财经法学 No. 1，2022
pp. 18 - 31

个人信息保护“目的限制原则”的反思与重构
——以《个人信息保护法》第 6 条为中心

朱荣荣*

内容提要：目的限制原则作为个人信息处理的基本原则，要求信息处理活动不得溢出信息收集时的初始目的，以保障信息主体对个人信息的自主控制与支配。然而，大数据时代个人信息的多维度利用日趋常态化与复杂化，导致信息处理目的难以在信息收集阶段完全确定下来，严格的目的限制原则忽视了个人信息的利用价值。信息保护与信息利用均为法律追求的价值目标，不能顾此失彼，因此，有必要在个人信息类型化视角下重塑目的限制原则的规范内涵。申言之，处理个人敏感信息必须恪守目的限制原则，禁止超越初始目的范围处理之；处理个人一般信息原则上亦须遵从目的限制原则，但特殊情形下允许超越初始目的而处理信息，前提是不得引发高于信息主体所预期的风险。

关键词：目的限制原则　信息保护　信息利用　个人敏感信息　风险限定

大数据时代，对于个人信息的获取与利用愈益普遍，信息处理者在挖掘、分析个人信息时可能在一定程度上侵害信息主体的合法权益。为规制不当的信息处理行为，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第 6 条确立了目的限制原则，该条规定“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息”。目的限制原则作为个人信息保护制度的基石，[1] 能够有效避免滥用个人信息现象的发生。

随着大数据分析技术的不断发展，社会对于个人信息的利用需求达到了前所未有的高度，目的限制原则要求处理个人信息应当具有明确、合理的目的，且后续的信息处理应当与初始目

* 朱荣荣，南京大学法学院博士研究生。

〔1〕 Vgl. Peter Schantz, DS-GVO Art. 5 Grundsätze für Die Verarbeitung Personenbezogener Daten, in Heinrich Amadeus Wolff, Stefan Brink (eds), BeckOK Datenschutzrecht (33rd edn, 2020), Rn. 12.

的直接相关，极大地压缩了信息利用的空间，不符合信息保护与信息利用动态平衡之立法理念。有鉴于此，有必要对目的限制原则进行深度考察，寻求其在新时代背景下合理的因应之道。

一、目的限制原则的内涵阐释与法理基础

（一）目的限制原则的基本内涵

根据《个人信息保护法》第6条可知目的限制原则包含两个方面，即目的明确与使用限制。前者指收集个人信息应当具有明确、合理的目的，不得过度收集个人信息；后者指个人信息的处理应当与初始目的直接相关，如果信息处理行为超出了初始目的则为法律所不许。可见，目的明确与使用限制是不可分割的有机整体，两者相辅相成、相互制约，目的明确原则是信息处理行为的逻辑起点，只有在收集阶段明确告知信息处理的具体目的并获取信息主体的有效同意方可处理他人信息。同时，为确保信息处理目的的效力性，后续的信息处理行为应当与处理目的直接相关，不得超越初始目的可能的范围恣意处理个人信息，否则目的明确原则将形同具文。

目的明确原则是维护个人基本尊严的重要工具，在收集和利用个人信息时，忽视或淡化“目的”意味着人格尊严将受到严重的侵蚀。〔2〕信息主体与信息处理者之间信息不对称的客观事实要求信息处理者在收集信息之时应当善尽说明义务，避免信息主体因信息的不充分而做出错误的决策。目前，我国《民法典》第1035条、《网络安全法》第41条、《消费者权益保护法》第29条等诸多规范都要求信息处理者明示信息处理的目的，但对于“目的”的具体要求则未言明。《个人信息保护法》第6条规定，目的明确原则应当满足两个要件，即目的明确与目的合理。目的明确性要求收集个人信息应当具有明确的、特定的目的，过于宽泛与模糊的目的可能被认为是不合法的，目的明确性迫使信息处理者在收集信息之前审慎思考信息处理的目的，可以在一定程度上制约信息处理者恣意处理信息。信息处理者在形成明确的信息处理目的之后，还须将此目的以一种可被理解的方式清楚地表达出来，确保相关主体对信息处理目的的认知不存在歧义。关于目的明确性的形式要求，立法没有明文规定，从规范目的来看，目的明确性旨在保障信息主体充分知悉信息处理的目的，因此，信息处理者借助于何种形式表明其目的在所不问。目的合理性要求信息处理目的必须符合社会一般人的事理认知，不得违反基本的伦理道德与公序良俗。目的合理性包含两个要素，即制度层面的目的合法与价值层面的目的正当。目的合法是信息处理的最低要求，信息处理者处理他人个人信息应当具备合法性事由，包括约定事由与法定事由，约定事由指双方当事人可以自行约定信息处理的具体事项，法律不得无故加以干涉。法定事由则指法律所规定的无需获取信息主体同意即可处理信息的事由，包括订立或履行合同所必需、履行法定职责

〔2〕 See Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, The End of the Purpose-Specification Principle in Data Protection, 24 *International Review of Law, Computers & Technology*, 102 (2010).

