴的内涵存在不确定性时,则可以对其作出更为弹性的解释。通过如下两个例证,得洞察通过对既有法律范畴的扩展性解释应对新问题的可行性。

例证一:个人信息的“可识别性”。

如果某个数据无法与特定个体的人格身份发生联系,就无法想象对这一数据的处理如何对个体产生不良影响,因此各国法中普遍将“可识别性”视为个人信息的核心要素。然而,“可识别性”本身具有一定模糊性,对其难以作出清晰的界定。因此有学者一度认为,“可识别性”这一概念是不可行、不确定的,对其予以界定的企图如同嘉年华“打地鼠”游戏一样的徒劳,法律学者和政策制定者应当就该问题寻求新的解决方法^[24]。我国学者丁晓东在新近的研究中指出:信息的个人可识别性并不存在一个客观的刚性规则,而是取决于识别的目标、被谁识别、识别的概率、识别的风险等多种因素;在信息技术飞速发展及产品商业日新月异的背景下,这些因素更变得日益多元,使得个人信息更难界定^[11]。“可识别性”的范畴本身具有一定包容性和不确定性,这在客观上使得对其作出扩展性解释变得可行。

基于此种不确定性,采用不同的解释方法可对个人信息“可识别性”的范畴作出不同的解读。从各国立法发展来看,最具代表性的解释路径有两种。一是对“可识别性”的范畴采用限缩解释立场,受保

护的个人信息被限定于“目前”可识别的个人信息。^①若采用这一解释方法,个人信息受保护的相对较小,《个保法》对新技术引发问题的应对能力受到一定限制。二是对“可识别性”的范畴采用扩张解释立场,认为“未来”可识别的个人信息亦在法律保护之列。欧盟《通用数据保护条例》即秉承了95指令对个人信息的扩张解释立场,其项下“可识别”的自然人,意指能够被直接或间接识别,特别是根据身份证号码或一个或多个特定于其生理、心理、经济、文化或社会身份等因素被识别的自然人。^②该规定从文义上并未明显表明“可识别”的内涵大小,但从立法目的与立法技术来说,这一界定的意图意在扩充或强调个人信息的保护范围,防范对个人信息作较窄理解^[11]。据此,个人信息可被解读为与“已识别或者可识别的自然人有关”的信息,既包括“目前可识别”个人信息,也包括“未来可识别”个人信息。我国《个保法》亦采用扩张解释的方法。在此种扩张解释论下,个人信息受保护的相对范围相应扩大,《个保法》对新技术引发问题的应对能力也大为提升。

例证二:作为个人信息处理之合法性基础的“法律规定”。

“法律规定”这一范畴的内涵大小存在一定的不确定性,从而为作出扩展性解释提供了可行性。以2019年英国高等法院关于南威尔士警方使用人脸识别技术合法性审查的立场为例,其对“法律规定”采用了宽泛的解释方法。法院认为,除普通法之外,法律框架由三个层级构成:(1)初始立法;(2)在初始立法下发布的二级立法文件,即实践准则;(3)南威尔士警方自己的政策。^③依据这一解释方法,除“初始立法”之外,“实践准则”和“政策”等文件也被纳入作为合法性基础的“法律规定”的范畴,适用范围上发生扩张,一定程度上更利于警方利益的保护,司法的天平向公权力倾斜。反之,若是将此类传统上“非典型”的法律文件排除在“法律规定”的范围之外,采用限缩性解释方法,则警方使用人脸识别技术的合法依据范围变小,司法的天平向个人信息主体的私权利倾斜。可见,通过对既有法律范畴的弹性解释,《个保法》的适用可以获得更大的活力。

正如有学者所指出的,新科技时代并没有“肇生”全新的法律问题,而只是提供了“激扰”法学的知识体系、促使对既有理解进行反思的新语境,但无法直接引起法学基本范畴的更新^[11]。基于法释义学的方法,结合特定立法目的对《个保法》中一些重要法律范畴作扩展性解释,赋予其更多的适用活力,使其得以应对一部分新的问题和挑战,而无须另行创制新的法律范畴。

(二) 司法适用技术的作用

不容忽视的一个客观事实是,学界提出了诸多构造精妙的新理论,其中一部分成果并不能有效应用于司法实践。司法机关总是在相对程度上尊重传统规则,并非在任何情况下都会优先考虑创制新的标准或规则。司法者在个案审理的过程中既有守成也有求新,通过特定技术路线的适用应对新的问题和挑战。

