个人信息保护原理之辨:过程保护和结果保护

蔡培如

【摘　　要】“过程保护”模式和“结果保护”模式是诠释和理解我国个人信息保护原理的重要视角。在过程保护模式中,个人参与乃至主导信息处理过程,这是以民法保护方式为基础,由补强型规则和削弱型规则共筑的保护理念;结果保护模式则是由公法限定个人信息可被处理的广度和深度以防止信息过度开采,从而于结果上保障个体的人格尊严价值或国家社会公共利益,这分化出社会控制论和国家保护义务论两种公法思路。在立法实践中,这两个模式不是排他互异,而是在不同的信息处理规则项下错落有致地组合,合力形成公私法共生的保护方式。

【关 键 词】个人信息;结果保护;过程保护;个人信息保护法

【作者简介】蔡培如,复旦大学法学院师资博士后(上海 200438)。

【原文出处】《行政法学研究》(京),2021.5.91~101

【基金项目】本文系中国博士后第69批面上资助项目“国家机关个人信息处理的公法原理释义”(项目编号:2021M690651)的阶段性成果。

引言

因计算机技术革命和大数据发展,我国个人信息保护原理研究在近十年逐步升温,伴随着《个人信息保护法》(以下简称《个保法》)的出台,实务界和理论界对此问题的研讨已进入白热化。《民法典》先已作出个人信息保护规定,《民法典》与《个保法》、私法与公法之间的关系,应如何解释?有学者认为,个人信息保护“难以在单一部门法中完全实现,故需要民法与行政法的结合来进行保护,这就产生了《个人信息保护法》,它本质上属于领域立法”。[①]但如何协同公法、私法保护模式?具体的个人信息保护规则又何以为公,何以为私?

本文主张,从“过程保护”模式和“结果保护”模式这两个视角,诠释和理解我国的个人信息保护原理。“过程保护”模式指,个人参与乃至主导信息处理过程,对具有人格利益的个人信息是否可被收集、如何被利用、是否可公开等事项具有一定的知情和决定权,从而确保个人得以自由地发展和培育独立人格。以告知同意规则为核心的民法保护模式是典型的过程保护,通过赋予个人知情、同意、撤回同意、信息携带、信息删除等权利,使其可深度参与、决定和控制信息处理过程。相对地,“结果保护”模式指国家权力代替个人决定,径直限定个人信息可被处理的广度和深度以防止过度开采,从而个体的人格尊严价值在结果意义上获得保障,或人格尊严因公共利益之维护,反射性地获得保护。因为结果保护模式需要公权力机关在抽象意义上划定个人信息处理的边界和深度,因而主要是公法保护。

“过程保护”模式和“结果保护”模式是对个人信息保护制度两种可能目的、侧重点的概括与阐释,但这不妨碍两者在一定范围获致相同结果。事实上,这两个保护模式处于理论坐标的两极,中间是一段连续的光谱,通过调整两者的构成比,可形成无数种可能的、复合型的个人信息保护进路。无论是立法

还是学理研究中关于个人信息保护问题的讨论，基本可在此光谱中思考。

本文首先以过程保护模式为分析对象，进而转向与之争锋的结果保护模式。通过对这两个理论视角的分析与反思，以《个保法》为对象，辨析过程保护模式和结果保护模式在个人信息保护立法中的结合与互动方式。

一、个人信息的“过程保护”模式

(一)基础版：民法保护

民法保护指以尊重个人意思自治为核心的、以形式平等为基本观念的私法自治，可拓展出人格权径路、财产权径路、人格权与财产权复合保护径路。其中，人格权径路又可细分为：广义隐私权保护、人格利益保护和具体人格权保护。总体上，个人本位是这些民法保护模式的共通理念，也即个人信息利益原则上归属于私人，不同之处在于个人对个人信息应享有的控制能力，以及由此形成的个人在信息处理过程中的主导程度和参与深度上的差异。落实到具体制度设计上，告知同意规则成为个人本位下的私法自治、信息自决理念的具象表达，并衍生出若干特定原则(如目的限制原则)、具体规则(如向第三方披露的规则)和个人权利(如同意权)。

因广义隐私权保护径路在我国日渐衰微，故此不再多论。以下简要对其余民法理论如何在信息处理过程中，安置个人权利，进行归纳分析：第一，人格权径路、财产权径路的理念差异在于个人信息财产价值与人格价值的构成比；反映在法律规则上的区别是，个人信息可否作为商品被完全让渡。当个人信息之于人的人格尊严、人格自由发展价值被渐次肯定，法律规则从充分尊重市场交易自由逐渐向维护信息主体人格尊严倾斜，即在个人信息处理过程中，个人可参与的信息处理环节得以增加，同时个人对每一环节的控制力度也相应增强。[②]当前，在美国较为盛行的财产权径路在我国遭遇水土不服，尤其是《民法典》已对此理论进行了阻滞。我国民法学者通过构造“财产性的人格利益”“人格权商品化”这一复合性通道，基本完成了在人格权项下保存个人信息财产价值的理论建构。