或法定义务等。目的正当性指收集个人信息必须具有充足的价值基础，合理兼顾信息主体与信息处理者的利益，目的正当性的判定依附于个案具体情境，随着社会的发展以及立法理念的变迁而动态调整。

目前，我国对于使用限制的判定标准采取的是“关联性”，要求信息处理行为不得与初始目的不具有关联性。然而，立法对于“关联性”的具体内涵没有予以明确，《个人信息保护法》认为信息处理行为应当与信息收集时的初始目的具有“直接关联性”，张新宝教授起草的《个人信息保护法（专家建议稿）》主张信息处理行为应当与初始目的具有“合理关联性”。《信息安全技术 个人信息安全规范》（2020 年）则认为，“关联性”包括“直接关联性”与“合理关联性”，其规定“使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围”。对于何谓“合理关联”，《信息安全技术 个人信息安全规范》（2020）并没有给出明确的答案，而是具体描述了属于“合理关联”的信息利用情形，其认为“将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内”。不同于我国，域外立法采取的是“兼容性”标准，第 29 条数据保护工作组指出，不同于初始目的的进一步处理并不意味着与初始目的自动地不兼容，某些情况下，信息处理虽然与初始目的不同，但二者可能是相符的。〔3〕关于“关联性”与“兼容性”的关系，有学者认为，在大数据产业下，数据机构对数据的二次利用往往跟初始目的没有关联性，但这并不意味着一定不相兼容。〔4〕换句话说，较之“关联性”，“兼容性”的涵摄范围更广，“关联性”要求后续的信息处理对于初始目的的严格遵循，可能在一定程度上阻碍大数据产业的发展以及创新型社会的构建。

（二）目的限制原则的法理基础

第二次世界大战结束后，国际社会开始深刻反思战争期间各种非人道的行为，普遍呼吁建立尊重基本人权的法律制度。黑格尔认为，人格的要义在于，我作为这个人，在内部任性、冲动和情欲以及在直接外部的定在等一切方面都完全是被规定了的和有限的，并在有限性中知道自己是某种无限的、普遍的、自由的东西。〔5〕当前，不论英美法系抑或大陆法系，相关制度安排均强调对于个人信息的利用不得以牺牲人格尊严为代价。受社会和他人尊重是人的一种基本需要，是人作为法律关系主体所享有的最基本的人格价值，自然人维护个人信息的准确性、控制个人信息的利用范围是保证个人尊严得到社会认可的体现。〔6〕在“小数据时代”，由于信息收集技术与收集能力普遍处于不发达状态，信息主体尚能有效控制信息是否被处理以及处理的方式，然而，随着大数据技术的突飞猛进，通过个人信息介入个人生活的广度和深度实现了从量变到质变，当个人成为纯粹的“个人信息客体”，被随意监控、分析和操纵，个人的内在决策和外在形象都被控

〔3〕 See Article 29 Data Protection Working Party, Opinion 03 /2013 on purpose limitation 15 (Article 29 Data Protection Working Party 00569/13/EN 2013), p. 21.

〔4〕 参见谢琳：《大数据时代个人信息使用的合法利益豁免》，载《政法论坛》2019 年第 1 期。

〔5〕 参见〔德〕黑格尔：《法哲学原理》，范扬、张企泰译，商务印书馆 2017 年版，第 51 页。

〔6〕 参见张涛：《个人信息的法学证成：两种价值维度的统一》，载《求索》2011 年第 12 期。

制时，个人作为人的完整性和主体地位便已分崩离析，个人的独立和尊严将直接受到挑战。〔7〕为稳固个人的主体性地位，《个人信息保护法》构造了以“人”为中心的制度体系，确保个人对信息的自主性与控制性，目的限制原则即是个人控制体系中重要的组成部分。

目的限制原则要求信息处理者在收集信息时明确告知信息主体信息处理的具体目的，并严格限定后续信息处理的方式，同时给予信息主体同意或反对的权利，能够在一定程度上保障信息主体自主控制信息被以何种方式处理，防止信息处理者以信息主体未能预见到的方式处理信息。自主决定与自愿承担风险是私人自治的重要体现，尊重个人自主决定是否接受信息处理可能造成的风险形塑了个人自治空间，法律对于信息主体真实的意思表示应予尊重，不得任意干涉。作为个人信息的原始所有者，信息主体对于个人信息的收集与利用享有绝对的支配力与控制力，除法律明确规定信息处理的合法性基础外，信息处理者只有在获得信息主体的同意或授权时才能收集或利用信息。目的限制原则要求信息处理者在收集信息阶段应向信息主体详细披露信息处理的方式、可能产生的风险等事项，并承诺在约定的目的范围内处理信息。一般而言，借由信息处理者收集信息时的说明义务，信息主体能够预判让渡信息可能需要承受的风险，并在此基础上作出是否许可他人使用其信息的意思表示。信息主体对于自我信息的控制力与支配力是目的限制原则的理论基础，亦是制约信息处理者尊重目的限制原则的动力来源，只有承认信息主体有权自主决定信息被如何收集与利用，才能促使信息处理者主动寻求信息主体的授权许可。为了获得信息主体的有效同意，信息处理者须将信息处理的目的向信息主体明示，并承诺在约定的目的范围内处理信息，信息处理者超过约定的目的范畴处理信息可能承担违约或侵权责任。

二、大数据时代目的限制原则的现实困境

目的限制原则的效力范围从信息收集开始，及于整个信息处理过程，在包括个人信息的存储、变更、传递与使用等的各个阶段，始终可以发挥其作用。〔8〕目的限制原则这种充足的法律效力力求全面保障信息主体的合法权益，然而在具体实践中，目的限制原则面临以下诸多龃龉。