一是新规则嵌入技术的应用。长久以来,司法者对于如何将特定新规则嵌入既有的法律框架积累了丰富经验,一定程度上得以保障法律制度在守成与求新中维持平衡。

以个人信息“可识别”规则在美国判例中的适用为例,得以洞察司法活动中新规则嵌入技术的应用。个人信息“可识别”规则得以确立后,美国判例实践中并非将其视为一个完全独立的新规则并围绕其创设新的适用条件,而是将其与传统的“普通人”标准相结合,使其被妥当地纳入既有法律制度框架之下。第三巡回上诉法院在Nickel案中对于这一嵌入过程作了详细的阐明:个人可识别信息是一个范围(Spectrum),(表面可识别个体的)姓名位于范围的一端;电话号码、街道地址等类似信息应位于中间位置,因为这些信息容易在公共记录中找到,同时要通过查阅电话簿或财产记录以识别个体;还有

^①尽管PII中的“I”一般被假定为表示“Identifiable”,但多数美国立法强调PII中的“I”为“Identified”,即“目前可识别”。

^②Article 2(a) of Regulation 2016/679 (GDPR).

^③EWHC 2341, CO/4085/2018, 04. 09. 2019.

诸如社会保险号的一类信息,其虽与个体相关,但在没有向其他实体(如信用报告机构或政府机关)查询的情况下可能不易与该个体相匹配。^①对普通人而言,IP地址或存在于cookie文件中的数字代码对识别一个事实存在的个体来说鲜有帮助。换言之,个人可识别信息应是一种“可以轻易让普通人识别特定个人的视频观看行为的信息”;据此,浏览器指纹、IP地址和唯一设备识别符等静态数字标识符“远落在范围之外”,普通人难以通过这些信息识别实际存在的个体,不应受到法律保护。^②从该案看出,一项新规则只有与既有法律实现良性咬合,方能发挥最佳效力。借由恰当的司法适用技术,即便法律适用的现实场景发生了变化,既有法律仍可以维持其特有的活力。

二是法官行使自由裁量权。如果说,将新规则嵌入既有法律制度框架展现了硬币的一面,那么法官通过自由裁量权的行使对既有规则作出弹性适用则是硬币的另一面。

亚里士多德认为,当法律因为太原则而不能解决具体问题时,就应该对法律进行一种校正^[25]。自由裁量权作为赋予法官的一个古老权能具有不可避免性。一方面,这是由社会事务、社会存在的复杂性所决定的。法律是社会关系的调整器,而社会关系是复杂的、不断变化的,因此要使立法精细而明确地规范所有的社会关系是不可能的^[26]。“正如现实的变化是生活的法律,回应现实的变化则是法律的生命”^[27],法官行使自由裁量权使得《个保法》与新科技发展背景下不断变化的社会现实更相适应。另一方面,世界是可知的,但人的认识存在局限性;人所制定的法律不可能对所有的事物都规定得很清楚,也不可能对所有的事物都作出明确无误的调整,客观上不得不用一些模糊概念加以规范^[26]。而且,无论成文法编写得如何明确,法律或者宪法的一切规范总是存在多种意义,必然要由法官来确定文本的意义,通过法律解释手段选择使得法律或者宪法条文具有规范性的意义,成为可以适用的规范^[28]。《个保法》作为一部成文法,其规范意义亦需要法官结合个案作出进一步解读,方能真正实现其规范目的。

法官自由裁量权在何种具体情形下方可启动?美国现代法理学家德沃金在《认真对待权利》一书中指出,“如果某法律不能正确处理案件,不存在看来合适的处理规则,或者处理此案的规则模糊,则不能靠法律的规则来解决该案件,必须由法官行使自由裁量权。这意味着法官已经走出了法律之外,以某种其他标准引导他创设出一条新的法律规则,或对旧的法律规则予以补充”^[29]。依据我国司法界主流观念,司法自由裁量权是一种选择权、判断权,是指法官或者审判组织根据自己的认识、经验、态度、价值观以及对法律规范的理解而选择司法行为和对案件作出裁判的权力^[26]。它发生于两种情况:一是法律没有任何规定的情况,不过,法律没有规定未必存在自由裁量权;二是法律有规定,但规定不具体或者不明确^[26]。就《个保法》而言,它具有跨学科性、技术性、变化性等特点,既涉及公权力又涉及私权利,较之一般部门法更为复杂。受限于前期立法缺失以及理论上的成熟度不足,我国《个保法》规定较之国内其他部门法或域外相关立法(如欧盟GDPR)更为概括,并未针对所有适用情形作出一一规定,具有抽象性的比例原则与均衡原则也由此成为其重要的调整依据。《个保法》的规定不尽全面以及相关原则性规定的存在,均为法官行使自由裁量权留下了一定空间。司法自由裁量权作为一个令法律调整具有更大包容性和可适用性的重要方法或机制,使得《个保法》的适用具有了更大张力。