第二，人格权理论内部主要划分出人格利益保护说和具体人格权保护说，[③]但仅具体人格权保护说才属于典型的过程保护。一些学者主张应基于德国法上的信息自决理论，确立个人信息权，以充分保证个人享有控制、支配、利用个人信息的权利。[④]王利明教授将这种控制权表述为，“个人信息的权利人有权排斥他人非法收集、处理和利用。未经法律的许可，任何机构不得非法收集个人信息，更不得对这些信息进行非法利用。即使有关机构掌握了个人信息，也不能将个人信息任意向社会公开。”[⑤]其中，信息主体的同意表示是信息处理最重要的合法性基础，[⑥]可拓展出信息决定权、知情权、更正权、锁定权、被遗忘权等一系列丰富的保障权利实现的权能体系。

相较而言，利益保护说几乎位于过程保护的最低点。个人仅能因个人信息被侵害而导致其他民事权利被侵害时，才能获得侵权法上的事后救济，且救济范围较狭窄，如需具有过错、违反法律规定或公序良俗，除非法律另有规定。[⑦]依循此逻辑，个人也不作为积极角色参与信息处理过程，仅因法律上对信息处理者的行为规范，反射性享有防御性的、有限的受保护利益。[⑧]

(二)改良规则

1.补强型规则

补强型规则是对以告知同意规则为核心的民法保护模式在实践中出现的失灵现象所进行的反思和改进。称之为补强型规则，是因其欲确保个人对于个人信息处理过程具有一定的知情和决定权。只是补强型规则意识到：囿于现实中消费者有限理性、信息过载、市场垄断等一系列知识、信息和权力偏差问题，遵循形式意义上的平等对待理念已无法确保一个公平自主的决策环境。[⑨]这将过度放任信息挖掘、无限制地拓宽利用场景，减损个人尊严。由此，消费者权益保护、信息信义义务等为个人提供倾斜保护

的规则被提出，以矫正告知同意规则在运行中出现的实质不平等问题，也就是思维上由“强式意义上的平等对待”转向“弱式意义上的平等对待”。[10]

其中，消费者权益保护理论认为“信息主体——信息处理者”因信息不对称和谈判力量不均衡而需要国家保护。基于“父爱主义”，国家应在程序规则设计上，对消费者进行倾斜保护，包括设置有利于消费者的默认规则，为消费者配置不可被任意剥夺的、有利于自主决策的权利，以修正信息市场中出现的非对称权力结构。[11]值得注意的是，尽管美国将信息隐私问题置于消费者保护模式之下，但在我国理论研究中，明确主张采用此保护模式的观点并不多。但很多关于个人信息保护的具体规则和制度设计建议实则可统合至此，典型如欧盟提出的“经由设计和经由默认规则的数据保护”，指在进行信息处理活动的计算机系统结构中，嵌入“个人信息保护法律规范中原则、规则所体现的价值”以在代码层实现隐私或个人信息保护。[12]比如，在苹果IOS14系统中，所有应用需取得用户同意后，才可以收集用户设备信息用以投放行为广告，这是在信息采集端采用了对用户更为有利的选择进入规则，用以充分保障其自主决定权。

另一种改良方案“信息信义义务”(information fiduciary)由巴尔金教授在2016年提出，已被我国一些学者敏锐地捕捉到并尝试进行本土化改造。[13]信息信义义务认为信息处理知识是专业而艰深的，由信息处理者垄断，信息主体没有能力或需付出过高成本去评估、监控信息处理过程中的风险。为了创建一个值得信任的数字环境，使个人可以像寻求医疗和法律援助一样，安心地参与互联网生活，法律规则要求信息处理者承担信托义务，将信息主体的利益置于首要地位，所有处理活动不得与其利益相冲突。[14]本质上，信义义务是法律强制约束信息处理者的自由意志和行为动机以保护信息主体利益。但信义义务的成立仍以个人知情并同意信息处理为前提，所以信息信义义务“并非取代而是充实现有基于个人控制的隐私保护框架，旨在要求数据控制者以数据受托人身份参与数据实践，从而使其负担更高的义务标准并据此增强它们的问责制。”[15]