（一）信息处理目的难以在收集阶段完全确定

目的限制原则要求信息处理的目的应在不迟于信息收集之时予以确定，且目的必须是明确的、合理的。目的限制原则可以有效保证信息主体事先知道信息利用的目的和范围，并能够控制信息收集在事先约定的范围内进行。〔9〕然而，在信息的流转、共享等信息的二次利用成为信息产业普遍遵循的商业运作模式的背景下，传统的目的限制原则受到挑战。目的限制原则依赖于一个前提条件，即信息处理目的在收集信息之时予以确定是可能的，然而大数据分析技术的价值恰恰在于提取隐藏的信息或对信息进行变革性利用，这使得信息处理者无法在信息收集阶段详细阐

〔7〕 参见郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 84 页。

〔8〕 参见谢永志：《个人数据保护法立法研究》，人民法院出版社 2013 年版，第 57 页。

〔9〕 参见王秀哲：《大数据时代个人信息法律保护制度之重构》，载《法学论坛》2018 年第 6 期。

明信息的所有可能用途。〔10〕于此情形，信息处理者为保障信息处理活动的顺畅进行，倾向于将信息处理目的以一种模糊或宽泛的方式表达出来，导致信息主体无法预期后续的信息处理行为，这种信息的不对称可能引发社会歧视、差别性对待等不公平现象。

目的限制原则要求对于信息的处理必须与信息收集时的初始目的具有直接相关性，反向推之，当信息处理目的与初始目的不一致时，信息处理者应当及时告知信息主体变更目的的缘由并再次征得信息主体的同意。大数据技术的运用使得在信息收集、利用、存储等任何阶段都可能发生信息主体同意信息收集时所未预期的信息处理方式，过于频繁地向信息主体告知变更事项不仅增加了信息处理者的工作负担，也在一定程度上干扰了信息主体的正常生活。此外，目的限制原则植根于私人自治理论，该理论预设信息主体只有充分了解信息处理目的才能决定是否将信息移交给信息处理者。然而，大数据环境中信息处理的复杂性，尤其是自动化决策技术的运用，增加了信息主体理解与选择的难度。实践中，信息主体很少仔细阅读冗长而繁杂的隐私协议，或者囿于自身有限的理性及相关知识的匮乏难以理解具体条款的含义，减损了信息主体同意的有效性。更为重要者，由于信息主体与信息处理者在市场地位、议价能力等方面具有实质不对等性，信息主体即使认识到隐私协议的不合理性也无法要求信息处理者对相关事项予以更正。

（二）忽视了个人信息的利用价值

个人信息所承载的利益形态具有多元性与复杂性，随着大数据处理技术逐渐渗入社会生活各个方面，在日常的人际交往与社会生活中，个人需要不断地与他人交换信息，公务机关与非公务机关亦频繁收集大量信息以改善行政管理或提供更好的服务，社会对于个人信息的客观需求愈益增多。实际上，个人信息不仅与人格尊严及人格自由密切相关，更是相关产业存在和发展的基石，因此不能只关注信息保护，而应将信息保护与信息利用放在同一维度。〔11〕值得肯定的是，立法不再单方面强调信息主体利益的保护，欧盟《一般数据保护条例》（General Data Protection Regulation，GDPR）及我国《个人信息保护法》都开宗明义地指出，应注重信息保护与信息利用之间的平衡。近年来，我国信息产业发展迅速，对个人信息利用的需求也越来越大，大数据分析技术通过结合不同来源的数据可能发现新的趋势、模式和关系，目的限制原则制约了大数据的规模和使用，可能造成经济和社会效益的重大损失。〔12〕根据目的限制原则的逻辑进路，当信息处理目的实现时信息处理者必须尽快删除个人信息，不得留存个人信息，更不得将信息用于其他目的，这严重降低了信息的利用效率，阻碍了信息价值的开发与再利用。从实际层面考量，多数情况下大数据分析所涉及的方法和使用模式是信息处理者以及信息主体在收集信息时没有预料到的，为了遵守目的限制原则，信息处理者必须密切监视处理过程以确保信息处理没有超出约定的范围，然而采取这些措施可能是代价高昂的、困难的甚至是不可能的。〔13〕

---

〔10〕 See Alessandro Mantelero，The Future of Consumer Data Protection in the E. U. Rethinking the “notice and Consent” Paradigm in the New Era of Predictive Analytics，30 *Computer Law & Security Review*，643－660（2014）.

〔11〕 参见谢远扬：《〈民法典人格权编（草案）〉中“个人信息自决”的规范建构及其反思》，载《现代法学》2019 年第6 期。

〔12〕 See Bart Custers，Helena Ursic，Big Data and Data Reuse：A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection，6 *International Data Privacy Law*，5（2016）.

〔13〕 See Tal Z. Zarsky，Incompatible：The GDPR in the Age of Big Data，47 *Seton Hall Law Review*，1006（2017）.