^①参见 *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 282 (3d Cir. 2016)。本案中,被告维亚康姆公司(Viacom)拥有一家名为尼克国际儿童频道(Nickelodeon)的儿童电视台,同时经营着一家面向儿童、提供流媒体视频和互动游戏的网站Nick.com。原告注册成为该网站用户,在其访问网站的过程中,被告利用cookie识别与追踪原告的在线行为,通过四种方式收集了原告的十一类信息并将其传输至谷歌(Google)。原告认为,谷歌拥有Google.com、Gmail以及YouTube等广泛的服务网络,其通过结合维亚康姆公司所提供的数据以及自有数据,能够确定Nick.com上视频观看者的身份,因此原告主张被告收集的信息系个人可识别信息,将其披露给谷歌公司的行为违反了《视频隐私保护法》。被告则认为,法案中的个人可识别信息仅限于“能够单独识别特定个人的信息”。

^②参见 *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 282 (3d Cir. 2016)。

概言之,在新技术引发既有法律冲击的情况下,通过司法者行使自由裁量权和对特定司法适用技术的选择,无须另行创制全新的规则亦能使得《个保法》适用中的部分新问题得以妥善解决。

四、结 语

从既有理论尝试来看,场景化应用和领域化方案对于《个保法》的适用具有特定的意义,然而,二者均在一定程度上对既有法律体系形成冲击。激进式的制度求新并非均为可取,《个保法》的适用宜采多元化方案,在规则求新的同时与既有法律体系实现良性咬合。本文主要阐明了如下论点:

一是场景化应用能在一定程度上缓解新问题对既有法律的冲击,这一目标通过制度规则的弹性设计、法官基于个案的场景化适用得以实现。法院或其他准司法机构具备接触正反双方意见的机会,得以通过双方举证、辩论等形式而深入个人信息实践的具体场景,并通过案例与自下而上的规则制定勾勒个人信息的边界^[11]。然而,场景化应用的“个别化立法”与我国的成文法特征并不契合,《个保法》在具体的场景化应用中仍需要另行缔造新的规则和标准,从而在客观上抵消通过场景化应用“维护既有制度外观”和“简化新问题适用”的部分努力。场景化应用的内在局限性表明,宜将其限定适用于《个保法》特定问题的解决,而不能成为一个普适性方案。

二是领域化理论的提出被视为新科技发展背景下应对《个保法》适用新问题的一个积极方案。但领域化理论难以实现其自身的独立性和体系性,不同法域之间的关系不易协调,且不能塑成统一的行为范畴。因此,领域法方案仍欠缺实践化的条件,如何将这一理念贯彻到《个保法》的适用过程仍存在一系列现实障碍。

三是《个保法》的诸多适用问题仍能在既有法律框架内得以妥善解决。一方面,法释义学仍具有充分的活力。在具体实践中,法教义学关注法律文本,坚持以一国现行法规范为中心,致力于寻求法律作为规范体系的内部知识,通过法律解释维持法律秩序的稳定性与法律系统的逻辑性^[19]。基于法释义学的方法,结合特定立法目的对《个保法》中一些法律范畴作扩展性解释,客观上得以应对一部分新问题和挑战,而无须另行设定更多的新概念和新规则。另一方面,通过司法适用技术的更优选择,将新的规则嵌入既有制度框架,并通过法官自由裁量权的行使对既有规则作出弹性适用,亦能有效地应对数字科技引发的一系列新问题。

参考文献:

- [1] 雷磊. 新科技时代的法学基本范畴:挑战与回应[J]. 中国法学,2023(1):65-84.
- [2] SCHWARTZ P M, SOLOVE D J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information[J]. New York University Law Review, 2011, 86(6):1814-1894.
- [3] STALLA-BOURDILLON S, KNIGHT A. Anonymous Data v. Personal Data-A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data[J]. Wisconsin International Law Journal, 2016, 34(2):284-322.
- [4] NISSENBAUM H. Privacy as Contextual Integrity[J]. Washington Law Review, 2004, 79(1):119-158.
- [5] NISSENBAUM H. Privacy in Context: Technology, Policy, and the Integrity of Social Life[M]. Stanford: Stanford University Press, 2009:141.
- [6] THE WHITE HOUSE. Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015[EB/OL]. (2015-03-05)[2023-05-06]. <https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>.
- [7] 蔡星月. 数据主体的“弱同意”及其规范结构[J]. 比较法研究, 2019(4):71-86.
- [8] 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[J]. 浙江工商大学学报, 2022(2):158-168.
- [9] MACENAITE M. From Universal Towards Child-specific Protection of the Right to Privacy Online: Dilemmas in the EU

