法学研究

个人信息有序共享的法理言说与制度构建

夏　伟

[摘　要]　传统社会向现代社会转型驱动的“压缩式”制度建构,虽然加快了个人信息保护体系的建设进程,但也加深了个人信息之权利保护与资源共享的制度性失衡危机。有序共享是对数字经济时代个人信息的重新定位,个人信息不再是专属于个体的自决权,而是兼具个体与社会属性的防御权。以立法对个人信息的分类分级为基础,应当在纵向维度根据个人信息的重要程度形成核心层、中间层与外围层的差序保护格局。推进个人信息有序共享,应当根据个人信息的内在层次结构分别确立“授权同意”“知情同意”“推定同意”的差异化规则,以此指导个人信息领域相关制度的民行刑一体化构建。

[关键词]　个人信息;分类分级;有序共享;同意规则;民行刑一体化

一、问题缘起:个人信息保护与共享的制度平衡困境

传统社会向现代社会的转型变迁对个人信息保护体系建构具有极强的内在塑造力。信息网络化与科技跨越式发展重塑了个体之间、个体与社会之间的关系,并使个人信息领域的旧问题与新问题“共时态”地存在于现代社会。在数字经济时代,以数据为主要存在形式的个人信息,一方面需要受到法律的全面保护,另一方面作为资源要素的个人信息如何被“高效流通使用、赋能实体经济”①以充分释放生产潜能,亦成为当今最鲜明的主题。以往个人信息的核心主题是如何保护,而现在人们更多地谈论如何对个人信息进行资源化共享,甚至在某种意义上,共享和使用“个人信息已经成为人们生活的组成部分……没有个人信息的透露就没有现代化的生活方式”。②

然而,作为私权利的个人信息保护逻辑与作为公共资源的个人信息共享逻辑之间存在着难以弥合的张力关系,它体现了从传统社会迈向现代社会的“时代裂隙”,“网络与数字技术的发展,摧毁了先前私域与公域之间的物理性边界,由此面临如何重建二者之间界线的时代命题”。③在个人信息权利保护与资源共享之间的紧张关系过于激烈的一些领域,人们可能下意识地将与传统决裂视为必经之路,认为削减个人信息作为私权利的保护力度与保护范围,适度牺牲个人信息的私权价值以维护

夏伟,法学博士,中国政法大学刑事司法学院副教授(北京 100088)。本文系国家社会科学基金项目“个人信息有序共享的刑民一体化保护研究”(20CFX027)与中国政法大学科研创新团队计划项目的阶段性成果。

①蒲实:《加快构建数据基础制度体系》,《学习时报》2022 年 7 月 11 日,第 1 版。

②刘艳红:《共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角》,《法学论坛》2020 年第 2 期。

③劳东燕:《个人信息法律保护体系的基本目标与归责机制》,《政法论坛》2021 年第 6 期。

公共利益具有实质正当性，进而淡化个人信息的私权利色彩并试图在该领域建立相对单一的资源共享秩序。例如，有学者指出，刑法中侵犯公民个人信息罪的保护法益“应该从私法角度转向公法角度，刑法保护个人信息的目的不是确权，而是规避风险”。[①] 这种做法“将中国传统与现代性之间的关系，描述为两种相互排斥的力量之间的关系，它们可以相互替代，但却无法真正交融在一起”，[②]具有鲜明的独断主义色彩并值得警惕与反思。

在数字经济时代对个人信息进行合理定位，必须兼顾国家层面的数字经济战略、产业层面的科技发展与个体层面的权利保护，在权利保护与资源共享之间寻求平衡。然而，个人信息的保护与共享之间原本就并非处于各安其位的和谐状态，加之在具体运作中又受到个体价值立场、数据技术发展与公共秩序塑造等因素影响，两者在许多场景中反而呈现出非此即彼的竞争乃至对抗状态。例如，无论算法多么精细、科学和严谨，利用网络爬虫技术获取网络数据都不可避免地搜集到个人信息，此时，要么坚守同意规则保护个人信息而禁止网络爬虫，要么适度降低个人信息保护标准、允许在算法合规情况下未经个人信息主体同意搜集个人信息，两者只能居其一。换言之，在现有的体系框架下，个人信息之保护和共享的平衡恐怕难以形成可操作的制度基础。

为了满足个人信息保护的时代需求，我国进入了个人信息立法的活跃化时期，有关个人信息的立法数量与制度供给均呈现爆发式增长，快速建立起了个人信息保护的法律法规制度体系。回顾个人信息保护立法与制度的发展历程，我国自 2003 年着手部署个人信息保护立法，在 2005 年初完成《个人信息保护法》专家建议稿，中间经历了 2009 年《刑法修正案（七）》将非法提供、非法获取公民个人信息的行为犯罪化（2015 年《刑法修正案（九）》进一步将其修改完善为《刑法》第 253 条之一“侵犯公民个人信息罪”）、2013 年通过《电信和互联网用户个人信息保护规定》首次界定了“公民个人电子信息”概念、2017 年通过《网络安全法》明确了“公民个人信息”概念及初步规则、2020 年《民法典》规定个人信息权利及一般性规则，直到 2018 年全国人大常委会才将《个人信息保护法》（草案）纳入第一类立法规划项目，即“条件比较成熟、任期内拟提请审议，尔后经多次调研、讨论、修改等形成正式提请审议的草案”，此间十多年里个人信息保护立法进展缓慢、几近停滞。换言之，我国个人信息保护相关立法与制度构建主要是近五年完成的，据统计，从 2017 年至 2022 年 10 月，国家机关及相关部门颁布的法律文件中出现“个人信息”关键词的法律有 33 部、行政法规与规范性文件 50 部、司法解释 105 部、部门规章 936 部，如此高频度地颁布实施与“个人信息”有关的法律规范，意在全面加快个人信息保护法律体系的建设进程。[③] 这种“压缩式”的立法建构利弊共存，它使得长期以来的个人信息保护立法的“赤字”得到了快速消解，促进个人信息保护立法紧跟时代步伐，又使得个人信息有关制度构建未经充分考量和理性权衡，反而陷入制度供给越多秩序却越少的尴尬境地，加剧了个人信息之保护与共享的制度性失衡。这主要体现在三个方面：