大数据时代的一个显著特征是，个人信息的价值不再单纯地来自其基本用途而更多源于信息的二次利用，很多信息在收集之时并无意用作其他用途，最终却产生了很多创新性的用途。〔14〕目的限制原则要求信息处理的方式应严格限定于初始目的范围内，不利于新产品、新服务的研发。此外，目的限制原则过于强调信息主体利益的保护，忽视了目的范围之外的信息利用可能造福于社会。2008 年，Google 公司利用用户的搜索关键词成功预测流感爆发趋势即为很好的例证，Google 公司最初收集用户搜索关键词的目的在于改善搜索引擎功能，对于流感趋势的预测显然逾越了 Google 公司收集信息时的初始目的，但毋庸置疑的是，流感趋势预测对于公共卫生部门及时采取防治措施提供了较大帮助。可见，严格的目的限制原则不符合大数据背景下信息多样性利用的现实需求，阻碍了信息经济与信息产业的进一步发展。

三、目的限制原则的改革方案及评价

（一）域外立法变革路径——以欧美为考察对象

目的限制原则最早由美国学者艾伦·威斯汀（Alan Westin）提出，威斯汀主张政府所收集的个人信息只能用于特定目的，不得用于其他目的或者进一步流转，除非提供信息的个人或群体的身份特征已经完全从该信息中移除，或者他们自由地对进一步流转表示同意。〔15〕立法上，目的限制原则可以追溯至 1980 年的《关于隐私保护与个人数据跨境流动的指南》，可以说，欧美国家对于目的限制原则关注的时间较早，积累了丰富的经验，通过考察欧美法的相关规定，可以为我国目的限制原则的优化调整寻求经验借鉴。

为缓和严格的目的限制原则适用上的僵硬性，95 指令规定了“兼容性使用”（compatible use），但并未正面规定“兼容性使用”的具体内涵以及判断标准，以致欧盟国家在评估兼容性时采取了不同的判定标准。具体来说，比利时主要根据信息主体的“合理期待”来判断兼容性，英国和希腊则通过“公平性”（fairness）与“合法性”（lawfulness）衡量兼容性，德国和荷兰则借助于“平衡测试”（balance tests）加以判定。〔16〕2013 年，第 29 条数据保护工作组发布了有关目的限制原则的意见书，明确指出“不同于初始目的的进一步处理并不意味着与初始目的自动地不兼容，在某些情况下，虽然信息的处理与初始目的不同，但二者可能是相符的”〔17〕。关于如何判定“兼容性”，第 29 条数据保护工作组认为应当考虑信息收集目的与信息处理目的之间的关系、信息收集的具体情境与信息主体的合理预期、信息的性质与信息处理对信息主体的影响以及

〔14〕 参见〔英〕维克托·迈尔－舍恩伯格、肯尼斯·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 197 页。

〔15〕 参见梁泽宇：《个人信息保护中目的限制原则的解释与适用》，载《比较法研究》2018 年第 5 期。

〔16〕 See Judith Rauhofer, Look to Yourselves, That We Lose Not Those Things Which We Have Wrought: What Do Proposed Changes to the Purpose Limitation Principle Mean for Public Bodies' Rights to Access Third-Party Data, 28 *International Review of Law, Computers & Technology*, 146－147 (2014).

〔17〕 前引〔3〕，第 21 页。

信息处理者采取的保障措施等。〔18〕《一般数据保护条例》承继了第 29 条数据保护工作组关于兼容性使用的判定方式，成为指导欧盟域内判断信息处理是否合乎初始目的的重要依据。有学者认为，虽然相关立法列举了“兼容性”的考量因素，但实践中判定信息处理是否与初始目的相兼容，仍需根据个案具体情境加以判断。〔19〕有学者更是直言，“兼容性评估”在大数据背景下有些抽象和困难，兼容性评估要求考虑信息收集时的具体情境、信息的性质等各种因素，而大数据的运行需要分析不同环境中的数据，使得静态的要素评价几无可能。〔20〕“兼容性使用”作为一个转接通道，为超越初始目的之外的信息利用提供了理论基础，缓和了信息保护与信息利用之间的紧张关系，拓展了信息利用的空间，具有一定的积极意义。然而，“兼容性使用”在判断后续的信息处理是否具有正当性时仍以信息收集时的初始目的为基点，忽视了时间、环境等外在因素的变迁可能导致信息处理目的的更迭。2017 年，第 108 号公约协商委员会主张，不应以信息主体可能认为无法预料的、不适当的或令人反感的方式处理信息，将信息主体暴露于不同的风险或比初始目的所预设的更大的风险，可以视为以无法预料的方式处理信息。〔21〕指南改变了欧盟一直以来所遵循的目的限制原则的调整思路，为目的限制原则在新时代背景下的灵活运用开辟了新的方向，遗憾的是，指南仅具有参考性意义，不具有强制的法律效力。

不同于欧盟立法，美国主要通过场景规则的构建来改革目的限制原则所面临的困境，场景规则的提出与美国隐私概念的不确定性有关，自 1890 年沃伦（Samuel D. Warren）与布兰迪斯（Louis D. Brandeis）提出隐私这一概念以来，理论界关于隐私的具体内涵一直存在争议。在此背景下，美国学者海伦·尼森鲍姆（Helen Nissenbaum）提出了场景完整性理论（contextual integrity theory），主张隐私的保护应与特定情境联系起来，信息的收集和传播应当符合具体情境并遵守特定情境下的相应规则，隐私是否受到侵害需要综合考量具体场景下的多种因素。〔22〕场景完整性理论由于其强大的包容性与灵活性得到立法者的青睐，2012 年，白宫在一份文件中明确提出“尊重场景原则”（respect for context principle），消费者有权期待企业收集、使用以及披露个人数据的方式与其提供数据时的场景相一致。〔23〕与此同时，联邦贸易委员会强调在符合一定场景下企业可以直接收集或使用消费者信息而无需征得消费者的同意，除非企业以信息收集时所声称的实质性不同的方式使用信息或出于某些目的而收集敏感信息。〔24〕2018

〔18〕 参见前引〔3〕，第 23－26 页。

〔19〕 See Bert-Jaap Koops, The (In) Flexibility of Techno-Regulation and the Case of Purpose-Binding, 5 *Legisprudence*, 179 (2011).