信义义务和消费者权益保护在一定程度上耦合，以构建信任关系为目的的信义义务的要求之一就是产品设计上要以委托人利益为首，如嵌入“隐私友好型”设计，从而帮助弱势的信息主体在友好的信息处理环境中，实现信息自治，比如定期向信息主体提示个人信息收集的类型、范围及处理的目的、频率。[16]

2.削弱型规则

削弱型规则是在承认个人信息人格价值的前提下，从信息流通之于社会生产和公共效益的维度出发，主张有条件地削弱、限制个人在信息处理过程中的参与度，从而构建一个可均衡个人信息保护与流通双重目的的制度体系，但没有脱离该制度的基本形状。典型建议是适用选择退出机制，创建合理使用制度。

选择退出机制主张削弱信息采集端上个人控制的强度，但不影响个人同意的范围。在《民法典》颁行之前，我国若干涉及个人信息保护的法律法规均将个人同意作为开启信息处理的合法性基础，甚至是唯一基础。若法律所要求的个人同意采用欧盟《通用数据保护条例》的积极同意方式——即信息主体应在自愿的情形下，明确、清晰得做出允许个人信息被处理的肯定性表示，可能过度束缚信息生产力并产生不必要的合规成本，这与数据时代的发展趋势背道而驰。为达平衡，选择退出机制试图通过对告知同意规则进行法规范演绎，建议按照信息的敏感度、重要性以及可能产生的风险层级，分别适用选择进入(明示同意)或选择退出(默示同意)规则。[17]

合理使用制度则缩减了个人对信息处理过程的参与范围，指经由立法价值权衡，处理者可以不取得自然人或者其监护人的同意就对个人信息进行包括收集、存储、公开等处理行为。程啸教授从《民法典》总则、人格权编原则以及具体的个人信息权益条款

中，抽析出三层合理使用规则，并概括为“为了维护公共利益”“保护民事权益”以及“处理已合法公开的个人信息”这三类合理使用情形。[18]值得注意的是，无论在《民法典》《个保法》以及推荐性国家标准《个人信息安全规范》之中，为了公共利益或第三人重要的人身、财产利益才是法律上认可的合理使用目的，纯粹私人经济利益——即商业利益被排除在外。相比之下，欧盟《通用数据保护条例》第6(1)(f)条将第三人的“合法利益”与个人同意、公共利益等并列作为信息处理的合法性基础，适用上无优先次序，如当行为广告营销的收益大于个人信息保护利益时，信息处理者可径直处理个人信息。[19]在此意义上，我国当前无论是在法律规范实践还是学理探索上，合理使用制度对私法自决理念的调整、限缩都是有限的，仅将之作为个人同意的例外情形对待。

尽管以上选择退出机制和合理使用制度两种方案都致力于削弱在信息处理过程中个人的参与程度或参与范围，但不同之处在于：选择退出机制仍遵照了私人自治的基本理念，只是原则上推定个人在信息采集端已作出了同意的意思表示，异议者需采取积极行动退出信息处理；相反，合理使用制度则从整体上切割出一块个人无须参与、不可自决之领域。

与补强型规则的区别是，削弱型规则不是实践问题导向，其并不关注告知同意规则在实践中已出现的失灵现象，甚至可能加剧失灵。例如，选择退出机制之所以可达到促进信息流通的目的，基本原理是个人对缺省规则具有非理性的黏性。据调查，仅有0.06%的脸书用户改变了个人简介信息向所有人公开这一缺省规则。[20]所以，选择退出机制表面上仍保留了个人在信息处理过程中的决定权，实际却是利用信息主体的人性弱点和行为习惯以达到促进信息流通之目的，并冠以同意、自愿、信息自决之名。

(三)对过程保护模式的整体性反思

纵观以上过程保护模式的若干具体进路，可发现过程保护基本围绕着个人参与信息处理的范围、强度，以及参与过程中的缺省规则、利益冲突解决规则展开。问题是，个人参与、主导信息处理过程和个人信息保护之间是何关系？过程保护模式的支持者近乎整体性得跳过了此论证环节。实际上，个人对信息处理的控制不是信息保护的充分条件。已有社会学研究证明，增加个人控制权反而可能使其更愿意公开而非保护隐私信息。当个人可以决定隐私信息是否公开，以及谁可以获取、查看时，这种控制感将提升他们的安全感，从而愿意披露更多的、更私密的信息，即使披露行为将产生更大的风险；相反，如果减少个人对信息的控制权，失控所引发的隐私顾虑将使其更不愿对外披露信息。[21]此乃风险补偿(risk compensation)理论在信息隐私领域的体现，指当个人感受到风险增大时，会变得更加谨慎小心；相反，安全感会使个人疏于谨慎。所以，将个人导入信息处理过程中并赋予其决定性权利，不仅可能无法达到保护信息隐私的目的，甚至有可能增加个人信息被处理的频率和程度，降低隐私保护水平，这被称为控制悖论(control paradox)。