第一，制度规范“交错重叠”。我国个人信息保护的立法体系，大致呈现出一种金字塔结构，自上而下分别是基本法律规范即《民法典》中关于个人信息的有关规定、专门性立法即《个人信息保护法》及关联性立法、各级部委规章、地方规范文件等，层次结构分明。然而，审查这些规范的具体内容，有关个人信息的制度规范普遍存在“交错重叠”现象，它表现在两个方面：一是下位规范对上位规范的复刻，产生了规范的重叠冗余。例如，目前很多地方规范文件中有关个人信息的规定，与个人信息保护法等上位法的内容并无二致，实质是对上位法的复刻和重述，缺乏体现地方立法独特性的创

①欧阳本祺：《侵犯公民个人信息罪的法益重构：从私法权利回归公法权利》，《比较法研究》2021 年第 3 期。

②[德]多明尼克·萨赫森迈尔、[德]任斯·理德尔、[以]S. N. 艾森斯塔德：《多元现代性的反思：欧洲、中国及其他的阐释》，郭少棠、王为理译，北京：商务印书馆，2017 年，第 68 页。

③数据来自“北大法宝”，统计日期为 2022 年 9 月 20 日。

新内容。二是同级规范之间的交错，制造了规范的竞合与冲突。例如，个人信息常常以数据的形式呈现，此时，相关问题的处理需要同时考虑《个人信息保护法》与《数据安全法》，这导致两法在调整具体事项时可能存在交错乃至冲突。制度规范的“交错重叠”反映了个人信息保护体系构建中存在“重立法数量而轻立法质量”的现象，由此导致某些新增立法的实效性不彰。

第二，法律部门“渐生罅隙”。目前，我国个人信息保护体系建构主要遵循“一法一部门”的逻辑，有的制度设计虽然也涵括了不同法律部门，但是尚未来得及进行系统的跨部门法整合，因此，个人信息主题下的各部门法之间还存在衔接不畅之处。例如，《刑法》第253条之一侵犯公民个人信息罪仅处罚三种行为，分别是非法出售、非法提供与非法获取，其中，非法获取是前端的不法行为，非法出售、非法提供是末端的不法行为，欠缺对中间层次的非法使用行为的有效规制。与之相对，《个人信息保护法》所规范的大量不法行为其实出现在非法使用环节，该法还系统规定了个人信息合法合理使用的要件，对个人信息中间层次的使用行为投入了大量立法资源。显然，两法对个人信息使用环节的规制存在明显的衔接错位。又如，与《个人信息保护法》第4条定义的“个人信息”相比，2017年5月8日最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称《侵犯个人信息刑事解释》）第1条规定的“公民个人信息”限于可识别“自然人身份或者特定自然人活动情况”的信息，概念内涵明显更为狭窄。部门法衔接不畅可能导致司法过程中的“同案不同判”现象，累及公平正义。

第三，制度立场“摇摆难定”。《个人信息保护法》虽然被冠以“保护法”之名，但是其中仍然有不少“促进法”成分。个人信息保护的一般原则是“知情同意”，然而，根据《个人信息保护法》第13条规定，“为订立、履行个人作为一方当事人的合同”、“为履行法定职责或者法定义务”、“为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息”以及“在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息”等情况下即使未经信息主体同意处理个人信息，也都属于合法行为。以上条文的设立，显然是为了促进个人信息的流动共享，带有明显的“促进法”色彩。《个人信息保护法》以“保护法”为名同时又纳入“促进法”内容，反映了立法者既希望加强个人信息保护又担忧保护过度抑制个人信息资源化共享的矛盾心态。然而，在个人信息保护的司法实践中，相关司法判决则更加倾向于构建“促进法”的裁判规则，与“保护法”的定位逐渐疏离。2022年8月杭州互联网法院发布“个人信息保护十大典型案例”，有9项判决都支持了未经同意或未经特别授权而使用他人个人信息的行为，包括国家机关依法公开的个人征信信息，可以进行商业化利用，[①]平台事前取得个人概括性同意，可视为个人知情同意[②]，等等。以上判决对个人信息知情同意原则的解释适用均采取相对限缩的立场，其目的是最大化激发个人信息的流通共享价值，“保护法”的逻辑在司法实践中频繁被突破。