〔20〕 See Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 *Seton Hall Law Review*, 1008 (2017).

〔21〕 See Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, available at https://rm.coe.int/16806ebe7a, last visited on May 27, 2021.

〔22〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Washington Law Review*, 136－157 (2004).

〔23〕 See See White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf, last visited on Aug. 20, 2021.

〔24〕 See Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid change, March. 2012, available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, last visited on Jul. 19, 2021.

年，《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）吸收了“尊重场景规则”，法案明确“若个人信息的处理符合信息收集时的具体情境，则认为信息处理行为是合理的、适当的”〔25〕。“尊重场景规则”主张不应严格固守信息收集时的初始目的，若后续的信息处理符合信息收集时的具体场景则判定信息处理行为是合法的，但“场景”具有流动性与易变性，不利于当事人合理预期的形成。有鉴于此，2020 年的《加州隐私权法案》（The California Privacy Rights Act，CPRA）对目的限制原则进行了调整，采取“初始目的”与“场景路径”双重认定模式，其规定“企业收集、使用、存储、共享消费者个人信息应当是合理的、必要的，并且与信息收集时的初始目的相符，或具有与信息收集时的情境相适应的其他披露目的”。易言之，若个人信息的后续处理与初始目的或信息收集时的场景相符，就应当认定为正当的信息处理行为。

（二）理论界的改革方案

大数据环境下，目的限制原则暴露出来的弊端愈来愈多，学界对此进行了反思并提出不同的改革方案。“合法利益测试说”认为“目的限制原则”已经无法适应社会发展的需要，应当评估为实现某项合法利益可以在何种程度上正当化信息处理行为，以此决定信息处理行为是否妥当。〔26〕“扩张解释目的说”主张综合考量信息收集时的情形、信息的性质以及信息处理对信息可能造成的后果等因素，来扩张解释信息收集时初始目的，禁止任何逾越初始目的的信息利用行为。〔27〕“风险限定说”建议融入场景与风险的理念，以“风险限定”替代“目的限定”，亦即处理个人信息不能引发高于原有程度的、用户无法预期的风险。〔28〕风险限定论认为，判定信息的利用是否具有正当性关键在于信息处理是否引发了不合理的风险，这种不合理的风险包括精神压力、差别待遇、人身财产损害的可能性以及是否符合信息主体的预期与信息披露时的情境。〔29〕

关于前述改革方案，“合法利益测试说”的观点较为激进，其认为应当彻底放弃“目的限制原则”的基础性地位，主张以“合法利益”作为信息处理是否具有正当性的唯一判断标准，如果信息处理是为实现某项合法利益所必需，则该信息处理具有妥适性，反之则否。“合法利益测试说”在一定程度上缓和了后续信息处理受限于初始目的的局限性，能够为实践中信息处理的适时变动提供理论依据。然而，“合法利益”是模糊且抽象的法律概念，其具体内涵及外延有待于个案情境中予以判定，由此可能导致不同主体对于“合法利益”存在不同的解释，无法为司法实践提供明确的指导。从实际层面考量，信息主体由于信息不对称、专业能力的匮乏等现实因素很难举证证明信息处理者所声称的“合法利益”是否合理，可能致使“合法利益测试”异化为强势地

〔25〕 The California Consumer Privacy Act of 2018（CCPA），available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121，last visited on Jul. 11，2021.

〔26〕 See Lokke Moerel，Corien Prins，Privacy for the Homo Digitalis：Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things，available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123，last visited on Apr. 23，2021.

〔27〕 参见前引〔15〕，梁泽宇文。

〔28〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 年第 5 期。

〔29〕 参见李媛：《大数据时代个人信息保护研究》，华中科技大学出版社 2019 年版，第 200 页。

位的信息处理者肆意处理他人信息的辩护工具。“扩张解释目的说”避免了后续信息处理溢出初始目的范围可能面临的“目的落空”之诘问，保障了“初始目的”存在的价值，但其通过采取综合考量模式来扩张解释信息处理的初始目的不仅不合理地改变了原本意义上的“目的”，还在一定程度上淡化了目的明确性，导致当事人无法产生合理的预期。需明确的是，个人信息保护并非旨在保护信息本身不被收集、利用，而是保护信息主体免受信息处理可能造成的伤害，严格限制信息的收集而放松信息的利用不符合时代发展趋势。“风险限定说”不要求信息处理者对于初始目的的严格遵循，只要信息处理者将信息处理可能引发的“风险”控制在合理范围之内就可以自由处理信息，符合实践中多元化的信息利用需求。然而，罔顾信息收集时的初始目的，不利于信息主体合理预期的形成以及社会的有序发展。

四、个人信息的类型化分析

（一）个人信息类型化的必要性

1. 个人信息固有的差异性

个人信息范围广泛、种类繁杂，不同的个人信息与自然人的关联性是不同的，面对丰富庞杂的个人信息集群，统一个人信息的保护模式忽视了个人信息的差异性及其对个人的影响程度，因此，区分规制个人信息从而提供更为细致的保护实乃现实必需。