曾有学者言道，“退一步讲，在被赋予权利后，人们完全有放弃权利的自由。但是，如果没有被赋予权利，人们就没有任何选择的自由。”[22]但该研究没有论证，在信息处理过程中的选择自由为何是值得追求的、首选的制度目的？在信息自决模式下，个人是否可让渡所有个人信息？个人可否在充分知情下，明确同意微信、淘宝采集其医疗、教育、通讯等各个领域的信息并加以分析、形成个人画像，再基于数据分析结果对其作出个性化广告推荐、保险定价、雇佣决定、犯罪分析？表面上，信息主体享有并且实践着个人信息控制权、信息自决权，但结果上，每一次同意表示都将其本人置于数据处理、分析的客体地位，人格尊严和个人自治私域在实质递减。[23]此假设固然极端，但追问的却是一个迫切但却被惯常忽视的问题：个人信息保护制度实质追求的到底是个人信息被法律保护的状态，还是个人对信息处理过程所享有的决定自由？在个人信息保护制度终极目的上产生的分歧，是下文即将展开的“过程保护”模式和

“结果保护”模式之根本分野所在。

二、个人信息的“结果保护”模式

过程保护和结果保护的主要分歧即在于对个人信息保护制度目的理解不一致。过程保护模式重视信息处理中的个人意志，通过创设同意权、访问权、更正权、删除权等一系列个人权利，推定享有决定自由就等于实现和维护了个人信息的人格利益价值，达到了制度目的。在法理上，通过将“同意”解释为“免责事由”“许可”，将信息流转理解为个人自由意志决定之结果，消解了个人信息处理可能对人格产生减损的事实。[24]相对地，结果保护模式的基本立场是：积极调动国家立法和行政资源规范个人信息处理行为，以将处理可能对个人和社会造成的侵害与风险控制于普遍可接受的程度之内。简言之，该模式追求的是个人信息处理结果的总体效益是正向的，成本收益是均衡的。而其中，个人参与只是可供选择的规制工具之一，视其有效性而定。对个人而言，个人信息及背后映射的人格尊严因国家权力行使而被动地、强制性地受到保护，也就是艾伦教授所称的“强制隐私(coercing privacy)”。[25]在此制度目的统筹下，理论界产生了社会本位论/社会控制论和国家保护义务论这两个重要的结果保护理论类型。

(一)类型：社会本位论和国家保护义务论

1.社会本位论

“社会本位论”的研究起点是打破个人信息私人归属这一命题，由此降低、甚至否定个人参与信息处理的价值。首要论点是个人信息具有经济价值，特别是个人信息是充裕的、不会耗竭的大数据产业发展的原材料，信息价值伴随着持续的流通利用递增；[26]另一论点是个人信息具有社会识别和交往功能；[27]再次是个人信息作为言论自由对象所具有的公共流通和讨论价值。鉴此，应将个人信息作为公共物品对待，从公法角度予以保护和利用。

在此基础上，社会本位论将促进社会效益、维护公共利益这些目的注入个人信息保护制度。一方面，信息流通的价值被推至首位，“有关立法目的应当是为了公共利益而促进个人数据信息的共享和使用，而不是直接为了保护个人私权”。[28]另一方面，防控大规模、持续性信息处理对社会、民主政体所产生的系统性风险也极其重要，个人信息保护的“直接目的更多地体现在公共领域，即规避因信息可能的泄露和滥用而导致的社会风险。”[29]需分辨的是，消费者权益保护虽也关注个人信息处理中的“社会问题”，但此处的社会性来源于规模和人群庞大，所侵害的利益实际仍可分解到具体个人；社会本位论则关注抽象的、整体性的利益，认为“由于社会利益具有整体性和公共性，因此不能简单将之化约为各主体利益的加总，更不能简单将之等同于某一群体的利益或是多数人的利益。”[30]所以，只是因维护社会公共利益之需，个人反射性地获得保护。

2.国家保护义务论

结果保护模式的另一分支“国家保护义务论”则未选择破除个人信息私人属性这一前提，而是从私主体间呈现出的非对称权力结构所产生的个人被支配的恐惧和风险切入，引入国家权力矫正这种不对等关系。“个人信息国家保护义务的价值基础便在于：在政府或商业组织积累和使用大量数据的场景下，面对个人与信息处理者之间存在的持续性的不平等关系，需要国家转变消极的‘守夜人’角色，通过强有力的规制手段保护处于弱势地位的个人。”[31]这与消费者权益保护理论有一定相似，即个人因“缺乏制衡能力与信息资源”而在信息处理关系中处于弱势地位，若无法律制度规则帮扶，将被迫屈从于数据权力。[32]两者的差异在于：消费者权益保护理论将实现个人意志自由瞄准为制度目的，法律对私法上的信息处理关系的干预，意在为个人创造一个可参与的、可自主决策的、实质平等的环境；而国家保护义务论认为，个人信息受保护的状态以及由此产生的其他宪法基本权利受保护的状态，才能体现和实现个体人格尊严这一宪法终极价值。换而言之，国家保护义务理论径直将个人信息受保护作为重要目标，否认个人有放弃个人信息被保护的自由。