综上所述，尽管目前个人信息保护体系已经初步建成，然而，过于快节奏的立法难以形成平衡个人信息私法权利保护与公共资源共享的规范秩序。建立契合数字经济时代需求的个人信息保护体系，需要深刻反思个人信息保护的制度性失衡问题，寻求个人信息保护与共享的平衡路径。基于该问题意识，本文的基本观点是：数字经济时代的个人信息兼具私权属性与公共价值，由此个人信息系防御权而非自决权；科学建构个人信息法律制度，应当在对个人信息进行分类分级的基础上，进一步形成核心层、中间层与外围层的差序保护格局，促进个人信息有序共享。

---

①杭州互联网法院（2018）浙0192民初302号民事判决书。

②杭州互联网法院（2020）浙0192民初4252号民事判决书。

二、立场辨正:个人信息有序共享的法理基础

基于个人信息既是私法权利又是公共资源的双重属性,数字经济时代个人信息法律制度设计的基础理念应定位为有序共享。共享是个人信息客观价值的现实路径,有序是个人信息主观权利的法治保障。个人信息从自主支配转向有序共享,需要从法理上对个人信息的基本属性进行重新定位,并在立法对个人信息进行分类分级的基础上,根据个人信息对信息主体的重要程度进行差序化的分层保护。

(一)个人信息的法律定位:从自决权到防御权

传统观点认为,个人信息乃自决权之范畴,个人同意是个人信息处理行为合法化的前提和根据。"公民个人有权积极利用其个人信息,'同意'构筑了信息自由与刑法介入之间的分界",①由此,只要未经个人同意而收集、存储、使用、加工、传输、提供、公开个人信息的行为皆属违法,达到一定程度,即构成犯罪。② 从为个人信息提供最优保护之视角,自决权理论无疑符合私法自由自治的理性考量。然而,个人信息在现代社会中的法律定位,不能仅局限于纯粹理性建构,还需要立足实践逻辑,科学的制度构建"不可能完全依据建构理性而为,而必定基于经验理性的探索试验渐进形成",③将实践经验与理性建构有机整合,是保持个人信息保护制度科学性的重要路径。

在现代社会,个人信息早已超出个人自决之范畴,而在很多方面表现出共治共享的鲜明特色。党的二十大报告提出,要"健全共建共治共享的社会治理制度",数字社会共建共治共享格局的形成,需要加强包括个人信息数据在内的数据资源共享。尽管《民法典》将个人信息规定在总则第五章"民事权利"中,确认个人信息的私权属性,然而,根据中国人大网最新公布的按照法律部门分类的现行有效法律,《个人信息保护法》被归入"行政法"部门,④这意味着该法具有鲜明的公法色彩。事实上,考察《个人信息保护法》的具体内容,该法以大量篇幅规定了个人信息的国家保护义务,还设专章规定了行政法律责任。由此可见,个人信息兼具私法与公法属性。从刑法角度来看,侵犯公民个人信息罪的保护法益即公民个人信息,也越来越被认为具有公私混合法的属性,本罪也被理解为自然犯法定犯化或混合犯的立法体现,⑤它既不是纯粹的自然犯又不是纯粹的法定犯,而是兼具两种犯罪的成分。⑥ 基于法秩序统一性原理,由于刑法是其他部门法的保障法,刑法对侵犯公民个人信息罪中个人信息的理解与定位来源于《民法典》《个人信息保护法》等前置法规定,同时,侵犯公民个人信息罪的混合犯属性也表明了刑法中的公民个人信息兼具私人与公共成分。

由此观之,个人信息的法律定位应当跳出纯粹自决权逻辑,而被塑造为兼具私人与公共色彩的防御权。个人信息的受保护性最初源于人格尊严,系(准)人格权,立法规定了一般性的人格权防御条款,其受侵犯时可依法排除妨碍,这种具有排除妨碍功能的权利在理论上被定性为"消极权利"或防御权。据此,将个人信息作为资源进行共享时不能侵害个人信息主体的权益,并且,对个人信息处

---

①冀洋:《法益自决权与侵犯公民个人信息罪的司法边界》,《中国法学》2019 年第 4 期。

②刘双阳:《论个人信息自决权刑事司法保护的边界——以已公开个人信息为中心的分析》,《人权》2021 年第 5 期。

③钱大军:《当代中国法律体系构建模式之探究》,《法商研究》2015 年第 2 期。

④中国人大网:《现行有效法律目录(298 件)》,http://www.npc.gov.cn/npc/c2/c30834/202309/t20230905_431560.html,2023-09-21。

⑤刘艳红:《民法编纂背景下侵犯公民个人信息罪的保护法益:信息自决权——以刑民一体化及〈民法总则〉第 111 条为视角》,《浙江工商大学学报》2019 年第 6 期。

⑥R. A. Duff, "Crime, prohibition, and punishment", *Journal of Applied Philosophy*, Vol. 19, No. 2, 2002, pp. 97-108.