司法实践中，法院首先认为信息的内容决定信息处理风险的高低，如果所涉信息的内容是普通个人信息，则诉请通常不会得到法院的支持，但如果相关的个人信息涉及当事人的隐私，或者个人信息属于敏感事项，那么相关的诉请就有很大的可能获得法院的支持，因此，只有对受保护的个人信息进行类型化处理，才能“避免个人信息概念的模糊性缺陷，防止规范适用的空洞化”〔30〕。个人信息固有的差异性要求我们对不同个人信息给予不同程度的保护，这是平等原则的内在要求，平等并非意味着忽视个人信息的差异性刻意追求均等化保护。平等原则包括两重含义：平等的必须平等对待，不平等的必须不平等对待。这意味着平等原则不仅仅允许差别的存在，而且允许差别对待。〔31〕个人信息之间天然地存在差异，不加区分地对所有个人信息实行同等保护，违背了平等原则的实质内涵。

2. 促进信息市场有序发展

历史上，无数次思想启蒙与思想解放运动的经验告诫我们，人类从愚昧无知走向文明发展的关键就在于信息的获取与利用。目前，信息的共享与流通已成必然趋势，信息壁垒逐渐被打破，任何阻碍或隔绝信息流通的行为都是违背社会实际发展现状的。信息时代对于个人信息利用的内在需求要求我们必须摒弃传统的只关注于信息主体利益的滞后观念，适度地释放信息的经济价值才能有利于社会的有序发展。在信息处理过程中，信息主体的利益与信息处理者的利益处于持续

〔30〕 前引〔11〕，谢远扬文，第 146 页。

〔31〕 参见〔德〕伯恩·魏德士：《法理学》，丁小春、吴越译，法律出版社 2003 年版，第 165 页。

的博弈之中，过于强化信息主体利益的保护，必将侵蚀信息的合理利用空间；反之，偏重信息处理者的利益，则势必影响信息主体的利益。

大数据时代，信息经济已成为我国市场经济发展的重要组成部分，个人信息一体化的保护模式增加了信息处理者处理信息的顾虑，信息处理者可能因惧怕动辄承担法律责任而放弃信息产品的研发与升级，这对于我国信息产业的长足发展是不利的。从成本收益的角度分析，统一保护模式虽然使公民信息得到了绝对的保护，但国家为此投入了大量成本，包括司法成本、社会成本等，总体上无益于社会效益的增加，因而并非是最优的资源配置方式。〔32〕

（二）个人信息类型化的路径选择

1. 个人信息类型化的理论尝试与规范应对

关于个人信息的类型化区分，我国理论层面与规范层面存在不同的观点，就理论层面来说，可谓众说纷纭，以下简要概述。有学者依据个人信息与人格关系的紧密程度将个人信息区分为人格紧密型个人信息和人格疏远型个人信息，凡符合直接识别性、敏感性、个体性强三个特征之一的个人信息即为人格紧密型个人信息，反之则为人格疏远型个人信息。〔33〕还有学者立足于个人信息生命周期及其在不同周期阶段呈现的利益形态，将个人信息划分为个人私密信息、个人事实信息以及个人预测信息。〔34〕还有学者将个人信息划分为自然性个人信息与社会性个人信息，自然性个人信息是信息主体与生俱来且无法轻易改变的信息，社会性个人信息是信息主体为了社会生活所必须而由个人主动或被动地获取的相应符号或信息。〔35〕由上述不完全列举可知，我国学者在个人信息类型化问题上各执己见，但其区别规制个人信息的意旨均在细化个人信息的保护方式，并在此基础上平衡信息主体与信息处理者的利益。

就规范层面来说，截至目前，我国诸多规范均对个人信息的类型化予以了明确规定。2012年发布的《信息安全技术 公共及商用服务信息系统个人信息保护指南》第3.2条明确表示“个人信息可以分为个人敏感信息和个人一般信息”。《民法典》第1034条第3款依据信息的私密性将个人信息区分为私密信息与非私密信息，第1036条则根据公开与否将个人信息区分为已经合法公开的个人信息与未公开的个人信息。新近颁布的《个人信息保护法》延续了区别规制个人信息的立法理念，将个人信息区分为个人一般信息与个人敏感信息以及已公开的个人信息与未公开的个人信息。可见，我国立法对于个人信息的类型化存在不同的规定，由此引发的问题是，不同类型化的个人信息之间可能存在交叉重叠之处，例如，性取向可能同时属于个人敏感信息、私密信息以及非公开个人信息，此时应当选取何种保护路径不仅关系当事人合法权益的保护，还关系法律体系的内在协调。

---

〔32〕 参见董悦：《公民个人信息分类保护的刑法模式构建》，载《大连理工大学学报（社会科学版）》2020年第2期。

〔33〕 参见项定宜、申建平：《个人信息商业利用同意要件研究——以个人信息类型化为视角》，载《北方法学》2017年第5期。

〔34〕 参见袁泉、王思庆：《个人信息分类保护制度及其体系研究》，载《江西社会科学》2020年第7期。

〔35〕 参见刘迎霜：《大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角》，载《社会科学》2019年第3期。

2. 个人信息类型化的理想选择

上述个人信息类型化的学说有一定的说服力，但都不足以成为重构目的限制原则的根本性的类型划分。笔者认为，以信息的敏感度将个人信息区别为个人一般信息与个人敏感信息进而对目的限制原则采取不同的解释路径，能统筹兼顾信息主体利益与信息处理者利益，实现信息保护与信息利用之间的动态平衡。根据《个人信息保护法》第 28 条之规定，“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息”。可见，个人敏感信息与个人一般信息的区分触及了个人信息保护实质意义上的差异性，较之于个人一般信息，侵害个人敏感信息对信息主体造成的损害更为严重，因而需要对其予以更严格的保护。