在强制保护理念下，如何化解《民法典》《网络安全法》以及《个保法》等制定法所规定的知情权、信息访问权、更正权、删除权等一系列个人权利或权能？国家保护义务论者认为，这些权利是国家为制衡信息处理者而赋予个人的工具性权利，“立法者只是通过特定的制度设计保障个人在与其相关的个人信息处理活动中的发言、参与和选择，以抑制个人信息处理者的恣意和滥权，但并非赋予个人对其个人信息的实体性控制权。”[38]反之，若立法者经慎思明辨认定，个体行权将使个人信息被过度处理，进而危及宪法所追求和维护的人格尊严时，可以截断个人对信息处理者所享有的一系列权利，此举不会受到宪法基本权利的制约和拦截。

(二)对结果保护模式的整体性反思

处于个人信息保护原理另一端的结果保护模式的整体缺憾是，未能从正面打破个人参与乃至控制信息处理过程的意义。对社会本位论而言，即使该理论尝试从信息流通之于社会交往和经济效益的角度解题，却未能充分回应多数个人信息可以识别到特定个人(个人信息的识别性标准)，并可体现该人的政治倾向、社交状态、消费偏好、兴趣爱好等多元人格面向(个人信息的关联性标准)，仅凭个人信息同时附着着公共利益、流通利益这一理由尚不足以完全替代和推翻个人信息的个人属性，以及由此延伸的个人参与信息处理的价值。更为艰难的是，既然《民法典》已将个人信息写入人格权编，如何在尊重立法价值判断的前提下，解绑个人信息的私人人格属性，是社会本位论需要面对和跨越的重大实体法障碍。

而国家保护义务论的问题是，未能充分回答为何个人信息受保护的状态才是个人所真正追求、但自身却没有能力实现的终极目的。再者，“以用户的知情、同意、选择、控制为核心来建构整体个人信息保护制度，以对抗强大的商业组织和政治力量的模式，其必要性取得了大多数人的共识，且在可见的未来，其他情形都难以撼动同意原则的主流和基础地位。”[39]如何通过法解释将已被立法广泛采纳的告知同意规则适当融合入此理论体系，也是亟待消解的理论障碍。

三、《个人信息保护法》中的“过程保护”与“结果保护”

上文将个人信息保护的若干进路置于“过程保护”模式和“结果保护”模式两个理论端进行比较分析。但正如开篇所指出，两个理论端中间存在无数种可能的结合方案。立法实践中，《个保法》正是在不同规则项下，错落有致地将两种模式结合，形成公私法共生合力的保护模式。这一部分以这两个模式为视角，撷取《个保法》第二、三章中重要的个人信息处理规则，研究实践中这两个模式的分工、互动问题，共提取出四个重要的信息处理规则。

第一，关于告知同意规则(第13-19条)。该规则作为个人信息保护制度中的基础结构型规则，主要作用是保障个人知情、参与、甚至决定信息处理。此规则要求：信息处理活动原则上应基于个人同意进行，并且信息处理的目的、方式以及所处理的信息种类受到个人同意的约束，也将因个人撤回同意而终止。为确保个人自主意志，第16条禁止个人信息处理者以拒绝提供产品或者服务为威胁，不正当地限制个人不同意或撤回同意的自由。这是对互联网服务提供者因锁定效应而获得的垄断地位，以及由此与用户形成的不对等关系的回应，本质上是在“消费者权益保护”理念支持下，对市场交易自由进行限制和约束。

但更仔细分辨可发现，法律在确保个人决定自由的同时，又将个人可得决定之自由限于法律所划定的范围之内。根据第6条，对个人信息的处理应当限于所能实现目的的最小范围，不得过度收集个人信息；同样，第19条规定个人信息保存期限应为实现信息处理目的所必要的最短时间。所以，即使在完全公平、自愿的情形下，个人也不可以自愿同意信息处理者处理非必要的个人信息或延长保存期限。[55]而且，当前实践中对何谓符合“处理目的的最小范围”的个人信息，是由国家机关以规范性文