理不需要授权的情形需要法定化，这样既可以促进数据产业发展，也尊重了个人信息权利主体的合理预期。[①] 个人信息的天然属性决定了它是防御权，由此在立法上确立其排除妨碍功能具有正当性。防御权的实现并不要求他人履行积极行为，其核心功能在于排除他人侵害。其实，在基本制度框架层面，作为个人信息保护核心的同意制度的运作，也有赖于公共力量的介入，融入公法监管因素。[②] 因为在现代社会，个人已经逐渐丧失真实的自决权，不太可能也没有足够能力对平台的个人信息保护条款进行实质审查。[③] 公权力的介入，弥补了个人在数字社会的能力短板，使同意制度得以真正落地。“在一般意义上，人身性或财产性的消极权利仅仅意味着他者不得侵害我们的权利，而不是要求他人必须为我们的人身或财产权提供积极保护”。[④] 按照传统自由主义的观点，所有权利都可以说具备着消极属性，权利概念可以一般性地表达为个人“自由行为与别人行为的自由的关系”，“任何人妨碍我完成这个行为，或者妨碍我保持这种状况，他就侵犯了我”的权利。[⑤] 这一自由主义的权利观道出了消极权利的形式一般性，即个人自由与他人自由协调并存的同时排除他人侵害。个人信息的人格属性决定了立法对其保护是以禁止侵害或排除妨碍为主，防御条款的设立正是以此为基础的。

如果说个人信息自然属性塑造了其防御性，那么社会属性的融入则进一步强化了这种消极防御性。因为个人信息要实现流通共享价值，必须适度抑制信息主体积极主张权利，否则在自由自治的市场关系中，完全由个人自决的个人信息不仅无法发挥其助力数字经济的社会价值，反而可能由于个人信息权利频繁被积极主张而抑制产业创新与科技发展。通常情况下，行为人只有妨碍了个人信息主体实现其权益时，才构成对其私法属性的侵害。当然，尽管个人信息是防御权，但是防御权并不排斥积极保护。任何权利的有效运行均需法律为之提供积极保护，对防御权而言，法律的积极保护仍然有其必要性，因为权利效力的实现要求法律“适用其强制性资源（coercive resources）来保障或限制私人自由”。[⑥] 只不过，在依靠法律与市场运行规律共同规范的市场秩序中，法律对个人信息的保护应以行为造成个人信息对应的人格尊严受侵犯的危险升高即增加自然人被识别的可能性为限。具体而言：在个人信息未被识别的场合，信息处理者应当尽到利用该信息时不被识别的合规保护义务；在个人信息已被识别的场合，信息处理者仅需尽到利用该信息时不被扩大识别的合规管理义务，这是个人信息作为防御权的当然逻辑设定。

（二）个人信息的层次结构：基于分类分级视角

个人信息的法律概念具有确定的内涵，也有不确定的外延。姓名、身份证件号码、通信通讯联系方式、住址、账号密码等信息虽然都冠以“个人信息”之名，然而，不同的个人信息的可识别性及其对个人与社会的价值往往存在极大差异，在法律评价的过程中难以等同视之。在传统社会向现代社会转型的过程中，个人信息的内涵发生了深刻变化，它源于人的自然属性，原本专属于个人，但是在复杂而深刻的社会发展中拓展出了内涵丰富的社会属性，20 世纪 70 年代后，“计算机技术的不断发展和交流机制的根本性变革改变了信息产生、获得、使用、传播的方式……信息分享和利用已成为常态。个人信息因此具有社会属性，其现实基础在于信息由个人生产却脱离其控制。”[⑦]因而，数字经济

---

①王利明：《数据共享与个人信息保护》，《现代法学》2019 年第 1 期。

②丁晓东：《个人信息公私法融合保护的多维解读》，《法治研究》2022 年第 5 期。

③F. Aldhouse，“Data protection in Europe：Some thoughts on reading the academic manifesto”，*Computer Law and Security Report*，Vol. 29，No. 3，2022，pp. 289 - 292.

④I. Persson，“The act-omission doctrine and negative rights”，*The Journal of Value Inquiry* ，Vol. 41，No. 1，2007，pp. 15 - 29.

⑤[德]康德：《法的形而上学原理——权利的科学》，沈叔平译，北京：商务印书馆，1991 年，第 40—41 页。

⑥[英]哈特：《法律的概念》，许家馨、李冠宜译，北京：法律出版社，2011 年，第 236 页。

⑦申卫星：《数字权利体系再造：迈向隐私、信息与数据的差序格局》，《政法论坛》2022 年第 3 期。

时代的个人信息较之以往具有更强的开放性与包容性。

由于不同类型的个人信息对个人人身、财产等状况识别的影响存在较大差异，可用于流通共享的条件与范围也有所不同，因此，对个人信息进行必要的分类分级是开展有序共享的重要前提。根据《侵犯个人信息刑事解释》第5条规定，行踪轨迹信息、通信内容、征信信息、财产信息是最为敏感的个人信息，住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的个人信息的敏感程度次之，除此之外都是普通个人信息，值得刑法保护的程度依次递减。《个人信息保护法》区分了敏感个人信息与非敏感个人信息，并对敏感个人信息处理作出特别规定。该法第28条规定，生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息均属于敏感信息；第29条规定，处理敏感个人信息需要个人的单独同意甚至书面同意。此外，对敏感个人信息还规定了严格的监管措施。非敏感信息的处理遵循《个人信息保护法》的知情同意原则，但并不要求单独同意或书面同意，监管措施相对宽松。个人信息的分类分级，初步确立了个人信息保护的差序化规则。然而，无论是《侵犯个人信息刑事解释》还是《个人信息保护法》都采取“列举＋兜底”的方式规定不同类型和级别个人信息的范围，即先列举若干类型，再以“等”作为兜底。尽管“等”的解释可以参照前述列举的个人信息类型进行同质解释，但其解释空间相对有限，这两部规范并没有抽象出具有共通性的归类标准。