此外，以个人敏感信息与个人一般信息的区分来构建个人信息保护规范体系符合国际立法趋势，也契合了我国的立法规范。目前，比较法上大多国家和地区采取区别规制个人敏感信息与个人一般信息的立法体例。例如，1981 年欧洲理事会颁布的《关于个人数据自动化处理的个人保护公约》、2018 年生效的《欧盟一般数据保护条例》、2018 年日本修正的《个人信息保护法》等。我国规范层面，《民法典》《个人信息保护法》《征信业管理条例》以及《信息安全技术 公共及商用服务信息系统个人信息保护指南》《信息安全技术 个人信息安全规范》等诸多规范性文件或直接或间接规定了敏感信息。司法实践中，法院亦认为应当对于敏感信息予以特殊对待。在“罗某与巢某土地登记纠纷”一案中，法院认为，合法权利人对于房屋相关权属信息为个人敏感信息，在非法定情形下，未经权利人同意不应公开。〔36〕在“朱烨与百度网讯科技公司隐私权纠纷”一案中，法院认为，将个人信息区分为个人敏感信息和非个人敏感信息的一般个人信息而允许采用不同的知情同意模式，能够在保护个人人格尊严与促进技术创新之间寻求最大公约数。〔37〕可以说，个人敏感信息与个人一般信息的区别规制能够成为我国个人信息分类保护的基础性框架，是适合于我国个人信息类型化保护的理想的路径选择。

五、类型化视角下目的限制原则的重构

（一）个人敏感信息：禁止目的外利用

个人敏感信息与信息主体的人格尊严以及人格自由密切相关，非法收集或不当利用敏感信息可能对信息主体的人身权益造成严重损害，这种损害不局限于隐私侵害，而是包括财产损失、歧视性待遇、精神伤害等在内的各种形式的物质性以及非物质性损害。处理敏感信息具有高度的危险性，因而在处理敏感信息时应当恪守目的限制原则，禁止超越初始目的范围处理敏感信息。

〔36〕 参见江苏省南京市中级人民法院（2020）苏 01 行终 480 号行政判决书。

〔37〕 参见江苏省南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

如前所述，收集个人敏感信息必须具有明确、合理的目的，其中“合理性”的判定涉及价值层面冲突关系的利益衡量，可以借助于公法上的比例原则进行判定。比例原则缘起于德国警察法，后发展为公法领域的“帝王条款”，比例原则内含三个子原则，即适当性原则（Geeignetheit）、必要性原则（Erforderlichkeit）及狭义比例原则（Verhltnismigkeit im engeren Sinne）。〔38〕近年来，比例原则在我国呈现出不断扩张的趋势，不仅行政法、刑法等公法领域强调比例原则的指导价值，私法领域也逐渐认可比例原则的作用空间，更有学者主张比例原则应当作为民法的一项基本原则，强调比例原则在私法领域的普适性。〔39〕比例原则作为方法论意义上的工具性原则，〔40〕考察的是目的与手段之间是否均衡，处理敏感信息是否具有“合理性”亦在评价信息处理者的处理行为与其所意愿达成的目的之间是否合理，与比例原则内蕴的价值取向具有一致性。此外，比例原则内含的三个子原则呈现阶层式的构造，在具体适用上具有严格的顺序限制。比例原则的阶层式构造以及顺序判断模式提供了精致的分析工具，使得“合理性”的判定既不过于空洞也有章可循。具体来说，适当性原则要求信息处理者的行为应当有助于合法利益的实现，此处的“合法利益”应作广义的解释，不仅包括法律明确规定的正当性利益，还包括法律虽然没有明确规定但从规范目的可推导出的合法性利益。需注意的是，适当性原则要求信息处理者的行为具有实现合法权益之可能性即可，并不要求该合法利益必须真切地实现，由于事物的普遍联系性，客观上有利于实现合法利益的信息处理行为可能无限绵延，行为的作用力大小亦不相同，但不得将过于遥远的作用力纳入合理性范畴，否则可能堵塞信息主体获取救济的途径。必要性原则要求信息处理者在处理敏感信息时必须选择对信息主体侵害最小的处理措施，且所采取的措施必须具有经济性与便利性，若实现该信息处理目的成本过高，应否定信息处理行为的合理性。均衡性原则要求处理敏感信息可能对信息主体利益造成的损害应当与所要实现的目的具有相称性，不能显著失衡，相称性内蕴多元的价值评价，需要在具体个案中综合考量。

（二）个人一般信息：适度允许目的外利用

大数据时代，个人的生活交往以及社会的存续发展离不开个人信息的收集与利用，对于与信息主体联系不甚紧密的个人一般信息，应更多关注于其在社会生活中的流转与利用，原则上来说，信息处理者必须谨遵目的限制原则，但为满足社会对于信息利用的需求，应当允许信息处理者在一定条件下超越初始目的范围利用信息，前提是不得给信息主体造成不合理的风险。

现代社会是风险社会，各种各样的风险无处不在。贝克认为，风险的概念直接与反思性现代

〔38〕 Vgl. Landessozialgericht Hamburg. Begrenzung der Erlschenswirkung bei Nichtanzeige einer Beschftigung，2006 Heft 1，S. 18.

〔39〕 参见郑晓剑：《比例原则在民法上的适用及展开》，载《中国法学》2016 年第 2 期；纪海龙：《比例原则在私法中的普适性及其例证》，载《政法论坛》2016 年第 3 期。

〔40〕 See Aharon Barak，Proportionality，Constitutional Rights and Their Limitations，Cambridge University Press，2012，p. 131.