件的形式确定，如《常见类型移动互联网应用程序必要个人信息范围规定》。这意味着，国家法律制度基本确定了抽象意义上的个人信息可被处理的体量和限度。

虽然个人决策自由无往而不在法律的枷锁之中，但将其与消费领域中的决策自由幅度相比，可发现个人信息保护中的个人同意边界受到更深度的法律限制。一方面是因为，我国将个人信息认定为人格利益的一部分，法理上对人格利益的保护应重于作为商品的信息交换、利用；另一方面，在立法进程中，因个人信息泄漏而引发的诈骗、骚扰电话等社会普遍性问题是促成立法的重要动因，因而克制个人信息处理中的数据体量、严控信息利用目的，限制信息留存时间等成为主要立法目标之一。[36]所以，考虑到个人对产品功能所必需的最小范围和最短期限这一技术问题缺乏判断能力，同时作为对社会现象的回应，《个保法》所确立的告知同意规则是在国家保护义务理念下，划定了信息可处理的范围后，有限赋予个人以过程保护。

第二，关于自动化决策规则(第24条)。对自动化决策的格外关注和警惕主要是因为，自动化决策往往是通过数据汇总形成群像分类，进而完成个人画像，这可能涉及数据或算法存在不准确、歧视、不公正等问题。《个保法》关于自动化决策的规定与欧盟《通用数据保护条例》第22条相似，对仅通过自动化决策而作出的对个人权益有重大影响的决定，个人享有请求说明权和拒绝权。但与欧盟规定所不同的是，欧盟对此类自动化决策行为原则上是禁止的，仅在例外条件下可得进行；[37]而从字面理解，我国采用的不是原则性禁止态度，自动化决策在满足透明、公正、自愿，并为个人提供解释说明权和拒绝权等条件下，即可进行。如是，《个保法》对具有重大影响的自动化决策这一信息处理方式并未施以实质性限制，自动化处理决定是否得以进行的最终决定权基本归属于个人。此外，个人有权退出通过自动化方式进行的商业营销、信息推送，对于那些对其个人权益有重大影响的纯自动化决定，个人亦有拒绝权。而为保障个人决策自由，第24条第2款和第3款，对以市场营销为目的而形成个人画像的信息处理，或纯粹自动化决策结果，个人享有不受惩罚的、无不利后果影响的退出权或拒绝权。所以，对既产生商业营销利益又存在个人权益风险的自动化决策规则，我国基本采用了消费者权益保护理念下的过程保护模式，并辅以禁止“大数据杀熟”“价格歧视”这样的结果保护。

第三，关于公共场所个人图像、个人身份特征信息处理规则(第26条)。为促进政府管理之效率、维护公共场所秩序安全，我国图像采集和个人身份识别设备已基本实现全方位覆盖，但此种实时的、持续性的、普遍无差异的远程生物识别技术，对个人隐私、人格发展和公民社会施加的负面影响已引发了大量警惕。在我国，近年来关于地铁、小区安装使用人脸识别技术的正当性和合理性成为讨论风口，杭州野生动物园人脸识别案也将此问题推向大众视野。[38]

《个保法》第26条正是在公共监控技术铺张背景下，对个人可被轻易识别和持续性监控的担忧中，应运而生。此规定可拆解为两层次进行解析：在第一层次“信息采集阶段”，为维护公共安全，在确保充分透明的条件下，可径直进行个人生物识别信息采集活动，但仅限于“公共安全”这一特定事由，这不仅排除了私人利益，也将诸如智慧城市建设等其他公共利益排除于外。问题是，若获得个人同意，是否可为公共安全之外的目的采集个人图像、个人身份特征信息？从法律规定来看，第26条仅规定“个人单独同意”可成为后续信息利用的例外，但对信息采集环节未做例外规定，此种区分对待表明，立法者拒绝让个人同意成为个人生物识别信息采集活动的合法性基础。这也符合“公共场所”这一具有高度开放性、流动性场域的特点，个人单独同意于此既不具有可行性，亦不具有合理性。因而，我国当前是在结果保护意义上强力控制公共场所中的个人生物

识别信息采集。

在第二层次“信息利用阶段”,对被搜集的信息之利用原则上应仅限于公共安全这一原初目的,取得个人单独同意的除外。这意味着在信息利用中,个人的自主意愿获得更强的尊重,但因人脸信息等生物识别信息的敏感性,我国又通过“单独同意”这一要求收缩个人参与的入口。