个人信息流通利用制度的缺失，可以说是整部《个人信息保护法》的缺憾，但是总体而言，《个人信息保护法》的相关法条也为个人信息流通利用的合理化提供了基础性规范，由此可以开展进一步的制度续造。① 为了促进有序共享理念以具体制度形式贯彻，有必要在分类分级基础上，根据个人信息的可识别性大小及其与信息主体的亲疏远近关系进行再分层。影响个人信息有序共享评价的基本要素有两点：一是个人信息的可识别性大小。有的个人信息能够直接识别个人人身、财产等状况，因而需要重点保护；有的个人信息需要组合起来增加可识别性才能够有效识别个人人身、财产等状况，因而受保护程度有所降低。二是个人信息本身的重要程度即与个人的亲疏关系。在个人信息的双重属性中，社会属性是个人信息流通共享的支持性要素，限制流通共享的主要是个人属性，立法应当在多大程度上限制个人信息的流通共享其实主要由个人属性决定。具言之，个人信息的敏感性越高，其流通共享也越要受到限制。对个人信息的可识别性与敏感程度进行统一考量，可以对个人信息进行差异化分层：

第一，核心层的个人信息是具有高度可识别性的生物信息、隐私信息、身份信息等个人信息，如基因序列、私人生活影像、身份证件号码等，这些信息的可识别性最高，对个人而言敏感性、私密性也最高，其流通共享条件最严格。②

第二，中间层的个人信息是具有相对可识别性的身份信息、财产信息及其他信息，如交易信息、电话号码、住宿记录等，这些信息的敏感性、私密性次之，且在自然状态下，他人无法单纯通过这些信息准确识别个人状况，需要查证或者与其他个人信息组合在一起增加可识别性，才能够准确识别。

第三，外围层的个人信息有两种类型：一种是不具有独立可识别性的个人信息，其处理对个人而言没有直接影响。有学者称之为间接个人信息，“与直接个人信息相比，间接个人信息并非不具备可识别性，而是不具有直接识别的可能性。某种单个信息可能不能识别特定自然人身份及其活动情况，将不同信息组合起来就具有可识别性”。③ 另一种是已公开的个人信息，包括自行公开的个人信息与其他依法公开的个人信息。已公开的个人信息之所以归入到外围层，是由于这类信息处于“法

①高富平：《个人信息流通利用的制度基础：以信息识别性为视角》，《环球法律评论》2022年第1期。
②顾理平：《面子里的人格尊严：智媒时代公民的隐私保护》，《南京师大学报》（社会科学版）2022年第4期。
③张勇：《敏感个人信息的公私法一体化保护》，《东方法学》2022年第1期。

律不设禁”的状态，通常情况下允许收集和处理。考察《民法典》第1036条及《个人信息保护法》的规范目的，立法者鼓励对已公开的个人信息进行合理利用，在一般情形下，个人信息的公开应当成为一般的民事免责事由。[①] 其中，自行公开的个人信息之所以不设禁，是由于个人通过自行公开的行为已经放弃了对个人信息匿名性的保护；而其他依法公开的个人信息，可能是国家机关依法收集公开、出于公共利益或者信息主体利益考量而公开等情形。

三、路径选择：个人信息有序共享的制度安排

数字经济时代的社会结构变迁引起了个人信息法律制度的更迭变化，法律调整着变化过程并促进了新制度的生成。在个人信息法律制度中嵌入有序共享理念，一方面需要根据个人信息的内在层次结构形成个人信息的核心层、中间层、外围层的差序保护格局，另一方面需要基于整体法秩序视角引入合规制度，进一步规范个人信息从诞生到消亡的全生命周期的处理活动。

（一）个人信息差序保护格局的制度设计

学界有力观点认为，同意是个人信息处理活动合法化的基础，应当作为个人信息处理的核心原则。[②] 由于“个人信息不仅关涉个人利益，而且关涉他人和整个社会利益”，[③]因而同意的适用需要受到适度限制。基于这种考量，《个人信息保护法》并没有将同意作为总则中个人信息处理的核心原则，而仅将其作为下位的规则。当然，这并不意味着同意的地位发生根本变化，构建个人信息有序共享制度，其核心连接点仍然是同意。根据个人信息所处的层次位置不同，其流通共享对同意程度的要求也应当有所差异，由此可构建个人信息核心层、中间层、外围层的差序保护格局。

1. 核心层的个人信息保护与授权同意

核心层的个人信息由于触及个人生活的最私密领域，关乎人格尊严，因而这类信息接近于人格权且具有高度的排他性，相应的信息主体具有高度的自决权。从尊重私人领域及个人信息高度自决权的角度来看，核心层的个人信息仅有少量流通共享的空间，这类个人信息的流通共享应当遵守最严格的同意规则即授权同意。例如，身份证号码、基因序列、个人在家庭中的影像资料等，信息处理者处理这些个人信息时，必须征得信息主体的授权同意，没有授权同意的处理行为即属违法。

为了充分保护核心层的个人信息，在授权同意的场景下，信息处理者有义务审查信息主体授权意思的真实性并保障流程的合法合规性。例如，信息处理者采集他人身份证号码时，必须由信息主体本人录入，并且核对身份证原件照片及人脸识别信息，确认无误后才能被认为已经获得授权同意。单纯录入身份证号码，没有身份证原件照片及人脸识别信息等比对确认的，不能推定得到信息主体本人授权，由此对信息主体产生不良影响的，信息处理者应当承担责任。