化的概念相关，风险可以被界定为系统地处理现代化自身引致的危险和不安全感的方式。〔41〕还有学者认为，风险是某种不可预见情形出现的可能性，其可能是自然事件或人类活动的结果，也可能是两者共同作用的结果。〔42〕可见，“风险”一词具有多重面向，其在不同语境中具有不同的含义。个人一般信息更多体现为信息利用价值，因此不宜片面强调信息处理对于初始目的的严格遵循，而应要求信息处理者将信息处理可能引发的风险控制在合理范围之内，以符合大数据时代信息多元利用的趋势。一般来说，影响信息处理风险程度的因素主要有以下几项：第一，信息的敏感性程度。个人信息的核心特征在于识别性，识别包括直接识别与间接识别，直接识别指通过该信息可以直接确认某一自然人的身份，间接识别指通过该信息虽然不能直接确认某人的身份，但可以结合其他信息加以确定。〔43〕个人信息的此种特性决定了个人信息的范围具有广泛性与动态性，具体个案中，如果信息的敏感度越高，则信息处理行为受到的限制越多。第二，信息处理者的风险控制能力。特定的行为或活动与特定的风险相联系，当行为人以其行为开启一定的风险或者维持一定的风险状态时，该风险实现时则行为人难辞其咎。〔44〕通常来说，信息处理活动产生的风险是由信息处理者制造的，信息处理者在享受信息处理带来利益的同时亦负有合理控制风险的义务。风险实现的可能性以及风险的严重性与信息处理者控制风险的能力密切相关，信息处理者控制风险的能力越强，则风险发生的可能性越低、风险的严重性亦越低。第三，信息主体的预见能力。合理的信赖受法律保护，信息处理者不得以信息主体基于信息收集时的初始目的所无法预期的方式处理信息。〔45〕信息处理者对于信息主体信赖其以约定方式利用信息的合理预期负有保护义务，不得无故使信息主体的合理预期落空，否则有碍于构建良性的信息处理环境，若信息处理产生的风险高于信息主体的合理预期则为法律所不允许，信息处理者需将相关风险告知信息主体并重新获得信息主体的授权同意。须注意的是，即使信息处理产生的风险在合理范围之内，但信息主体明确表示拒绝接受信息处理的，信息处理者亦不得继续处理信息，除非信息处理者有证据证明信息处理的利益大于信息主体的利益。

六、结　语

法律需要稳定，但不能一成不变，所有关于法律的思考都是在努力调和稳定与变化这两种相互冲突的需求。〔46〕目前，大数据技术渗透到社会生活的各个方面，信息科技的快速变革要求个人信息保护理念应从严格限制信息收集转向平衡兼顾信息保护与信息利用，传统的目的限制原则

〔41〕 参见〔德〕乌尔里希·贝克：《风险社会》，何博闻译，译林出版社 2004 年版，第 19 页。

〔42〕 参见〔英〕罗伯特·鲍德温、马丁·凯夫、马丁·洛奇编：《牛津规制手册》，宋华琳等译，上海三联书店出版社 2017 年版，第 348 页。

〔43〕 参见黄薇主编：《中华人民共和国民法典人格权编解读》，中国法制出版社 2020 年版，第 209 页。

〔44〕 参见叶金强：《风险领域理论与侵权法二元归责体系》，载《法学研究》2009 年第 2 期。

〔45〕 See Dag Elgesem, The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data, 1 *Ethics & Information Technology*, 283－287 (1999).

〔46〕 See Roscoe Pound, Interpretations of Legal History, Cambridge University Press, 1967, p. 1.

无法有效应对社会的发展变化，有必要对其加以修正。

个人信息种类繁杂，不同个人信息与信息主体的紧密程度差异甚大，统一的个人信息保护模式无法合理兼顾信息保护与信息利用之双重价值目标，类型化构建个人信息保护制度实有必要。具体而言，由于个人敏感信息关系信息主体基本的人格尊严，在处理敏感信息时必须恪守目的限制原则，禁止恣意扩大初始目的应有的范围，而对于个人一般信息，可以适度允许超越初始目的范围的信息利用行为，但不得超过信息收集时信息主体能够合理预期的风险。我国《个人信息保护法》虽然规定了目的限制原则，但基本沿用传统的保护路径，存在不足之处，应适度调整目的限制原则的内涵以期助力我国信息产业与信息社会的有序发展。

Abstract：As the basic principle of personal information processing，the purpose limitation principle requires that information processing activities shall not overflow the scope of the original purpose at the time of information collection，which guarantees the subject of the information independent control and dominate over personal information. However，in the era of big data，the diverse use of information is becoming more and more normal，and the purpose of information processing is difficult to be fully determined at the information collection stage. Besides，the strict purpose limitation principle ignores the use value of personal information. Information protection and information utilization are both value goals pursued by the law，and we can't ignore one and lose the other. Therefore，it is necessary to reshape the connotation of the purpose limitation principle from the perspective of personal information typology. In other words，when dealing with personal sensitive information，we must strictly abide by the purpose limitation principle，and processing beyond the scope of the original purpose is prohibited. In principle，the processing of personal general information must also comply with the purpose limitation principle，but under special circumstances，it is allowed to process information beyond the initial purpose，provided that it shall not cause risks higher than expected by the subject of personal information.

Key Words：the purpose limitation principle，information protection，information utilization，personal sensitive information，the risk limitation

（责任编辑：王叶刚　赵建蕊）