第四,关于个人信息跨境提供规则(第38-43条)。第三章个人信息跨境提供规则是第二章个人信息处理规则的场景之一,只是因其涉及跨境信息传输问题,关涉数据主权、国家数据战略、数据安全和国家安全等议题而具有特殊重要性,故而单列为一章,并与《数据安全法》衔接。正因其涉及国家安全和主权问题,跨境个人信息传输活动需遵循严格的合规义务以预防、控制风险,比如跨境提供个人信息需通过网信部门的安全评估、满足本地存储要求等。故而,本环节着重通过行政法上的合规义务将个人信息跨境传输活动控制在高法律保护水平之内,基调是结果保护。

难点是其中个人同意的定位。第39条规定,个人信息处理者应当告知个人有关个人信息跨境的相关信息,并取得个人的单独同意。而第38条要求,个人信息处理者确需向境外提供个人信息的,应当至少具备下列一项条件:一是通过国家网信部门组织的安全评估;二是经专业机构进行个人信息保护认证;三是遵守国家网信部门的标准合同要求。问题是,第38条和第39条之间是并列还是叠加关系?若是并列,无论信息接收方的保护水平如何,个人明示同意即可推动信息跨境流通;若是叠加,则意味着个人同意在信息跨境中不具有唯一决定性作用。欧盟《通用数据保护条例》选择了第一种模式,根据第49(1)(a)条,在缺乏适当性决定(adequacy decision)和适当保护措施(appropriate safeguards)的情况下,数据主体的明确同意也是数据跨境流通的合法性基础,可径直推动数据跨境传输。所以,欧盟的跨境流通规则是以尊重个人决定自由为核心的过程保护。而在我国,结合《网络安全法》第37条、《数据安全法》以及2019年网信办公布的《个人信息出境安全评估办法(征求意见稿)》,个人信息跨境传输主要是置于国家安全战略布局之中,其中个人同意只是作为风险可预期、风险自甘的环节之一被纳入整体法律框架中。另外,根据《个保法》第38、39条的顺序,如果个人同意可以成为免除安全审查的合法理由,其应规定于第38条之中,与安全评估、认证等作为并列条件。所以,结合我国个人信息跨境的法律制度背景以及法条次序,《个保法》中个人信息跨境提供规则更合理的解释应是第二种,即需在合规的前提下获得个人同意。实际上,从第三章的整体内容观察,在结果上确保信息跨境安全,从而维护国家社会公共利益是该规则的核心目的,个人是否参与此过程不具有主要价值。

如是,通过对《个保法》个人信息处理规则进行扼要分析,可发现:首先,当前整体的立法思路是过程保护和结果保护交叠,任一模式不具有唯一主导性;其次,决定采用何种保护模式,取决于具体问题的重要性,及个人自主与国家社会整体利益之间的关系,所以从总体视角抽象地分析《个人信息保护法》的定位难逃以偏概全的问题;最后,从所择取的规则观察,多数信息处理规则是过程保护和结果保护的综合体,由公法确定个人信息处理的限度或底线,再选择性地保留个人自主决定空间。

结语

近十年是我国个人信息保护研究的高峰期,若干个人信息保护的思路理念竞相角逐,但始终缺少可串联起这些理念的线索。鉴此,本文试图在解释性而非制度建构性立场上,提出以“过程保护”模式和“结果保护”模式来分析、统合整体的理论进路。此种理论整合意在为我国个人信息保护原理研究提供对话平台,理清当前的研究进展和发展方向;更意欲为我国立法实践中,设立个人信息处理规则时,如何处理、应对公法和私法保护方式的竞争与结合问题,提供理论分析工具库。

注释：

①王利明：《和而不同：隐私权与个人信息的规则界分和适用》，载《法学评论》2021年第2期。

②郑维炜：《个人信息权的权利属性、法理基础与保护路径》，载《法制与社会发展》2020年第6期。

③代表性研究：程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018年第3期；王利明：《论个人信息权在人格权法中的地位》，载《苏州大学学报》(哲学社会科学版)2012年第6期。

④王利明：《论个人信息权在人格权法中的地位》，载《苏州大学学报》(哲学社会科学版)2012年第6期。

⑤王利明：《论个人信息权在人格权法中的地位》，载《苏州大学学报》(哲学社会科学版)2012年第6期。

⑥王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

⑦程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018年第3期；程啸：《侵权责任法》，法律出版社2021年第3版，第148-150页。

⑧王利明：《民法上的利益位阶及其考量》，载《法学家》2014年第1期。

⑨郭春镇、马磊：《大数据时代个人信息问题的回应型治理》，载《法制与社会发展》2020年第2期。

⑩王轶：《民法价值判断问题的实体性论证规则——以中国民法学的学术实践为背景》，载《中国社会科学》2004年第6期。

⑪我国理论研究中对消费者权益保护到底属于公法保护还是私法保护存在分歧。从国家权力是否介入私人事务的角度观察，这可认为是公法保护模式；但本文认为，从权力介入目的观察，消费者权益保护更适宜被纳入私法领域，因为国家介入的目的是创建和维护私人自治环境。丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》2018年第6期。

⑫郑志峰：《通过设计的个人信息保护》，载《华东政法大学学报》2018年第6期。

⑬我国相关代表性研究包括：吴泓：《信赖理念下的个人信息使用与保护》，载《华东政法大学学报》2018年第1期。

⑭See Jack M. Balkin, "Information Fiduciaries and the First Amendment", UC Davis Law Review, Vol. 49, No. 4, 2016, pp. 1215-1225.