基于核心层个人信息具有高度私密性特征，处理这类信息应当将用途特定化，遵循“一用途一授权”的原则。为了防止信息处理者在获得授权同意后在平台或一定范围内随意处理个人信息，应当根据用途来锁定个人信息的使用范围，实现对核心层个人信息的精准保护，这一模式在相关立法规范中也有所体现。例如，2013年1月21日《征信业管理条例》第42条规定，超过约定用途使用征信方面的个人信息属违法行为，应当承担民事、行政乃至刑事责任；2022年9月2日《反电信网络诈骗法》第16条也规定，银行有义务按照国家规定提供开户情况和有关信息，这些风险信息不能用于反

①程啸：《论公开的个人信息处理的法律规制》，《中国法学》2022年第3期。
②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。
③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。

电信诈骗网络之外的其他用途。将核心层的个人信息按照“一用途一授权”的模式处理，严格限定其流通共享，体现了对这类个人信息中个人自决权的尊重。

2. 中间层的个人信息保护与知情同意

中间层的个人信息是信息主体自主提供最频繁的个人信息，其私密性相对不高。在数字经济时代，频繁进行的经济、社会活动加剧了个人信息泄露，如网购中需要提供姓名、电话号码等，这些个人信息虽然专属于个人，但是在自然状态下，中间层次的个人信息不足以识别个人的人身、财产等状况，需要组合起来提高可识别性，才能准确识别。而中间层次的个人信息流通共享是数字经济有序运转的重要基础，因此，其同意规则相对于核心层的个人信息而言应当有所缓和。

基于有序共享理念，中间层的个人信息同意规则应当是一般意义上的知情同意，其不需要明确的书面同意，在多数情况下仅需要作出概括同意。例如，App 在信息主体使用时会弹出隐私条款，获取位置信息、个人手机号码等，通常情况下信息主体点击“同意使用”，并且 App 提供了可以拒绝的方式，该 App 的处理行为即可正当化。为了促进中间层次的个人信息的流通共享，对这类信息宜实行“一领域一同意”原则，信息处理者在获得同意之后，有权在平台领域内处理该个人信息而不仅限于特定用途。

3. 外围层的个人信息保护与推定同意

外围层的个人信息的个人属性被大幅度剥离，因而流通共享受限程度最低。这类个人信息的可识别性极低，对个人的影响最小。单纯根据这类个人信息一般不能识别个人的人身、财产状况，因此，其虽然是由个人所产生，且与个人活动有一定关联，但是由于其与个人过于疏远因而导致受保护性较低。在个人信息保护实践中，这类个人信息的处理大多随中间层的个人信息一并授权，采取概括同意规则。不过，这种做法可能并不符合数字社会的既定规则。例如，由于 App 或网页产生的信息是在信息主体使用之后产生的，与其说是在事前进行了概括同意，毋宁说当新的信息产生之后，根据平台规则推定信息主体同意，平台处理此类个人信息的行为由此具备合法性。因此，对于私密性最低的外围层个人信息，没有必要采取概括同意规则，仅需采取推定同意规则即可。第二种类型的个人信息是已公开的个人信息。由于这类信息由信息主体自行公开或者其他情形依法公开，因此，处理这类个人信息时只要在公开的范围内、符合公开的目的即可阻却违法性。在此意义上说，在公开范围内、符合公开目的处理已公开的个人信息的行为实质上遵循着推定同意规则。

（二）个人信息全生命周期合规制度的民行刑一体化构建

个人信息处理风险存在于个人信息从产生到消亡的全生命周期，个人信息相关制度设计应以此为逻辑起点，对个人信息全生命周期的关键节点问题作出个性化回应。为了避免传统“一法一部门”模式下民法、行政法、刑法之间的衔接障碍，还应当对个人信息领域的制度规范进行民行刑一体化的垂直整合。

1. 个人信息全生命周期的风险类型与流程控制

首先，个人信息搜集风险与控制。搜集个人信息通常有三种方式，分别是用户提供、从第三方搜集以及通过公开网络获取。在用户提供场景下，平台的主要义务是告知，在履行充分告知义务后用户仍然提供的，则应当认为已取得用户同意；在从第三方搜集场景下，根据既往的裁判规则，原则上应当经过“三重授权”，[①]但是，在为了维护信息主体或者公共利益的场合，即使未得到个人信息主体

①所谓“三重授权”，是指在相对开放的平台，信息处理者收集个人信息需要经过“用户 + 平台（企业）+ 用户”三重授权才具有合法性。具体来说，平台（企业）对用户首次收集数据需要用户授权，这是第一重授权；信息处理者通过第三方应用间接获取用户数据，需要该第三方应用对应的平台（企业）授权，这是第二重授权，并且还需要获得用户授权，这是第三重授权。参见北京知识产权法院（2016）京 73 民终 588 号民事判决书、杭州铁路运输法院（2017）浙 8601 民初 4034 号民事判决书。

同意的，其搜集行为也不违法；在通过公开网络获取的场景下，信息主体在一定程度上已经放弃了个人信息权利。由于个人信息已经公开，通常情况下获取已公开的个人信息并不违法。