- General Data Protection Regulation[J]. *New Media & Society*, 2017, 19(5): 765-779.
- [10] 王苑. 敏感个人信息概念界定与要素判断——以《个人信息保护法》第28条为中心[J]. *环球法律评论*, 2022(2): 85-99.
- [11] 丁晓东. 论个人信息概念的不确定性及其法律应对[J]. *比较法研究*, 2022(5): 46-60.
- [12] 李润生. 论个人健康信息“利用友好型”保护模式的建构[J]. *行政法学研究*, 2021(5): 79-90.
- [13] 丁晓东. 《个人信息保护法》的比较法重思: 中国道路与解释原理[J]. *华东政法大学学报*, 2022(2): 73-86.
- [14] 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[J]. *法学研究*, 2018(2): 3-23.
- [15] 赵祖斌. 从静态到动态: 场景理论下的个人信息保护[J]. *科学与社会*, 2021(4): 98-116.
- [16] 石佳友, 刘思齐. 人脸识别技术中的个人信息保护——兼论动态同意模式的建构[J]. *财经法学*, 2021(2): 60-78.
- [17] 马新彦, 张传才. 知情同意规则的现实困境与对策检视[J]. *上海政法学院学报(法治论丛)*, 2021(5): 99-109.
- [18] 余倩影. “领域法学”: 法理视野与话语共建[J]. *法学论坛*, 2018(4): 87-97.
- [19] 刘剑文. 论领域法学: 一种立足新兴交叉领域的法学研究范式[J]. *政法论丛*, 2016(5): 3-16.
- [20] 何松威. 论领域法的私法研究范式——以《个人信息保护法》研究为例[J]. *当代法学*, 2022(4): 92-104.
- [21] 刘剑文. 领域法学: 社会科学的新思维与法学共同体的新融合[M]. 北京: 北京大学出版社, 2019: 4.
- [22] 刘剑文. 作为综合性法律学科的财税法学——一门新兴法律学科的进化与变迁[J]. *暨南学报(哲学社会科学版)*, 2013(5): 25-35.
- [23] 侯卓. “领域法学”范式: 理论拓补与路径探明[J]. *政法论丛*, 2017(1): 87-96.
- [24] OHM P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization[J]. *UCLA Law Review*, 2010, 57(6): 1701-1778.
- [25] 博登海默. 法理学: 法律哲学与法律方法[M]. 邓正来, 译. 北京: 中国政法大学出版社, 2017: 16.
- [26] 江必新. 论司法自由裁量权[J]. *法律适用*, 2006(11): 17-22.
- [27] 巴拉克. 民主国家的法官[M]. 毕洪海, 译. 北京: 法律出版社, 2011: 16.
- [28] 石佳友. 民法典与法官裁量权[J]. *法学家*, 2007(6): 58-65.
- [29] 丹宁. 家庭故事[M]. 刘庸安, 译. 北京: 法律出版社, 2000: 157.

Application of Personal Information Protection Law in the New Technology Era

FENG Kai

(College of Comparative Law, China University of Political Science and Law, Beijing 100088, China)

Abstract: In the context of new technological development, how to maintain the applicable vitality of the Personal Protection Law is an important proposition. The scenarios model and domain law scheme have proposed new approaches for the application of the Personal Protection Law. Although the scenario-based application caters to the specific needs of personal information law, it has an inherent confliction with the canonical norms and cannot be universally applicable. The domain law scheme has specific legal value, but its own independence and systematicity is hard to be achieved. Moreover, its relationship with the departmental laws, namely relevant field laws, is difficult to be coordinated and it is not easy to form a unified category of behaviors. As a result, the domain law approach faces a series of practical obstacles. Meanwhile, the existing local system has a strong adaptability. With the current two applicable approaches, the Personal Information Law is still able to effectively cope with a series of new problems: (1) based on the method of legal interpretation, the connotation of some basic categories can be expanded with the purpose of the specific legislation; (2) the new rules can be embedded into the existing institutional framework through the judicial application techniques and the exercise of judges' discretion can be emphasized.

Key words: personal information protection law; scenarios model; domain law; legal interpretations; judicial application technique



(责任编辑 张伟 郑英龙)