⑮解正山：《数据驱动时代的数据隐私保护——从个人控制到数据控制者信义义务》，载《法商研究》2020年第2期。

⑯李芊：《从个人控制到产品规制——论个人信息保护模式的转变》，载《中国应用法学》2021年第1期。

⑰吕炳斌：《个人信息保护的“同意”困境及其出路》，载《法商研究》2021年第2期。

⑱程啸：《论我国民法典中的个人信息合理使用制度》，载《中外法学》2020年第4期。

⑲Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/47/EC, adopted on 9 April 2014, WP 217, pp. 24-26.

⑳See Ralph Gross & Alessandro Acquisti, Information Revelation and Privacy in Online Social Networks(The Facebook Case),2005, https://www.heinz.cmu.edu/ ~ acquisti/papers/privacy-facebook-gross-acquisti.pdf,p.7.

㉑See Laura Brandimarte, Alessandro Acquisti and George Loewenstein(2012). Misplaced Confidences: Privacy and the Control Paradox, Social Psychological and Personality Science 4(3), pp. 340-346.

㉒王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

㉓See Anita L. Allen, "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm Commentary", Connecticut Law Review, Vol. 32, No. 3, 1999, pp. 865-869.

㉔程啸：《论侵害个人信息的民事责任》，载《暨南学报》(哲学社会科学版)2020年第2期。

㉕Generally see Anita L. Allen, "Coercing Privacy", William and Mary Law Review, Vol. 40, No. 3, 1999.

㉖吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016年第7期。

㉗高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018年第3期。

㉘吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016年第7期。

㉙梅夏英：《在分享和控制之间 数据保护的私法局限和公共秩序构建》，载《中外法学》2019年第4期。

㉚王怀勇、常宇豪：《个人信息保护的理念嬗变与制度变革》，载《法制与社会发展》2020年第6期。

㉛王锡锌:《个人信息国家保护义务及展开》,载《中国法学》2021年第1期。

㉜王锡锌:《个人信息国家保护义务及展开》,载《中国法学》2021年第1期。

㉝王锡锌:《个人信息国家保护义务及展开》,载《中国法学》2021年第1期。

㉞申卫星:《大数据时代个人信息保护的中国路径》,载《探索与争鸣》2020年第11期。

㉟根据相关新闻,在个人信息保护法修正草案二审稿的审议过程中,信息存储和销毁问题获得广泛讨论,主要关注点是在信息利用的目的完成后,应尽快将信息销毁、去标识化、匿名化,以防止其流入黑产。故而,立法过程并不重视存储环节的个人控制问题,更关注的是信息隐私受保护问题。《数字化时代,个人信息如何保障——个人信息保护法草案分组审议侧记》,中国法院网,https://www.chinacourt.org/index.php/article/detail/2021/04/id/6010376.shtml(最后访问时间:2021年4月29日)。

㊱杨立新:《个人信息:法益抑或民事权利——对〈民法总则〉第111条规定的"个人信息"之解读》,载《法学论坛》2018年第1期。

㊲Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, pp. 19-20.

㊳郭春镇:《数字人权时代人脸识别技术应用的治理》,载《现代法学》2020年第4期。

The Distinction of Personal Information Protection Principles: Protection by Process and Protection as a Result

Cai Peiru

Abstract: The "protection by process" model and "protection as a result" model are instructive perspectives for interpreting and understanding the principles of personal information protection in China. On the one hand, in terms of the "protection by process" model, it is the data subject that dominates the information processing process, which is based on the civil law method and supplemented by reinforcing rules and weakening rules. On the other, the "protection as a result" model requires the public law to limit the breath and depth of information processing, so as to prevent over-exploitation of personal information, thereby protecting the individual's personal dignity value or the national and social interest. This model can be divided into social control and the state's duty of protection theories. In legislative practice, these two models are not exclusive in effect. Under different information processing rules, they are combined in corresponding manners, which reflects the symbiosis of the public and civil law for the protection of personal information.

Key words: Personal Information; Protection as a Result; Protection by Process; Personal Information Protection Law