其次，个人信息存储、管理风险与控制。个人信息处理者应当采取安全保障措施，包括特别声明、技术保护措施等，以确保个人信息不被非法使用、泄露。个人信息处理者未采取安全保护措施的，可能构成行政违法；因未采取安全保护措施，造成个人信息泄露的，还可能构成刑事犯罪。在该环节，个人信息处理者的合规义务主要体现在三个方面：一是设立管理机构、配置处理权限以及加强对企业内部管理；二是采取技术保护措施等防范网络爬虫等技术侵入风险；三是采取合规措施仍然无法避免个人信息泄露的，在发现个人信息泄露之后应当及时采取补救措施以防止风险蔓延。

再次，个人信息使用风险与控制。个人信息使用环节具有场景多元化特征，如个人信息数据共享、自动化决策、跨境流动等。《刑法》第253条之一侵犯公民个人信息罪只处罚3种行为，分别是非法获取、非法提供、非法出售公民个人信息。非法获取个人信息入罪，规制对象是非法的信息流入，非法提供、非法出售公民个人信息入罪，规制对象是非法的信息流出，中间层的非法使用个人信息行为并未完全涵括。这意味着平台依法搜集个人信息之后，其使用行为原则上不构成犯罪。例如，个人信息处理者将个人信息用于自动化决策，按照现行刑法规定不构成侵犯公民个人信息罪。不过，这种非法使用行为在《个人信息保护法》中仍然被禁止，故平台使用合法渠道搜集个人信息时仍要履行合规义务，这种意义上的合规义务并非刑事合规，而应当归属于民事、行政合规之范畴。

最后，第三方关联责任风险与控制。在《个人信息保护法》确立的全生命周期保护模式下，企业不仅要对自身处理个人信息进行合规化管理，还应当负有对关联第三方的合规监管义务。在合法的框架下允许个人信息在不同主体间进行流动，让个人信息在合规治理中创造公共价值，是个人信息有序共享的重要体现。个人信息处理平台对关联第三方的合规监管义务既源于科技伦理与行业规则的共同要求，也是构建行之有效的合规体系的重要课题。考察合规的一般法效果，管理好关联第三方是个人信息平台合规之应有内容，个人信息处理平台将个人信息提供给关联第三方，导致个人信息泄露的，或者有其他侵犯个人信息权益行为的，应当与关联第三方共同承担责任。为了避免陷入第三方关联责任之中，信息处理者应当就与合作方的合作事项进行合规监管，除了在合同中明确作出禁止未经授权泄露个人信息的声明之外，还应当对合作方在合作事项中的不合规行为进行审查，在对合作方履行充分合规监管义务仍然无法避免合作方的不法行为时，信息处理者可以免责，由合作方就个人信息非法泄露、非法使用等行为承担责任。

2. 个人信息全生命周期的民行刑一体化合规方案

在《个人信息保护法》颁布之前，我国有关个人信息的立法散布于民法、刑法及其他规范之中，并且总体上表现为“一法一部门”，即一个法律规范仅涵盖民事、行政或刑事规范之一，立法的碎片化特征明显。当《个人信息保护法》实施之后，面对民法、刑法以及其他规范中的碎片化现象，还需要进行第二次的规范整合，消除法法之间的冲突与衔接困境，以民行刑一体化理念促进个人信息在全生命周期中的有序共享与合规建设。

一方面，基于法秩序统一性原理，立法者在制定部门法时既要考虑部门法独立性，也要考虑部门法在整体法秩序中的地位尤其是该部门法与其他部门法之间的关系，消除部门法之间的冲突。“整个法律秩序，也就是大量有效的具体规范与所有法律部门的法律的综合，形成一个统一体、一个‘体系’”，[①]由于我国个人信息立法存在刑事立法先行的客观事实，而《民法典》与《个人信息保护法》一前一后已经进行协调，并无矛盾之处，因此，个人信息领域法秩序不统一、法法不协调问题主要在于

①[德]伯恩·魏德士：《法理学》，丁晓春、吴越译，北京：法律出版社，2013年，第316页。

刑法层面。具体而言:首先,关于个人信息概念,《刑法》第253条之一侵犯公民个人信息罪中的“公民个人信息”应当以《民法典》与《个人信息保护法》中的“个人信息”为参照进行适当扩容,涵盖生物识别信息、宗教信仰信息等,从而确保个人信息概念在不同部门法中的协调一致。其次,根据《侵犯个人信息刑事解释》第2条规定,侵犯公民个人信息罪构成要件中的“违反国家有关规定”,包括违反法律、行政法规与部门规章,这显然是立法者在个人信息有关法律、行政法规较为紧缺的时期,对《刑法》第96条不得已作出的扩张解释。在个人信息立法体系健全的前提下,应当修改该司法解释,将部门规章从国家规定中去除。最后,现行《刑法》第253条之一侵犯公民个人信息罪对中间环节的非法使用行为规制存在明显空白,而《民法典》《个人信息保护法》均重点规制非法使用行为,加上非法使用行为较之非法获取、非法提供、出售等行为具有等质甚至更高的危害性,因此,刑事立法宜将非法使用个人信息行为犯罪化,以填补立法漏洞,提升制裁的实效性。

另一方面,基于民行刑一体化理念下民事、行政、刑事制裁的梯度关系,对侵犯公民个人信息行为的治理宜以必要性为限度。具体而言:一是坚持先私法后公法,对侵犯公民个人信息的行为宜尽可能控制在私法范围内,民进行退、民先刑后。根据现代法治国比例原则的适合性(Geeigneäßig)原则,社会关系的调整应以私法为优先,超出私法调整范畴的社会关系,不得已需要以公权力介入时,也应当以对私权利的影响最小为限度,同时,还应当考虑消除公权力介入后的不良影响。① 例如,短视频博主在平台上传的视频中包含了大量陌生人的人脸识别信息,其事实上也不可能取得个人信息主体同意。而如果完全根据《个人信息保护法》及《刑法》规定,这种行为不仅涉嫌个人信息侵权,还可能构成侵犯公民个人信息罪,若如此认定,势必引起全民违法现象及大规模犯罪化,不符合数字社会个人信息有序共享规则,应当予以适当调整。行政法与刑法作为公法,原本就是在涉及公共利益等重大事项时才应当介入,个人信息首先作为私法权利而存在,不得未经同意侵害个人信息权利是信息处理者需要遵循的第一重合规义务,当信息主体与信息处理者之间产生纠纷时,优先考虑通过民法中的合同、侵权等制度加以规范调整。二是坚持先行政后私法,行进刑退。“从全体法秩序的视角出发,违法性存在量和质的区别,对法益侵害极其轻微的行为将由于欠缺可罚的违法性而阻却实质不法。”②侵犯公民个人信息罪兼具自然犯和法定犯的特性,这意味着本罪可罚的违法性判断需要同时考虑民法与行政法。③《个人信息保护法》大量规定的个人信息国家保护义务与信息处理者义务,构成了信息处理者行政合规的基本要求,违反此项义务优先承担行政责任。三是穷尽替代政策才可启动刑法。根据刑法谦抑主义,“刑法介入剥夺社会成员的身体、自由、财产等重要法益的场合,必须是刑罚以外的其他社会管控手段无法起到合适效果时,刑法的启动才有正当性”。④ 刑法在个人信息领域之所以容易被滥用,一个重要原因是个人信息作为数字经济时代最核心的资源要素,往往伴随着新技术新业态而生,而新技术新业态诞生之初由于欠缺管制,会经历一段时间的“野蛮生长”时期,在一定时空范围内造成社会的失序,面对这种状况,刑法作为最直接有效的手段成为首要考虑对象,网络爬虫技术、自动化决策技术、区块链技术等领域侵犯公民个人信息罪的过度扩张尽皆源于此。基于此,刑事立法通过修改司法解释适度提高侵犯公民个人信息罪的入罪标准,或许是可行的方案。当然,最为稳妥的做法是,个人信息处理者履行好个人信息权益保护及合规管理方面的义务,配合网信等部门的行政监管调控,从而有效抑制违法行为的产生以及防止轻微违法行为演变为严重犯罪行为。

---

①須藤陽子:《比例原則の現代的意義と機能》,東京:法律文化社,2010年,第23—29頁。
②中山研一、浅田和茂、松宮孝明:《レヴィジオン刑法3:構成要件・違法性・責任》,東京:成文堂,2009年,第136頁。
③姜涛:《新罪之保护法益的证成规则——以侵犯公民个人信息罪的保护法益论证为例》,《中国刑事法杂志》2021年第3期。
④關哲夫:《講義刑法總論》,東京:成文堂,2015年,第21頁。

四、结　语

个人信息从自主支配向有序共享的理念转换与制度构建，是传统社会转向现代社会尤其是数字经济时代的自然演化结果。有序共享理念立足于个人信息作为私法权利与公共资源的双重属性，贯彻该理念必须在制度层面扎牢根基。数字经济时代的个人信息在内容上极具开放性和包容性，相关制度建构必须穿透“个人信息”的表象，在对个人信息分类分级基础上进行二次分层，构建根据信息与个人的亲疏远近关系分别配置保护规则的差序格局。个人信息领域层出不穷的新技术新业态，无力通过单纯立法实现有序共享和有效规制，立足信息处理者视角的合规制度建设，是解决该问题的首选策略。合规制度的契入，赋予个人信息有序共享体系更高的科学性与更强的生命力。

（**责任编辑**：吴　欢）

Legal Theory and System Construction for Orderly Sharing of Personal Information

XIA Wei

Abstract: Although the construction of the “compression” system driven by the transformation from traditional society to modern society has accelerated the construction process of the personal information protection system, it has also deepened the institutional imbalance crisis between the protection of private law rights of personal information and the sharing of public resources. Orderly sharing is the reshaping of the legal position of personal information in the digital economy. Personal information is no longer the right to self-determination of individuals, but the right to defense with both individual and social attributes. On the basis of classifying and grading personal information in legislation, a differential protection pattern featuring core layer, middle layer and periphery layer should be formed according to the importance of personal information in the vertical dimension. In order to promote the orderly sharing of personal information in the digital economy era, the general rules of “presumptive consent”, “authorized consent” and “informed consent” should be established according to the internal hierarchy of personal information. In this way, we will build a system integrating civil, administrative and criminal considerations for personal information protection.

Keywords: personal information; classification and grading; orderly sharing; consent rules; integration of civil, administrative and criminal considerations

About the authors: XIA Wei is Associate Professor at School of Criminal Justice, China University of Political Science and Law (Beijing 100088).